# SYSTEMS APPROACH TO ENGINEERING DESIGN

PETER H. SYDENHAM

# Systems Approach
# to
# Engineering Design

For a listing of recent titles in the *Artech House*
*Technology Management and Professional Development Library,*
turn to the back of this book.

# Systems Approach to Engineering Design

Peter H. Sydenham

Artech House, Inc.
Boston • London
www.artechhouse.com

**Library of Congress Cataloguing-in-Publication Data**

A catalog record for this book is available from the Library of Congress.

**British Library Cataloguing in Publication Data**
Sydenham, P. H. (Peter H.)
Systems approach to engineering design—(Artech House technology management and professional development library)
1. Engineering design—Management 2. Systems engineering
I. Title
620' .0042

ISBN 1-58053-479-1

**Cover design by Gary Ragaglia**

**685 Canton Street**
**Norwood, MA 02062**

The following are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University: Capability Maturity Model®, CMM®, and CMMI®.

International Standard Book Number: 1-58053-479-1
A Library of Congress Catalog Card number is available from the Library of Congress.

10 9 8 7 6 5 4 3 2 1

# Contents

CHAPTER 7

CHAPTER 8

## CHAPTER 9

## Suitability and Operability Aspects of a Design 219

## CHAPTER 10

## Legal and Security Issues 249

# Preface

Since the 1970s, when systems engineering (SE) became an identified set of ordered principles, many books have been written that interpret what SE is perceived to be in the mind of the author.

This book shows how to use key elements of SE and systems thinking to support engineering detail design.

It addresses activities that are used to make design efficient; techniques that can be implemented by staff within the time limits of relatively moderate size design execution. It covers what is not, in my opinion, based on experience, given in engineering courses where depth still seems to be the emphasis at the expense of breadth of the knowledge now needed to be an efficient engineering designer.

It is written for those who have, or aspire to team leadership or want to take on increased team interfacing responsibilities. It enhances the material provided in engineering courses, thereby providing an element of finishing for its readers.

Each chapter covers different aspects of the technomanagement process used to develop an engineering design. The book generally deals with issues in the chronological order that they first arise in a project. Some topics, however, are relevant to the whole process. These have been placed appropriately in the sequence.

For best use of the book's content, read all of the chapters in sequence to gain a grasp of the whole. Once the topics and their relationships are understood, the book can be referenced for more information on specific topics.

Space limits the extent of the contributions; deeper material can be sourced via the citations given to relevant journals, books, and Web sites.

Content has developed naturally out of repeat deliveries of an annual semester-length course (also offered as a short course) given to new and mature students, graduate and undergraduate engineers, and applied scientists over the last 15 years. Many of the students involved, plus coworkers in Australia, Scandinavia, the EU, UK, and United States, have provided ideas, material, and useful critique by way of access to their teaching materials. Their assistance is gratefully acknowledged.

## CHAPTER 1

# Systems Thinking and Systems Engineering

This chapter explains the:

- Elements of systems engineering and systems thinking, these being the basis for understanding the methods and processes given in successive chapters;
- Drivers that influence good engineering design;
- Development of the holistic detail design philosophy and the programmatic viewpoints needed to execute good design;
- Distinction between the thinking styles of engineering reductionism and soft systems methods;
- The systems of systems approach to the design of very large systems;
- Place of test and evaluation at the systems thinking level and the special attention needed to measure performance control compared with the time and cost control techniques;
- Need to scale the degree of application of systems thinking to suit a given design team situation.

## 1.1 Systems Engineering Briefly Explained

### 1.1.1 The Systems Engineering Task

This book supplements engineering design practice by providing knowledge of ways to improve that activity through adoption of the so-called systems engineering (SE) culture and its related methods. To give a sharp focus it targets the level of responsibility of the design team leader. However, the techniques are applicable to designers within the team and to those in charge of several design teams.

A top-down approach is used to provide a reasonably logical framework for the materials. Content starts with development of the cultural aspects of systems engineering followed by an explanation of techniques that are mostly, but not solely, applied in the successive stages of the systems engineering life cycle. Some topics relate to the whole life-cycle activity; they are placed at a position where their background has been developed in earlier chapters.

A simple definition can be used to start to develop an understanding of the systems engineering (SE) task. Many exist; they all say much the same thing. The QinetiQ staff in the U.K. developed this conveniently short one:

> A set of activities which control the overall design, implementation and integration of a complex set of interacting components or systems to meet the needs of all users.

This clearly recognizes that engineering design tasks have to include numerous interacting issues to obtain a sound solution to the client's needs. SE, but not alone, makes use of a set of principles and processes that efficiently use resources to optimize a development project's progress toward a sound solution to a customer's need. The definition also highlights that SE deals with more than the physical energy/mass relationships of a system design that are well covered by detail engineering work. SE also deals with how the technical design task is executed moment by moment.

Systems engineering is not just a set of rules that are slavishly applied but more about a way of thinking and attitude that is an extension of much of conventional engineering design practice. Understanding of this thinking needs to be developed to the point where a good designer will readily select sound solutions to design situations not previously encountered.

Where the personal memory requirement needed to track the many issues that arise during a design exceeds one person's "brain-full," it becomes necessary to employ recorded processes to ensure each person assists in carrying out the design of the "right" thing.

Without the overall technical coordination supplied by SE practices, a design direction can be in quite the wrong direction yet is still being executed to the standards of best practice—as they were when a pallet loading system designed for a military transport aircraft was, all too late, found to need a custom-built forklift truck to load the pallets, to quote one costly example.

Technical designers tend to emerge from undergraduate education with heavy emphasis on the detail aspects of design in their field. For instance, an electronic engineer will be well able to design the circuitry and the packaging but will be far less skilled at knowing how to decide and justify which design method to use; how to interface it with its intended application; and what will be needed to satisfy health and safety issues.

Applying the SE culture is a case of being a specialist at being a generalist. It applies the widely used human thinking process wherein a large complex topic is to be broken down into smaller tasks until they lay within the expertise of the various specialist capabilities and can be understood.

Application of systems engineering is about deciding, for the technical aspects of a project, what should be done by whom and by what time? This kind of management task differs from that of office, corporate, or project management, however, the distinctions are not always that black and white. Figure 1.1 provides a simple model of the human teaming aspect of the engineering of systems task.

All teams must be efficient in their duty in order that the whole set of teams delivers the best practice design organizations constantly seek. Note also that numerous interactions will take place between the teams as the project passes from "customer need in" to "satisfactory system out." We return to this model later.

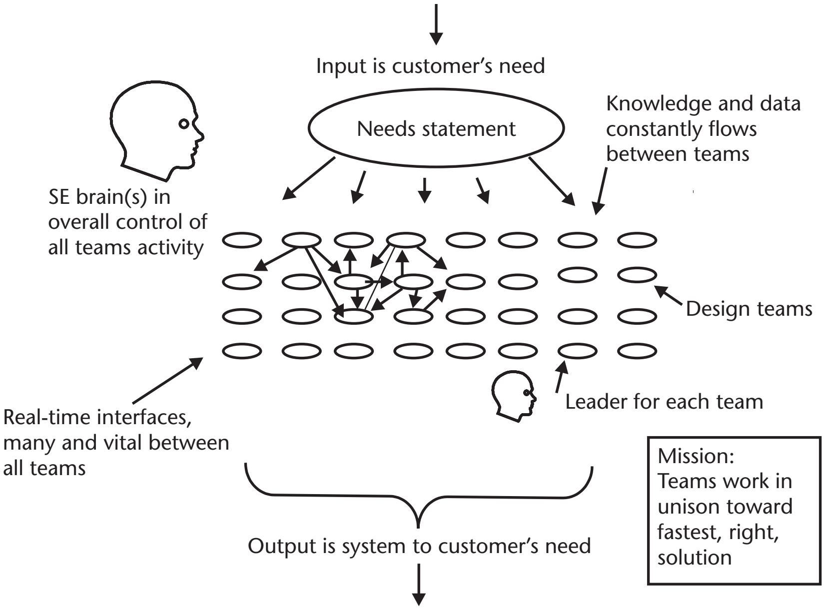


**Figure 1.1** Teaming representation of the SE situation.

### 1.1.2 Paradigms of Life-Cycle Management

The most popular way to provide a representational foundation for systems development uses the system life-cycle model. Development and use of all product or service systems follow the same generic sequence of life-cycle stages. While various specific expressions of this life cycle exist they generally follow the simple one illustrated in Figure 1.2.

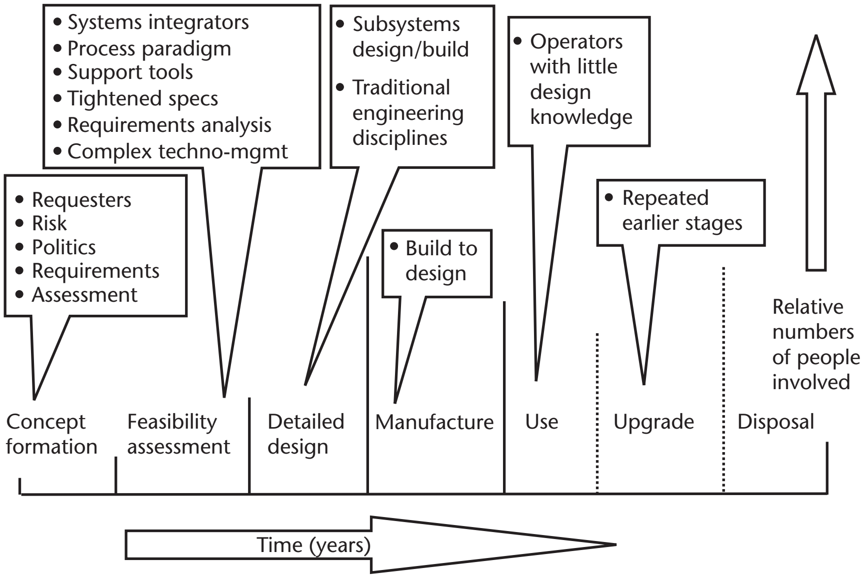


**Figure 1.2** Life-cycle stages of a product or service.

Good design and effective application of systems thinking are key issues within the tasks of all of the stages. To appreciate the differences between them we need to walk through the life cycle, beginning at the time of conception.

*Concept formation stage.* A need for a system arises. Creation of several operational scenarios here allows their comparison for selection of the best. Application of detailed design thinking here can be attractive as it might seem to provide a more comfortable feeling than the necessary vagueness of concepts. However, starting into detailed design thinking must be resisted at this stage. Instead, scenario building, mind-maps, systems dynamics, and other motivational modeling methods are used to support the creation of operational concepts that crudely, but sufficiently, model the various systems situations so that the salient features of an intended system can be investigated.

Development in this stage is best executed with top-down thinking starting from the requirement that is also fed with some bottom-up knowledge to keep key parameters bounded within practical possibility. This is where modern engineering design begins to create a range of computer-based system models that flow onward, with increasing sophistication, throughout all of the life-cycle stages of the application. Output of this stage is a small number of likely solutions that now need to be further developed to see if they are practical to build. It is also necessary at the end of this stage to assess if the project should be continued or shut down because it seems unreasonable to pursue. It is quite usual for many of these initial studies to not go on. Often it is used to sort out potential suppliers and their ideas for solutions to a need.

*Feasibility assessment stage.* Concept models are too coarse to allow it to be seen if they can be made within practical time, cost, and performance limits. Feasibility of the selected candidate options can now be assessed from their integration and implementation viewpoints. Here sufficient flesh has to be added to the conceptual bones of the system design to allow major practical limitations to be seen. The output of this stage should be a better understanding of reality about the small number of possible solutions realized in the previous stage.

*Detailed design stage.* Specialist area engineering designers continue here to flesh out the design by developing the details of the actual nuts and bolts decisions that allow things to be physically formed. The output here is a large set of detailed plans and considerable design information that collectively dictates the actual physical features of parts that when manufactured will assemble to yield the system needed. At the end of this stage, the information must be near to being absolutely right, for it is now very expensive and time-consuming to change design features. Error correction at this stage is most expensive. The end of this stage also takes the project from a paper or computer-based study into the often irreversible commitment to "cut metal" that, if wrong, is usually sent to scrap with hard-to-correct loss of time to use.

*Manufacture stage.* Technical design now passes on to manufacturing of the system. An important transition takes place. What the designer thought was satisfactory is tested here when applied to large-number production levels. Design activity of earlier stages must have thought ahead to this stage to seek out and correct errors in the information passed on. The output of this stage is the deliverable system that is able to perform its role as originally intended. Too often one hears of major products that need extra work to make them operate properly. A good example of this defective state was a much-hailed portable computer that needed a dongle to correct its operation. To get it to work, this inserted dongle used up most of the computer's working memory.

*Use stage.* It is here, in the final operational role, that the quality of the design will be tested. This is the toughest test—where it hopefully stands up to all that is asked of the design by users. The output here is a long useful life in which costs of ownership and use are as expected. Discovery of more knowledge about the system is useful spin-off as that allows upgrades and new systems to be explored.

*Upgrade stage.* The original design will often be upgraded throughout its working life. This arises due to improvements in technological capability, especially in the IT regime, changing user needs, and the constant pull of the marketplace to maintain competitiveness. Good design will have already looked ahead to allow for this and provided a good set of understandable and reusable design records.

*Disposal stage.* Early design consideration is essential to obtaining efficient and safe decommissioning. Overlooked things can be very costly to correct. For example, a radioactive source used in a density-measuring gauge should be formed as a self-contained unit that can be removed for disposal without the whole unit having to be recycled in the same rigorous manner as the radioactive material.

We now look at the evolution of this basic life cycle, as that will allow an understanding of how we came to be where the industry is today.

The first well-disseminated definition of the SE life cycle assumed that each stage could be completed with little regard for the needs of later stages. After all, if it starts out with a clear and correct user requirement, then if each stage is done well enough, it seems reasonable to assume the whole will work out as needed.

This simplest life-cycle model became known as the waterfall process because the outcome of each stage, its documents, flowed over the edge out of its life-cycle stage to fall into the pool of the next stage. A commonly heard alternative metaphor portrays documents, on their completion from a stage, being thrown over the wall to the people executing the work of the next stage. In its worst case of use, no one looks far enough ahead and no one looks back. Justification for this being a sound way to proceed is that if the design process can be perfected, and if enough time and resource can be devoted to each stage, then all that is needed will be made available to the next stage.

This thinking is, however, easily shown to be flawed. The process of design of a system that has not been created before is itself a creative scientific learning experiment. Not all of the information needed is available as design proceeds.

The waterfall idea will only work well enough for closely replicated systems where little change in design is needed. The engineering of new systems will invariably have to cater to elements of major change.

The waterfall life cycle is, however, the basic one from which better ones are generated. It needs modification in use because it too easily fails due to long delivery times and inefficient interfacing between stages. It is not realistic to think that a project can be set off into the future without any feedforward and feedback of ideas—extensive amounts of iteration are absolutely essential to reveal errors early where they are inexpensive to correct.

The teaming model of Figure 1.1 shows that there exist numerous interfaces for communication of design information that need to be satisfied for design decisions to be adequate. An analytical systems investigation technique known as $N^2$ analysis has reliably shown that at least 50% of all potential interfaces between designer's briefs will be invoked at some time in a project's life cycle. That is a lot of communication!

A significant improvement can be obtained by adding means to verify that the requirements, not the stage tasks, are maturing satisfactorily at the end of each stage. By adding testing and validation paths, the simple SE life cycle can be redrawn as the Vee life-cycle process (Figure 1.3). Note that the tasks on the left side are all paper- or computer-based design activities and those on the other side are those involving manufacturing implementation of the system.

A significantly better process results but still more improvement can be obtained.

Carrying out some tasks of different stages in parallel, rather than in serial, results in the concurrent engineering approach. An integrated product team (IPT) is established from the outset to represent, in each stage, the important needs of all life cycle stages.

Figure 1.4 demonstrates in a simplified fashion how concurrent working saves time. It also shows how it encourages iteration; reviews of a previous stage output can be a useful input to other stages.

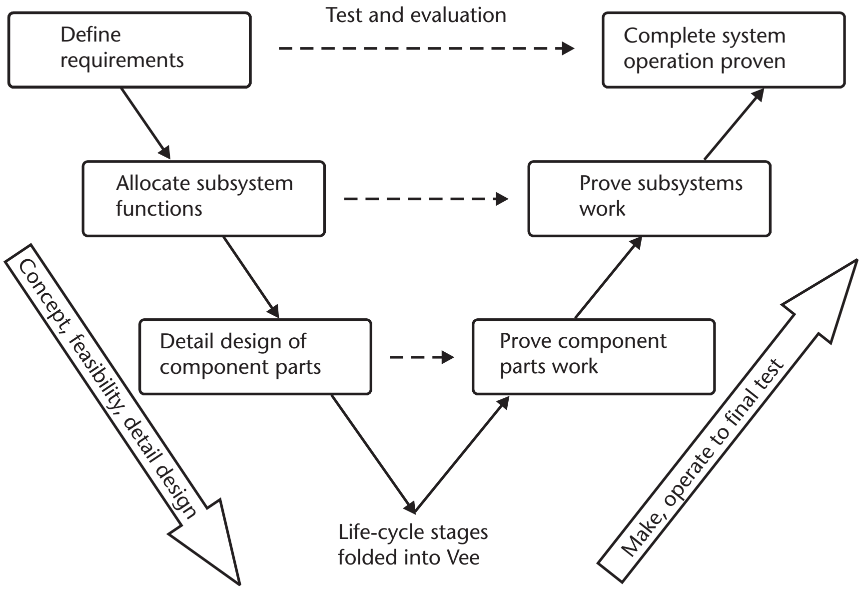


**Figure 1.3** Folding the stages of the waterfall life cycle and adding evaluation links leads to the Vee life-cycle process.

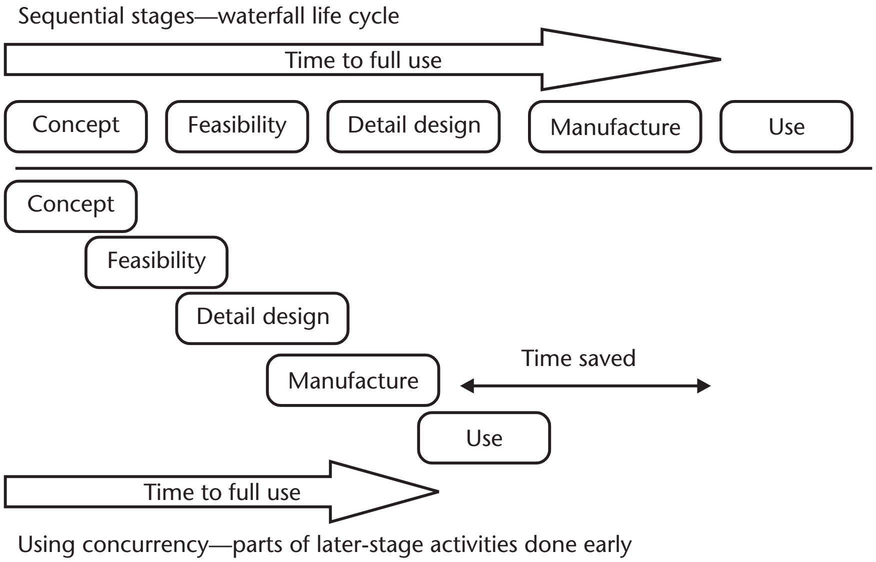


**Figure 1.4** Concurrency is used to speed up and improve the efficacy of the SE life cycle.

Further tuning of concurrency and timing issues leads to variants of the basic SE life cycle. Some examples that are commonly used are:

*Spiral diagram method.* Concepts transform into robust designs by spiraling many times around the "concept to use" stages of the life-cycle loop. This is used extensively in software systems development. Hundreds of such spiral cycles may take place before a product is ready for use.

*Evolutionary acquisition.* Here improvement in system capability is continuous as new knowledge is obtained about the maturing need. Commercial product development uses this form extensively, allowing new applications for a proven technology to be exploited via progressive advances. Examples are found in the development of the automobile and the cell phone system.

*Incremental acquisition.* This is similar to the evolutionary approach, but here a small number of planned upgrades increase progressively the originally intended functionality.

### 1.1.3 Kinds of Activity of SE

Many SE activities arise within a project. The ISO/IEC 15288 systems engineering standard states these to be:

6. System Life-Cycle Processes

    6.1 Agreement Processes
        6.1.1 Acquisition Process
        6.1.2 Supply Process

- 6.2 Enterprise Processes
    - 6.2.1 Enterprise Management Process
    - 6.2.2 Investment Management Process
    - 6.2.3 System Life-Cycle Processes Management Process
    - 6.2.4 Resource Management Process
- 6.3 Project Management Processes
    - 6.3.1 Planning Process
    - 6.3.2 Assessment Process
    - 6.3.3 Control Process
    - 6.3.4 Decision Management Process
    - 6.3.5 Risk Management Process
    - 6.3.6 Configuration Management Process
    - 6.3.7 Quality Management Process
- 6.4 Technical Processes
    - 6.4.1 Stakeholder Needs Definition Process
    - 6.4.2 Requirements Analysis Process
    - 6.4.3 Architectural Design Process
    - 6.4.4 Implementation Process
    - 6.4.5 Integration Process
    - 6.4.6 Verification Process
    - 6.4.7 Transition Process
    - 6.4.8 Validation Process
    - 6.4.9 Operations Process
    - 6.4.10 Disposal Process

A particular design team's activities may not encompass all of these but members do need to be aware that they are going on within the project at large. The various activities need to be allocated an appropriate amount of effort to suit the size of the project. The list finds use in identifying any overlooked issues of system development.

### 1.1.4 Drivers of Change in SE

Leading innovation is often very risky. System developers tend to follow the design fashions of their time. To stay competitive, lead designers need to follow the market. Several drivers are now identified.

Universally, demand for systems requires three dominant aspects of a project to be optimized, generally described as the cost, time, and performance (CTP) factors.

*Cost:* The financial control regime. Those paying for the development invariably expect the system to be less costly to develop than previous similar forms.

*Performance:* The performance control regime. Customers and users demand more functionality, easier-to-use systems, greater reliability and supportability, less maintenance, and many other performance issues.

*Time:* The time-management regime. The "time to use" has to be timed to meet market windows of opportunity and to be ever shortened, these being done to hopefully fend off competition.

Attempting to optimize all three factors simultaneously flies in the face of expectation, as they do not appear to be mutually acceptable. However, adoption of improved SE processes seems to be able to significantly improve all three simultaneously.

Other key drivers for change exist.

*Smarter customers and buyers.* Customers are getting ever smarter in stretching requirements by extrapolating them and joining sets together. All too often they inappropriately combine good performance parameters that were not previously obtained in one system design. Unrealistic demands are often bid for by a contracting organization in order to win a contract tender. The less smart customer subsequently then has to live with an unrealistic development situation after the contract has been signed.

*Lead-time to market.* This is ever reducing. The degree of reduction is often almost unbelievable—the time taken from need to delivery into service of a major passenger aircraft development can now be a mere 3 years, not the 10 years of earlier times. Automobiles take typically 3 years to reach the market. Many electronic consumer products are now developed, manufactured, and shipped in as little as 6 months!

*Digitization of everything.* Analog information systems will be reborn in their digital equivalent form for they are usually more reliable, easier to modify (via its software), more accurate, cheaper to make, and conform better to market expectations.

*Communications advances.* All systems generally have a significant IT component so this is almost always an important driver. The application of Internet and cell-phone technology networks, plus the hunger for wider band information flow, constantly fuels a seemingly never-ending expansion of communication networks and products. Their components soon find their way into other product areas. Commercial off the shelf (COTS) subsystems create new design solution opportunities for systems builders. For example, the low-cost, high-performance subminiature Blue Chip™ transmitter/receiver systems is now found in many instrumentation products and most modern laptop computers.

A project should never lose sight of its design drivers. It is necessary to realize, however, that while the design team has some control over them within their own subsystem activity, overall success of a development depends much on how the systems engineering of the project is being managed within the whole of the systems development organization.

Change is ever present so the above factors need constant attention, a matter taken up in Chapter 12.

## 1.2 Overview of Systems Thinking

### 1.2.1 Basics of Systems Thinking

Applying SE to the design task is a matter of being able to recognize what kind of activity is appropriate to do at any particular time. This ability is developed by reading, taking courses, working with experienced practitioners, and using every opportunity to bring fresh, better, solutions to design situations.

Underpinning the professionalism of SE is an appreciation of what is known as systems thinking. Before we can delve more deeply into that, we need to first discuss how engineers and physical scientists go about their thinking.

In the seventeenth century, Descartes suggested we solve problems by applying a consistent paradigm of successively breaking down a problem until a level is reached where sufficient understanding exists. Do this for all branches of the resulting tree. If all subproblems are solved, then an overall solution to the problem would seem to be a certain result.

This paradigm for problem solving is known as reductionism. Most engineers may not have heard of the word yet practice it extensively. It is the basic thinking methodology of science and engineering. It has been applied with great effectiveness in the hard sciences and in detail engineering situations making use of science.

Taking the idea to the next logical step, it is seems reasonable to assume that a system rebuilt from a set of subsystem solutions must be a sound overall solution. This is, however, not necessarily so.

A significant reason limiting its success is that small deviations in subsystem solutions propagate upward, leading to major errors in the overall required performance. This difficulty compounds as the systems get larger and the subtasks are sufficiently different from a person's prior experience.

Difficulties in not meeting requirements, despite the best intentions and professionalism, can also be put down to the fact that the traditional engineering viewpoint often cannot cope with the complexity of real systems unless reductionism is supplemented with other kinds of thinking.

In the reductionism design approach, a closed model of the design situation has to be realized to complete and close the design boundaries. Care is needed in setting up these boundaries. This is taken up in Section 5.2.1. For example, consider the design situation for the data logger circuitry of a geophysical borehole logging system. If the most commonly encountered electronic circuitry technology (silicon) is selected, then it will surely fail to operate properly due to the steady temperature rise as the depth of the borehole increases. Silicon substrates are so commonly used that it will be expected that this technology would be selected, but in this application the useful borehole depth is limited by the temperature limit of silicon. Gallium Arsenide technology would be needed for the deeper probes.

A very common design error is to not fully investigate the extent of the influencing boundary of the system; it may be closed too far in from reality. Many engineering design situations contain issues that do not lend themselves to reductionism thinking. The ability to recognize the nature and scope of these limiting parameters needs skill in design team operations.

Systems thinking aims to create a methodology to assisting reasoning for understanding and creating evolving systems. It includes attention to:

- Human activity systems, not just the inanimate physical objects that make up the whole;
- Operational readiness and suitability (i.e., will it do the job when called upon and will it continue to perform its task for as long as expected?);
- Systems at all levels and types.

The fine points of systems thinking are far from settled areas of intellectual thought; authors are still interpreting the issues. Key statements have been published on systems thinking by engineers involved in major projects; [1] is well worth visiting for its mind-opening views.

An essential need in the engineering of systems is to optimize the use of all resources involved in a development (see Chapter 8). Use of the reductionist paradigm is very attractive, as it seems to give solid, defendable answers to design problems.

Pragmatics, however, dictate that engineering designers cannot work with fully closed design circumstances, but instead, must wrestle with numerous problematic issues using a toolbox of different thinking methods.

Some key tenets of systems thinking are:

- It is concerned with wholes and their properties—the term *holistic*, much used in the humanities but less so in engineering, is an appropriate descriptor.
- It is concerned with systemic thinking (i.e., including all of the issues) as well as with systematic thinking (i.e., being methodical in tackling problems).
- Systems consist of hierarchies that relate to each other through numerous interfaces, each having their own kind of requirement.
- All parts of the whole are interconnected (interface is an alternative term) to a varying degree; some are very dominant and thus have greater influence on the behavior of the whole. The $N^2$ interface study, mentioned previously, shows that designers should not work in isolation!
- Parts of the whole will have their own important emergent properties. These are key performance parameters that may not have been expected. They can exert a great influence on the other systems with which they interface. Unexpected nonbeneficial emergent properties become very apparent once the system is in service. For example, it might be have been decided to use a microminiature wireless telemetry system to communicate temperature data from inside the flying suit of a pilot, only to find after commissioning that it causes the flight navigation system to be inaccurate. Today this is an obvious design factor to expect, but that was not always the case or we would not have to turn off mobile phones in hospitals and aircraft.

### 1.2.2 Emergence of Systems Thinking

The study of living systems in the 1940s seems to have been the starting point of scholarly researched systems thinking. Researchers in the life sciences were driven by a need to better understand how nature works and controls itself. Out of this pioneering work emerged general systems theory, cybernetics, self-organizing systems, automation, automaton systems, organizational science, operations research, systems science, and more—topics with which engineers are not usually that familiar. These are now yielding knowledge of use to engineering design.

Those explorations have given sounder understanding about the relationships between the various paradigms of problem solving, of the nature of inquiry, of what kind of system is needed in a given situation, and of possible solution methods.

The bases of systems thinking are illustrated in Figure 1.5.

A model of the layers of system openness starts with the outer total shell that includes everything thought to be of relevance to the problem that Figure 1.5 represents.

Inside this layer is placed the study of how the different systems viewpoints are expressed. This has two thinking aspects—philosophical systemic thinking that is often hard to apply, and the various pragmatic-working areas that the various kinds of thinking use to advance their problem solving. Engineering can be seen there as generally making use of all of the domains shown in Figure 1.5 with the exception that the use of the soft kind of systems is not well developed. We return to that deficiency in Section 1.3.

### 1.2.3 Models of the Hierarchy of Systems

Trying to represent the whole of all systems activities and the relationships would be a massive task; there are too many issues to cover. Instead, we must make use of models that give insight into aspects of the whole. Here we show three different models, each revealing different characteristics of the same generalized whole.

The first model relates the groups of people involved and the sciences, as well as the thinking involved (Figure 1.6).

Three key kinds of interrelated activities are shown: the natural world, the sociopolitical system, and engineers and scientists at work. The needs of all three must be met for a system design to be successful. Not long ago, engineering largely neglected the other two, but today sociopolitical and natural-world aspects are taken into account.

Each regime can be represented by a triangle. At the base of each triangle sits the scientific formal, quantitative thinking workers. Moving up each triangle, the thinking style used changes from essentially quantitative to qualitative, taking in people's feelings and emotions. The bottom areas are where the engineering and science disciplines operate best. The middle ground is where the use of SE finds effective application. At the top, all manner of often inexplicable decision-making takes place, not because of lack of skills but for lack of any formalized way to do it better.

Why is the representation given as a triangular shape? The width of the triangle at any given level crudely depicts the number of people involved. It is interesting to note that as little as one person at the top of the triangle can decide how the many

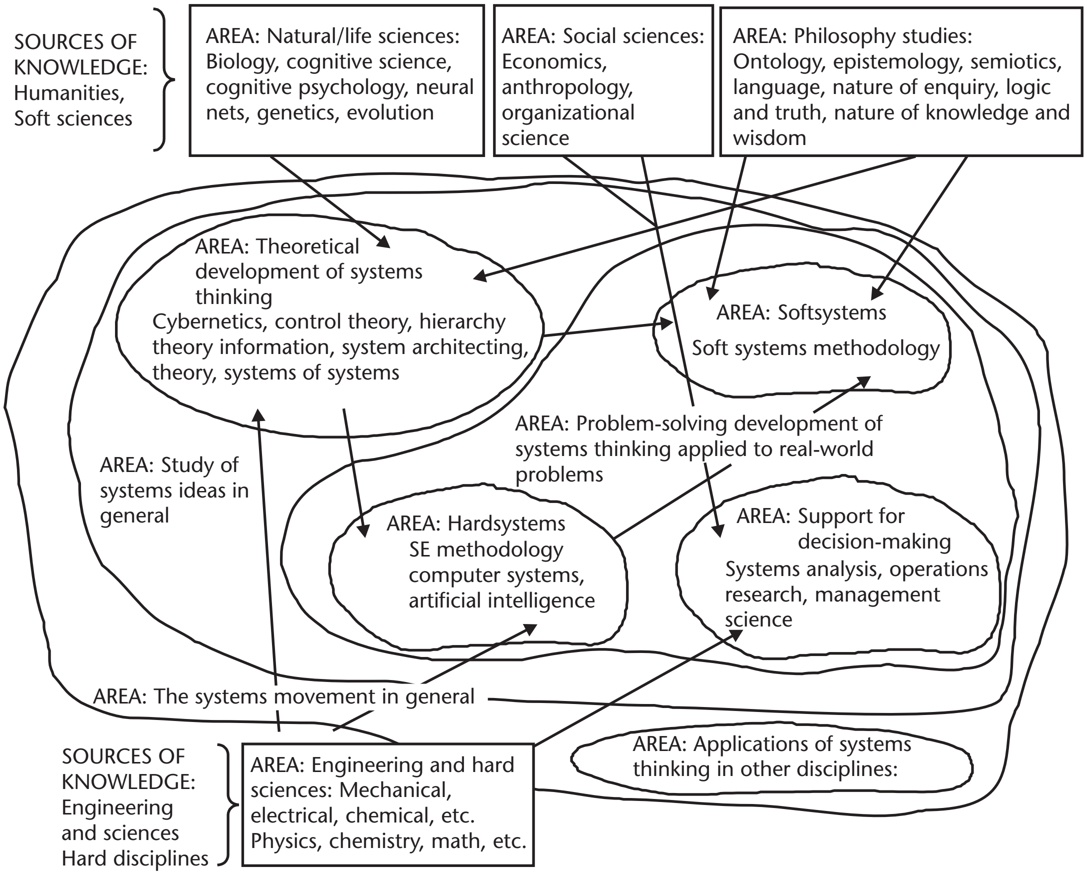


**Figure 1.5** Representation of the relationships of the key disciplines. (*Source*: [2].)

people below use their personal resources and skills. Large groups of designers are involved in taking the ideas of a few to fruition. The designer generally has little influence over the top-level needs and has to work within given requirements.

The second model, Figure 1.7, shows how the design team works within a multilayered set of quite different environments. For overall success, a project must make allowances for the nature of the limitations and controlling factors that exist for the type of enterprise in which the design team works. These issues vary greatly. For example, a private organization does not have to disclose as much information about its processes to the public as does a government institution. To keep on top of many problematic issues, it pays to appreciate the higher layer affairs that are impacting on a design team!

This book largely addresses how to better practice design in the interface area between detail engineering and systems engineering. More detail of this situation is given elsewhere [1] and [3].

The third model [4] given here as Figure 1.8, assists appreciation of the classes of system design that can arise. It assists a designer to identify what kind of difficulties the design team might expect to encounter.

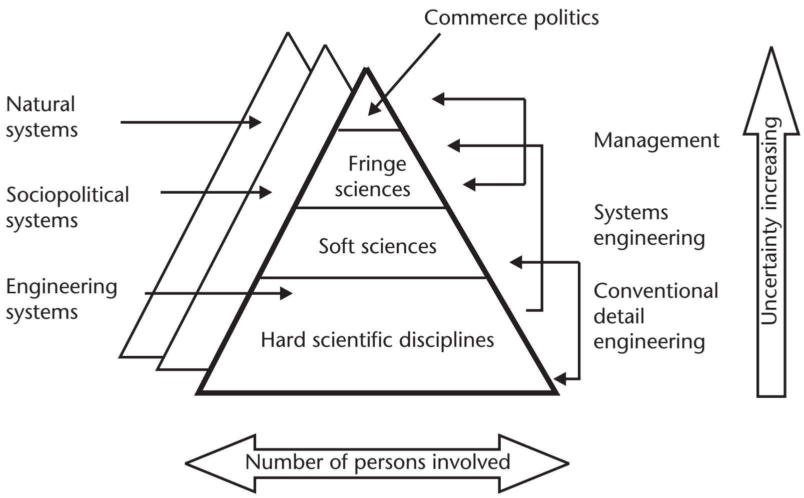


**Figure 1.6** "People and science" model of a systems activity.

This model is based on mapping the various kinds of systems that arise onto a space represented by two variables: the degree of disagreement on systems issues that exist versus the degree of uncertainty of their characteristics.

The types of systems shown in the diagram are:

1. Straightforward technical design tasks that inherit considerable know-how and have low risk in execution (e.g., a simple road bridge or electronic amplifier board).
2. Technical tasks with a modest degree of design change and thus including a clear degree of risk (e.g., a network for 3G mobile phones, a major automobile model change with advancing functionality such as moving to all-wheel drive from dual-wheel drive, or a ground station controlled space telescope).

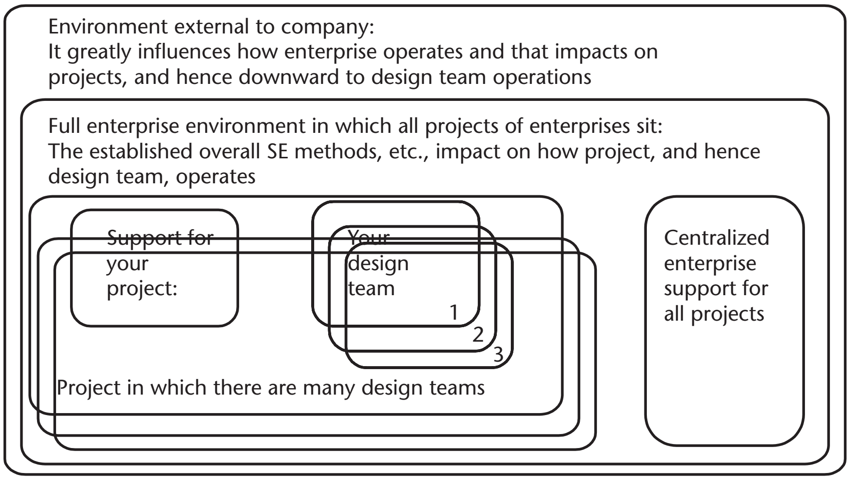


**Figure 1.7** Environment layers in which a design team works.

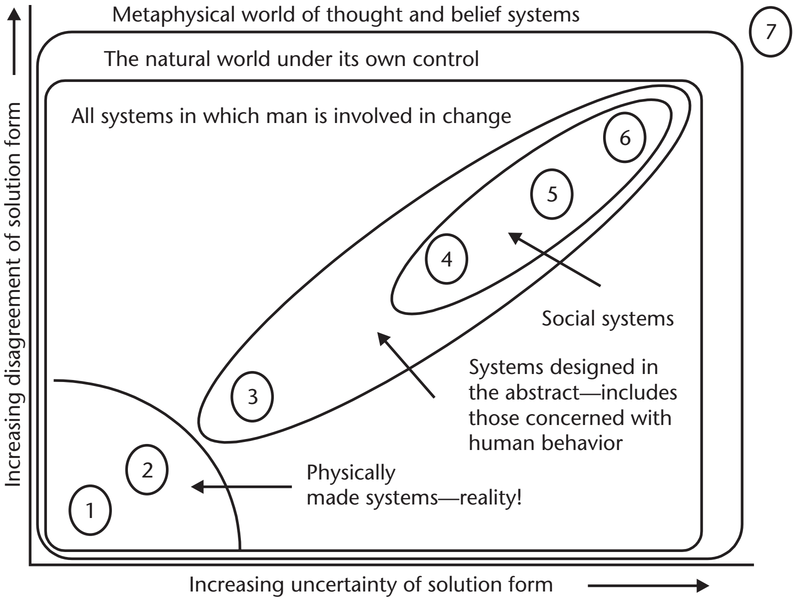


**Figure 1.8** Diagrammatic representation of a hierarchical classification systems. (*Adapted from*: [4].)

3. Engineering systems involving considerable human control and intervention in their operation but not so much in the overall organization (e.g., control and command systems in civilian and defense applications, production line manufacturing systems, or transport systems).
4. Systems where their major subsystems components are associated heavily with human organization. Here engineering risk issues are low compared with the risks of understanding the human behavioral aspects (e.g., evacuation systems, airport systems, or educational support systems).
5. Systems where human attitude is dominant and largely unpredictable (e.g., change management taking place in a factory, speed control on roads, or engendering professionalism).
6. Systems that are as complex as people think they can build and so often attempt (e.g., war and fighting, and harder, peace-making and -keeping at the top, and societal policy systems).
7. Systems that can only yet be represented by the abstraction of the thinking world of science fiction and theology (e.g., utopian worlds or God-like abilities of design).

As the risks rise and the system's nature becomes more problematic, it becomes increasingly impossible to be certain about numerous critical systems issues. Those involved are increasingly unable to agree on what kind of solution to use.

Another way to recognize what class of design problem is involved is explained in Section 1.3.1, where an organization-type classification is given.

Most civilian commercial projects sit in the lower two classes because they tend to exploit proven technologies and because they need to work in relatively low-risk areas.

The engineering detail design team is usually working, by necessity of delivering a reliable outcome, in the high certainty and low disagreement area with respect to their design solutions. However, they may well be involved in the execution of most of the classes given. As the position number increases, the detail engineering design component becomes of lesser importance to the execution of the whole as it, in itself, is unable to provide solutions to the problems at the current state of best practice.

It is, therefore, important to be able to recognize the class of system in which the team is working; the surrounding climate of thinking can make a large impact on progress and on the type of solutions that will be accepted. Staffing issues are taken up in Chapter 3.

## 1.3 Modern Systems Thinking in Engineering

### 1.3.1 Soft Systems Methodology

Reductionism has served engineering and science well but it cannot provide all of the solutions to systems design above around level 2 to 3 in Figure 1.8. In those areas the reflective, broadly thinking, person is expected to find solutions by use of engineering design know-how as is seen to work elsewhere. This is a flawed approach. Design engineers overly seek to use the reductionist approach because that is the main method in their design toolbox. They are less well equipped to find sound solutions that suit systems involving extensive human activity.

In the 1970s, an engineer in charge of major engineering projects in the U.K. was dissatisfied with the fact that reductionist engineering approaches were not always working well enough. He subsequently devoted time to developing an improved methodology [2, 5].

Figure 1.9 gives the flow of activities for finding and implementing a solution in a soft situation. This methodology is of the phenomenological kind used extensively in the humanities disciplines, but less so in the hard sciences and engineering. It became known as the soft systems approach to systems. Out of that pioneering work developed the soft systems methodology (SSM).

The SSM process begins with the problem being identified as being unclear and lacking an obvious reductionist solution. As a start it will invariably contain a large people element.

Applying whatever method works to obtain the system's key parameters, the need is then expressed in writing.

The kinds of purposeful activities are identified and conceptual models generated and compared with the former starting point of the real situation.

Extreme differences are then rectified in that model and the implementation is adjusted to make it sufficiently acceptable to the people involved in the necessary change. This type of modeling is not nearly as precise as found in conventional hard science, but it is satisfactory.

The overall design loop is then closed by implementing the best available plan.

This process is then repeated until reasonable success is achieved. Considerable iteration may be needed to reach an acceptable situation.

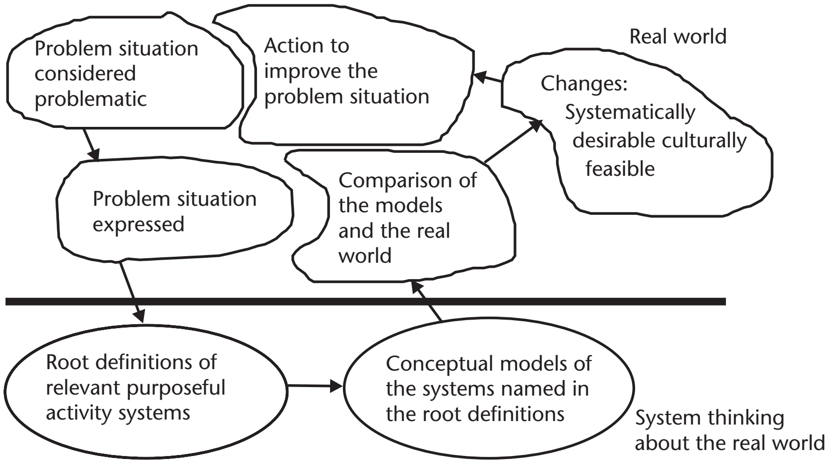


**Figure 1.9** Flow of activities in finding and implementing a solution to a soft system situation. (*Source*: [2].)

As is well experienced from observation of the outcomes of so many of the large systems developments, sitting in the higher classes this form of problem-solving does not have the success rate associated with those systems design needs where reductionist methods clearly do work. Success is not assured with the soft system methodology but this is one of the few ways known to seek design solutions for problematic system designs.

While this does apply elements of reductionism—it uses a less-certain form of the formal scientific investigation process—it is different in that with this solution methodology, the system designers get "inside" the system situation trying out various candidate solutions on the existing system to find out what works well enough.

In contrast, the hard engineering solution path starts by developing a separated model of the whole by metaphorically pulling it all apart to identify its subsystems. The resultant set of component parts and their interrelationships are then simulated using a computer to investigate the sensitivities of the various critical issues. Optimization methods are then applied to facilitate changes to be made to the model. When the right model and its parameters have been realized, the real system is rebuilt to form a new system. Parts are then put back into place to see if the whole works as intended.

Humans, however, cannot be understood as technical machines. The physical part of the whole, the body, behaves reasonably well according to well-known scientific laws, but the mind in control of the body does not! People can be slow and reluctant to respond to the direct process of change. Changing organizational cultures can be very difficult, costly, and take a long time to achieve. People have self-will and often will use it in quite contrary ways.

How else can one recognize the type of organizational situation that exists for a new project? Some useful ideas on this are found in organizational science [6]. Systems will first be either of the simple or complex kind. Complexity here is not only determined in terms of the number of variables involved but also on how they interact, and if human behavior is involved.

On the other hand, the "actors" in a system situation can take on one of three basic attitudinal standpoints of behavior. First, they may all think alike and cooperate using the same methods. This is called unitary behavior. Second, they may well think somewhat differently from each other but still work as a coalition team with all having a common goal. This is called pluralist behavior. The third state is where all of the actors are certainly not pulling together, and in fact are all attempting to pursue quite different agendas. This is called coercive behavior.

Using these five simply understood variables, a chart can be constructed [6]; see Figure 1.10.

The main theories purportedly available for handling the various types of system problems are shown in the various locations of the chart. Note that there are no accepted workable methods for the more difficult complex-coercive (C-C) situations that generally represent the systems classes of 3 and higher in Figure 1.8. Routine engineering design, unfortunately, fits well only in the simple-unitary (S-U) location.

However, it is often engineers who are expected to develop solutions for the kinds of systems with which they are not well versed, and for which there is often little chance of success as measured in hard science ways.

The differences and capabilities of the various methodologies that are encountered in SE activity can be plotted onto the appropriate box of the chart in Figure 1.10.

Engineers feel comfortable in the S-U box (locations 1 and 2 in Figure 1.8) but less so elsewhere. Reductionist-trained people find it hard to accept most of the methodologies shown, for they are considered to be inadequately formal, quantitative, and scientific (i.e., not reductionist enough).

The design team leader needs to recognize the kind of system class in which the design team is involved and set up appropriate team membership.

### 1.3.2 Systems of Systems

As people have learned how to better organize and design technical systems, these systems have grown in size to an enormous extent. Many of today's major

| | | All think alike | All think as a coalition | All disagree, all of the time |
|---|---|---|---|---|
| Complexity of relationships | | Unitary | Pluralist | Coercive |
| | Simple | • Operations research<br>• Systems analysis<br>• Systems engineering<br>• Systems dynamics | • Social systems design<br>• Strategic assumption surfacing and testing | • Critical systems heuristics |
| | Complex | • Viable system diagnosis<br>• General system theory<br>• Sociotechnical systems thinking<br>• Contingency theory | • Interactive planning<br>• Soft systems methodology | No adequate methodology —but this is the real SE problem area |

Type of relationships

**Figure 1.10** Mapping of various systems methodologies onto an organizational space. (*Source*: [6].)

man-made systems have evolved from existing systems projects that are progressively combined to form very large systems.

For example, availability of the early automobile, a system in itself, created other emergent requirements for a highway system formed of roads, service stations, fuel production, spare parts, hotels, traffic signals, road rules, vehicle registration, and so on. At some stage, such large wholes are seen to be too large to be considered as suited to the usual methods of management and design. In recent years the name "systems of systems" (SoS) has been coined for such systems.

A main driver for SoS developments has been in defense systems. There first was the personal weapon system. Then came team use of weapons, combining the various forms of firepower with behind-the-lines support logistics and intelligence inputs. That was followed by many kinds of platforms combined with the necessary command and control needed in a campaign structure.

The sophistication and number of cooperating systems has ever increased in defense, civilian commercial and government systems, and in the search for solutions to societal and humanitarian problems.

It became obvious that the former paradigm of first building general utility platforms (the ship, airframe, armored vehicle, etc.) on which are then mounted control and command, weapons and other systems, as separate entities were not adequate. This system needed the SoS approach. Similar thinking is needed in civil aircraft control systems that now span countries, and in integrated power grid operations.

So what are the differences between systems thinking and SoS thinking? This seems to be a matter of degree. An SoS is an extension of general holistic considerations and has the following characteristics:

- High complexity comprising relatively independent systems that can each be regarded as a sophisticated system in their own right;
- Continuously evolving as the emergent properties of each system interact;
- Have no obvious start or endpoint goals for their existence;
- Parts are often geographically distributed;
- Component systems retain much of their independence, pursue their own goals, and have independent management;
- SE activity is dispersed and loosely controlled;
- They are viewed as a set of interacting, separate systems;
- Understanding the behavior of constituent systems needs transdisciplinary (each is learning from the other) approaches, not just multidisciplinary (each does its own thing, usually with an insufficient number of disciplines).

The concept of an assembly of systems is not new, but here it is used to assist management of a larger whole than has hitherto been experienced as a class with its own specific characteristics.

## 1.4 Role of Test and Evaluation

### 1.4.1 Need for Test and Evaluation

The design drivers of cost, time, and performance (the CTP factors) each need their own management specialties to control them:

- Time is managed with project management.
- Cost is controlled with accounting practices.
- Performance can be managed with formalized test and evaluation (T&E) but this does not (strangely!) attract the same level of resources as the other two control mechanisms.

Implementation of sound, through-life T&E practices can provide ongoing data on the maturation of the system's critical issues (CIs). These can be used to tell managers, clients, and financiers that development is moving toward completion on time, within budget, and with the performance required.

T&E should be regarded as a whole of life process, not just as a set of tests made at strategic times. The need for T&E is summed up by asking three key questions of a system development:

- What are the system's development teams trying to achieve?
- How will those concerned know when the performance objectives are reached?
- Who is responsible for a satisfactory performance outcome?

The test aspect of T&E is often seen as all that is involved. It is not practical to test everything. Data from tests has to be relevant and collected according to a preset plan. A well-run project will not be using testing as an experiment to find out what has been developed, but to verify that the performance of the system is where it is expected to be. A "no-surprises" project situation should be the aim, and T&E is a key mechanism to achieve that condition.

The first text on T&E as such seems to be that by Stevens [7]. The case for T&E to be given more status in systems development and operation has been well made [8, 9].

Investing more resources in T&E for a project has the potential to prevent cost overruns and failed systems. Unfortunately, all too often this apparent overhead cost is the first to be pruned when overruns arise.

### 1.4.2 Nature of T&E Practices

T&E is often practiced in an ad hoc informal manner, as a band-aid activity to find out things when a project is not going well. In this form it has the following deleterious features:

- No adequate traceable or recorded control process exists.
- Success relies on the various designers' abilities to know when and what to test, after which they often have no adequate records addressing the three T&E questions given in the previous section.

- There is a real chance that the system elements the various design teams are developing will not integrate without considerable rework. This situation can arise, not because of lack of competency in performing good detail design, but by simply designing the wrong thing.
- Omitting the overhead of planned T&E activity can indeed save short-term cost. Doing this, however, significantly increases the risk of not obtaining final success. T&E expenditure can save wasteful later rework by detecting early design errors at a time in the life cycle where it is much less expensive to correct while the design is still on the drawing board. Early error detection is taken up in Section 5.2.3.
- Last-minute decisions are made on what to test. This can lead to poor testing, as the materials and equipment, not being planned ahead, are often not available.
- There exists too much flexibility in setting up tests and how to process the data for evaluation purposes. This leaves things very open for biased tests to be implemented to obtain an apparently satisfactory result.

This surely must be an overstatement of the situation. Reality, however, has many systems development lessons to be learned on record that show how devoted managers can become in defending their project by hiding and distorting the truth. T&E acts as the honest broker.

So what can be done that is better than the ad hoc situation?

The first step is to recognize that T&E is an activity required across all life-cycle stages. The range of tasks involved covers assisting with systems engineering planning through budgets for test equipment and facilities, to conducting tests using the data to carry out evaluations of how well activities are progressing. Figure 1.11 provides a simplistic overview of these activities. With the increasing use of modeling and simulation, the T&E task also includes model verification as well as setting up and conducting field tests of equipment (see Section 11.4.6).

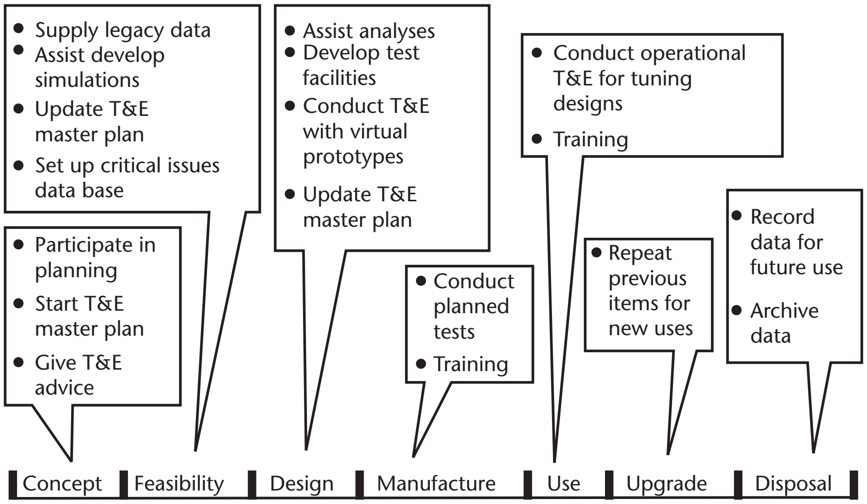


**Figure 1.11** Some key T&E activities during stages of a project.

An important thing to recognize is the need to plan T&E activity from the commencement of a project, not at the end of a development stage. A suggested methodology for implementing T&E is given in Section 2.5.2.

## 1.5 Application of SE to Design

### 1.5.1 How to Apply SE to Engineering Design

When a design team is part of a large systems provider house, there is usually a person responsible for organizing the systems support for all teams. Indeed, many larger engineering corporations have a corporate vice president to cover SE. In such situations, teams usually are provided with a:

- Company-specific SE process manual;
- Computer-based support tool system and support mentors;
- Special development facilities as needed according to the project;
- Sound communications and design records archiving, and configuration management system;
- Safety control process;
- Design controls;
- Sources of advice and mentoring for junior staff;
- In-house training and more.

This book does not attempt to cover the broader systems engineer level of appointment. That kind of know-how takes years of experience to develop, starting out as a team designer to eventually attain the "reflective practitioner" status needed.

Material presented here is a support resource for people in design teams and their leaders. It aims to provide concepts and practices that will assist these people to cope better with design in the more open design environments that are increasingly called for today.

As a guide, design team leaders need to be familiar with the basics of systems thinking and the culture of systems engineering. They need to have to hand copies of foundational books on SE practice [10–12] and refer to these for concepts and methods to employ as project problems arise. A sound source of SE knowledge is found in the general pages, and those of the technical committees of the International Council on Systems Engineering (INCOSE) [13].

The U.S. Department of Defense (DOD) *Military Handbook on Systems Engineering* MIL-STD-499B [14], although being comparatively old as standards go, is still an excellent source of ideas for use at the various stages of the life cycle. Other works giving various views of SE are [15–19].

### 1.5.2 Matters of Size

The final topic for this chapter is that of "how much is enough" when executing SE and T&E practices in a project.

Overhead costs of a support process are hard to justify when the results of that process are of an abstract nature, cover long-term issues, and appear to not produce easily measured value-adding components to a project.

SE and T&E activities are often seen as costly luxuries. They are, however, as important as accounting and management in that they also assist early detection and control of design error. Who in their right mind would make a development journey without sound assurances all design work is on track and moving the design forward in the right direction?

The design team leader has to use personal judgment in setting the scale of use when applying these techniques or support mechanisms. A single team comprising a dozen or so staff working in a start-up company will probably not be able to devote the time to writing an SE manual. They might instead simply align with an SE standard. The team leader in that case, however, still needs to apply SE principles as part of routine technical management.

Throughout this book, comment is given as to how to make such sizing judgments. All examples given in the subsequent chapters are usually scaleable to suit the situation.

## 1.6 Summary

This chapter has provided the material needed for developing a holistic thinking attitude for ensuring that design teamwork will integrate into the whole project.

Elements of system thinking and SE have been provided to support this intention. The scope of these topics has been stated along with some basic terms and definitions.

The following chapters of this book use this high-level understanding as background to the explanation of methods and techniques for achieving more successful design over the various stages of the life cycle.

This short introduction has laid down the main points about SE that need to be appreciated by the members and leader of the engineering design team.

## References

[1] Hitchins, D. K., *Putting Systems to Work*, Chichester, West Sussex: Wiley, 1992. Free download version is available from www.hitchins.org/prof, April 2002.

[2] Checkland, P., *Systems Thinking, Systems Practice*, Chichester, West Sussex: Wiley, 1981.

[3] Grady, J. O., *System Engineering Planning and Enterprise Identity*, Boston: CRC Press, 1994.

[4] Boulding, K E, "General Systems Theory—The Skeleton of Science, *Management Science*, Vol. 2, No. 3, 1956.

[5] Checkland, P., and S. Howell, *Information, Systems and Information Systems*, Chichester, West Sussex: Wiley, 1998.

[6] Flood, R. L., and M. C. Jackson, *Creative Problem Solving*, Chichester, West Sussex: Wiley, 1991.

[7] Stevens, R. T., *Operational Test and Evaluation*, FL: Kreiger, 1989.

[8] Crouch, V. H., "Test and Evaluation as an Important Emerging Discipline," *Proc. Australasian Instrumentation and Measurement Conference*, Adelaide, South Australia, April, 1992, pp. 7–17.

[9] Reynolds, M., *Test and Evaluation of Complex Systems*, Chichester, West Sussex: Wiley, 1996.

[10] Blanchard, S. B., and W. J. Fabrycky, *Systems Engineering and Analysis*, (3rd edition), Upper Saddle River, NJ: Prentice-Hall International, Inc., 1998.

[11] Sage, A. G., and W. B. Rouse (eds.), *Handbook of Systems Engineering and Management*, New York: Wiley, 1999.

[12] Ferris, T. L. J., *Systems Engineering Management N, Course Notes 13437*, 2001, Systems Engineering and Evaluation Centre (SEEC), University of South Australia.

[13] INCOSE, 2002. International Council on Systems Engineering, http://www.incose.org, March 2002.

[14] US DoD MIL documents, 2002 http://astimage.daps.dla.mil/quicksearch/.

[15] Faulconbridge, I., and M. Ryan, *Managing Complex Technical Projects: A Systems Engineering Approach*, Norwood, MA: Artech House, 2003.

[16] Buede, D. M, *The Engineering Design of Systems: Models and Methods,* New York: John Wiley, 2000.

[17] Stevens, R. et al., *Systems Engineering: Coping with Complexity*, Prentice Hall PTR, 1998.

[18] Westerman, H. R., *Systems Engineering Principles and Practice,* Norwood, MA: Artech House, 2001.

[19] Hitchens, D. K., *Advanced Systems Thinking in Engineering and Management*, Norwood, MA: Artech House, 2003.

## CHAPTER 2

# Systems Design and Project Management

This chapter moves the level of discussion inward from the holistic limits of consideration, taking the previously given ideas toward practical application of systems thinking in design. It explains:

- The various systems perspectives that engineers could encounter and therefore be able to draw upon for problem solving;
- The problematic differences between SE and project management, showing how their unique and overlapping features are of use in the engineering design team situation;
- How to implement T&E at the higher levels of project management;
- How to implement a design team situation that has a sound amount of SE and PM practices in place.

## 2.1 Systems and SE: Understanding Interpretations

### 2.1.1 Systems from the Hard Science Perspective

Conducting successful systems design requires the combined use of many different methodologies and cultural thinking modes. In this section, we compare several kinds of systems thinking to illustrate the breadth of differences in use of the word "system."

Those trained in electrical engineering generally operate predominantly at the hard end of the span between hard reductionism and soft phenomenological thinking. This discipline regime has developed a widespread attitude that a system should be reduced to a formal mathematical model that is then analyzed to investigate its behavior. This situation probably emerged because many of the pioneering design needs could be based on the physics of material systems such as the apparatus of telegraphy, telephony, and later the electronic amplifier. They developed in concert with the classical physics topics of mechanics, heat, electrochemistry and electromagnetism. The already developed disciplines were able to provide good mathematical models for taming systems understanding of the abstract-like entity, electricity. Some aspects of the nineteenth and early twentieth century developments involved less deterministic effects, such as user audiometry, but generally hard science methods sufficed.

There is a distinct danger of falling into the intellectual belief that all system design needs to fit well within the reductionist methodology, or that a problem must be squeezed into that thinking mold no matter what. Figure 1.10 showed the type of organizations that seek solutions. Engineering education and training, however, does not suit all of them.

Reductionist thinking can serve the designer well where mathematical representation can be developed for a reasonable cost. Where prior causal modeling development has been done, the cost of application can be quite reasonable. For example, the embedded mathematics of simulation tools can be used for circuit investigations without the user needing to be an expert with the math involved. Figure 2.1 shows the schematic diagram of a representative electronic system where hard science can deal with most of the design problems involved.

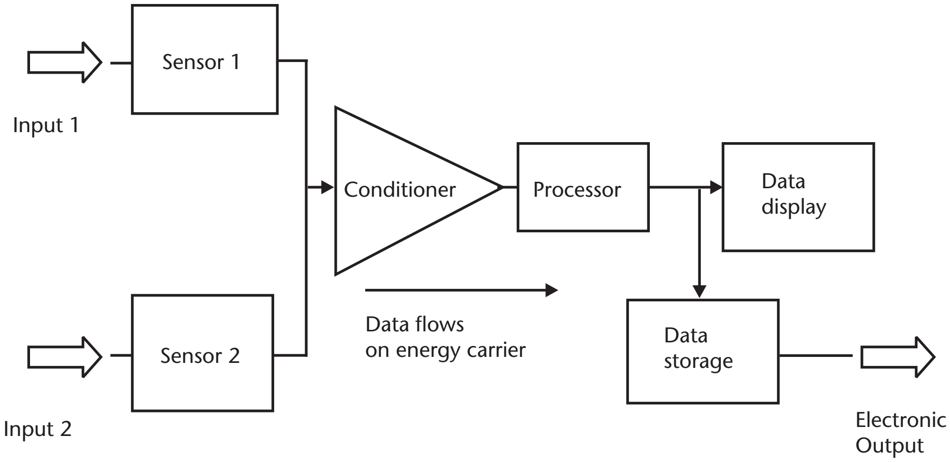
Reductionism will work well if the following sets of conditions each apply to the system being developed:

- Truly a completely closed system;
- Concerned only with energy or mass transfer;
- The mass or energy flows are interacting in some kind of closed system network.

If problems involve any significant element of human thinking within the modeling environment that cannot be described in mathematical models, they rapidly become unsuited to reductionist methods.

Consider the teaming model of SE that is given previously in Figure 1.1. Each design team is a part of a dynamic process in which ever-updated design knowledge is passed around so that the team can alter their design to integrate it into the whole.

Creating a formalized system model of this overall design activity by the reductionist approach suggests that a model can be formed as a network of teams operating within an interconnected network. The optimization goal for model use is to get the right design done to satisfy the faster, cheaper, better drivers.



In electronic block diagram systems representations, the energy supply and earthing lines are omitted by convention. This kind of system contains little human element that needs to be allowed for.

**Figure 2.1** Schematic model of a typical electronic system.

In formalized systems thinking, the solution path is to then identify the characteristics of each block and decide how the connections behave in the network. That results in a formal mathematically describable model. The problem here with human teams, however, is that the stuff flowing in the network is not energy or mass, but cognitive information.

Unfortunately, there are no formal theories available for mapping information, knowledge, and wisdom into satisfactory reductionism representations. To gain an appreciation of the hard methodology in action, simply browse the shelves for electrical engineering, classical control, manufacturing, mechanical design, and electronic engineering.

It needs to be recognized that while tools to consider in design problem solution may well be those based in the hard mathematical methods, they do have limits of applicability in high-level system design situations. Other styles of systems thinking need to be adopted to suit the need at hand.

### 2.1.2 Systems Regimes with a Softer Perspective

The electrical engineering (EE) thinking mode has been singled out as the engineering thinking that has been able to usefully take formal representation a long way. However, not all of engineering design succumbs to formal description, especially in nonlinear situations, or where people form part of the system.

In hydraulic engineering, for instance, pragmatic methods have been found to be necessary using fudge factors, rules of thumb, coefficients, or constants (or whatever term you like) that are only applicable in well-defined closed system situations. For example, calculation of the Reynolds number for a given fluid flow will show whether the flow is laminar or turbulent. In control engineering, it is the closeness of dynamic behavior curves to a defined point on a mathematical model plane that enables the designer to gauge the degree of stability of the closed loop feedback system.

Some disciplines need to use a soft approach at times. Take civil engineering for example. Reductionist techniques can be used most effectively to design and optimize the complex stress-strain relationships existing in a frame structure for a building, or the bending and shear forces for a concrete bridge. At the other extreme of the systems-thinking spectrum, the civil engineer is also deeply concerned with aspects of project management (further studied in Section 2.4). Figure 2.2 illustrates some of the many aspects of a design need that a civil engineering designer might need to manage.

Civil engineering design projects also often impact deeply with societal and environmental issues (see Figure 1.6) and may have architects and others involved as the experts on the fine arts, use, living, environmental, and amenities parameters. Systems problems of this type and extent cannot be easily separated out from the real world in order to set up the totally closed design environment needed for reductionism approaches to properly function.

Civil, environmental, transportation, and production engineering all have a large degree of phenomenological thinking explained in their texts and reference works. Titles are deceptive—the word system has acquired numerous interpretations over time. Civil engineering texts on project management are representative of the broader systems thinking needed in engineering applications.

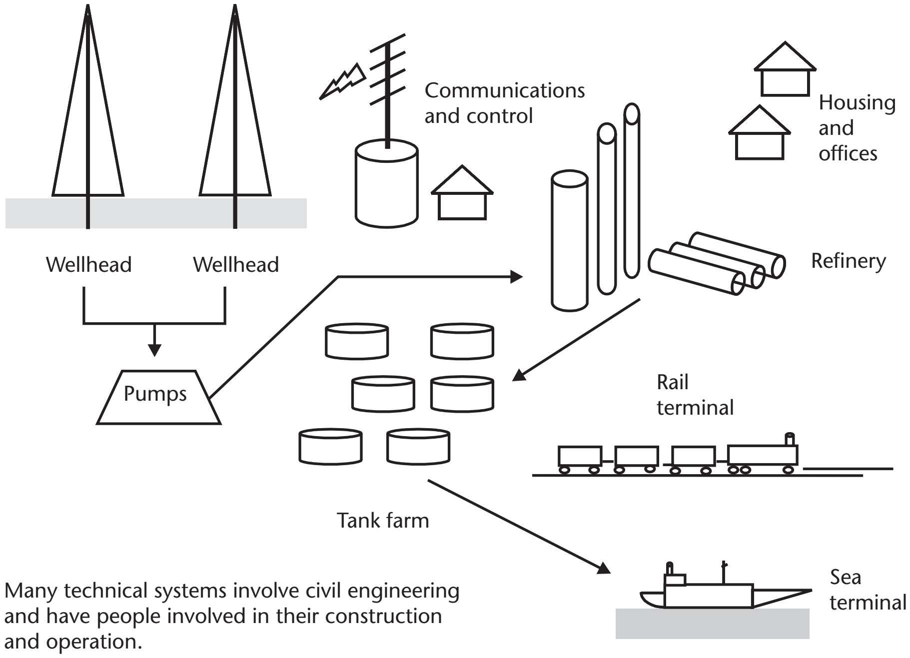


**Figure 2.2** Model of an engineering system involving construction.

Many discipline specialties assert that they cover systems. Their texts and standards documents will list often identical terms, giving the impression that "systems" are covered in the same way across the board.

Differences are seen as the degree of attention given to the respective issues. A single 1-hour lecture is all students get on requirement management in one manufacturing systems course, whereas a systems engineering course would devote many lectures to the topic.

### 2.1.3 SE Perspective

By now, systems thinking is becoming clearer with respect to its place in an engineering design project. We can now move on to discuss its application by engineering within the so-called SE.

SE is concerned with applying adequate breadth of ideas and methods in the search for finding the right solutions to engineering design needs. It is about being systematic and rigorous in finding, assessing, and applying the ideas. The following chapters of this book introduce many SE techniques, showing how they can be applied to design activity.

The problem of being a systems engineer for a project is well summarized by a simple but profound quote paraphrased from Bronowski's series, the *Ascent of Man* [1]: "A core requirement in design is not so much what to know about things; but which things to know about."

Once an engineering problem has been identified, it will usually not be too difficult to locate an expert who can handle it. This implies that the systems engineering role requires an engineer who has extended competency from the basic degree education. This is not a new finding. The cartoon in Figure 2.3 [2] emphasizes this point well.

It is necessary to be in tune with the optimization of CTP variables at all times (see Section 1.1.4). Will the design problem solution about to be used lead to improvement of any one of those variables, or will it actually result in negative added value?

One needs to be cognizant of expected conflicting relationships as a design variable is optimized. These are:

- To reduce cost at constant risk, performance must usually be reduced;
- To reduce risk at constant cost, performance must usually be reduced;
- To reduce cost at constant performance, higher risks must usually be accepted;
- To reduce risk at constant performance, higher costs must usually be accepted.

Regardless of one's own area of engineering experience, it is likely that without exposure to systems thinking, the thinking applied will not be broad enough. It is easy to be constrained in a tight cultural way of thinking for that appears to carry the least risk. We work within the belief system(s) in which we have been immersed all our lives.

Other people impacting on the design team will not necessary understand the relevance of need for knowledge from the softer sciences found in the humanities, or that a "good enough for the time being" method is actually an optimal way to approach some design problem needs.

At times criticism, even ridicule, will have to be endured. Try telling the senior project manager for an electronic system development that the services of an anthropologist are needed to sort out some technosocietal problems aspects of the

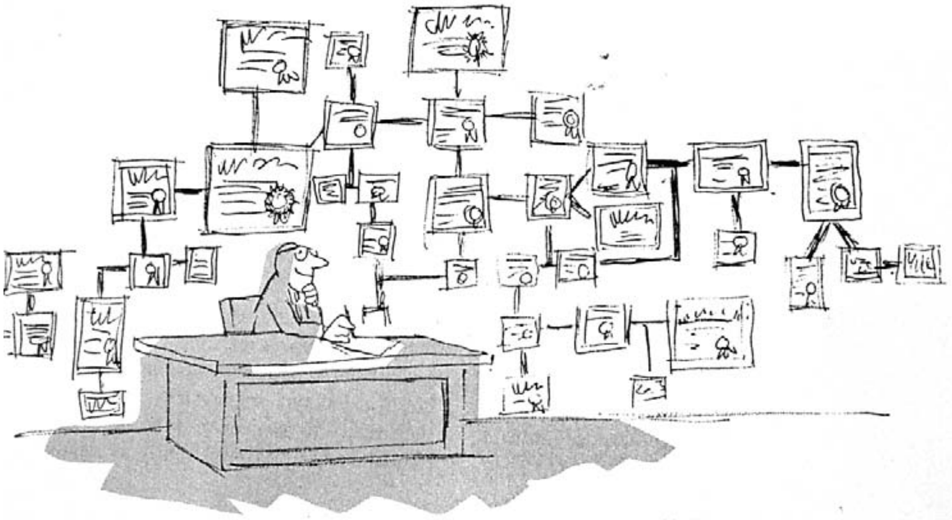


**Figure 2.3** A systems engineer is a good engineer—only more so. (*Original source*: *International Science and Technology,* November 1964, republished in [2].)

design team performance; that a grammaticist is needed to shed light on some human communications problems; or that a theologian could help with the philosophical issues being faced at some stage of a design. The reaction by engineers is highly predictable!

Hence, the problem of being a systems engineer is very much one of having the ability to be a good specialist at being a good generalist, which usually means being more broadly educated in the ways of problem comprehension and solving.

The SE situation is represented by the degree of breadth versus the degree of depth that a task requires. The so-called T diagram, Figure 2.4, is used to portray this metaphor.

Listing the main areas needed and how the SE person uses them in the various stages of the SE life cycle, Figure 2.5 yields another portrayal [3].

Where does one go to obtain this breadth of knowledge? What actions might be needed to support the designers? These issues are now explored.

Libraries supporting engineering design groups usually do not have well-developed holdings on the various systems disciplines. The word "system" in the title is a very generally applied word. Many are actually books about the deeper engineering design detail and contain little on real systems thinking.

There are literally hundreds of books published on systems in all of its manifestations. Unfortunately they are classified in library catalogs spanning many call numbers. Browsing across a shelf with a single call number is not exhaustive enough. It is necessary to know the key words to use and to make good use of the library search system.

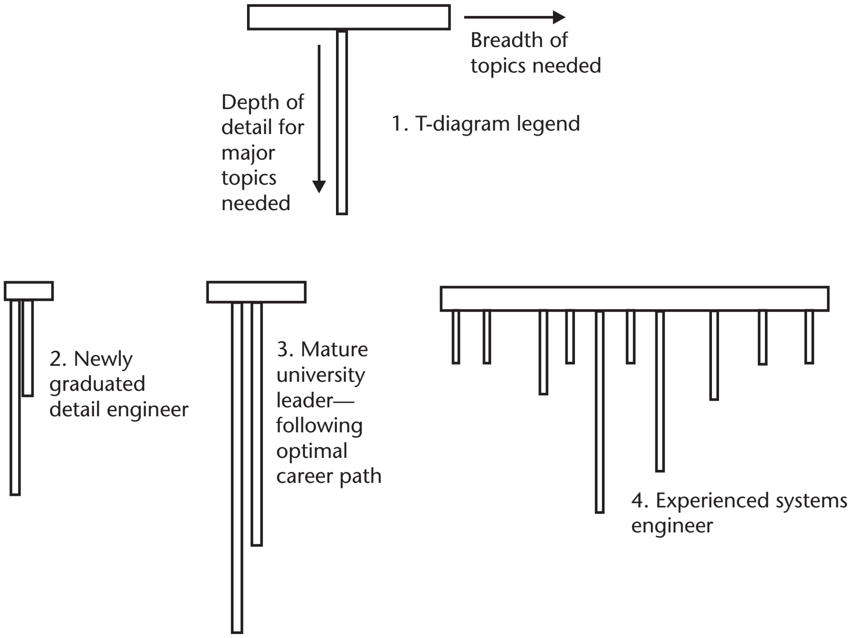


**Figure 2.4** Breadth versus depth of knowledge in different roles and stages of staff development.

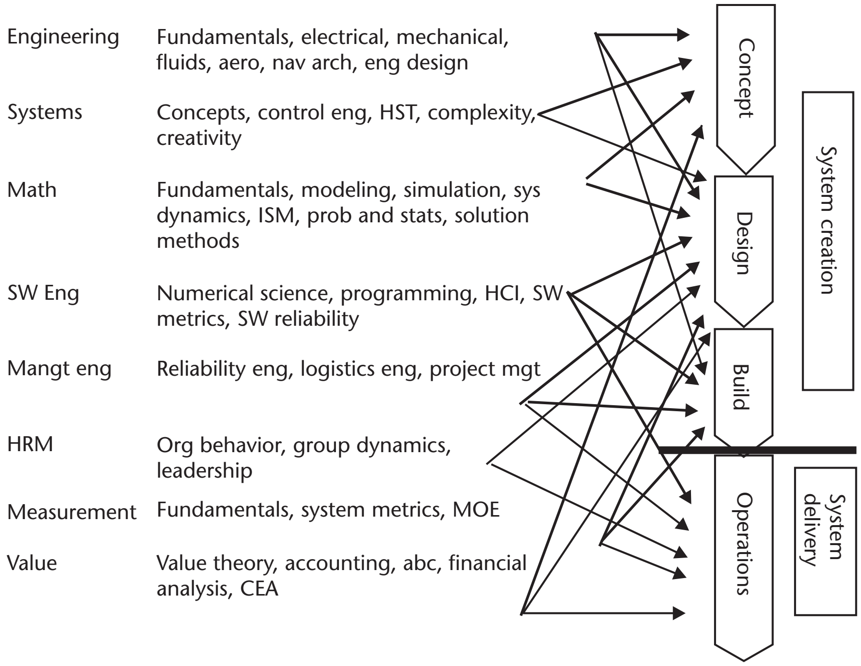


**Figure 2.5** Mapping the disciplines used onto the SE life cycle shows the difficulty faced in obtaining the breadth needed to be a systems engineer. (*Source*: [3].)

Books closely related to the kind of SE dealt with here possibly exceed one hundred. No bibliographies seem to have been freely published that lists and divides them into themes or disciplines of application.

The team needs to have references on hand that cover the nature of systems engineering and systems thinking as their main topics to be able to rapidly compare descriptions of similar topics of SE (see, for example [4–7]).

## 2.2 Overview of PM

### 2.2.1 Principles of PM

Within the management discipline as a whole there are several layers and types of activity.

Corporate management has a viewpoint from the overall operation of a corporation. It will not usually directly address detailed understanding of technical processes and technology itself. These managers steer the group of companies and are the organizers of major reengineering exercises, cultural change, and overall organizational support. Knowledge of a technical nature rises up to this level via the various project or program managers. There exists a well-entrenched tradition that a master of business administration (MBA) postgraduate education provides the management needed to cope with technical operations. That is often a wrong assumption for most such degrees are directed to corporate problems, not at engineering operations.

Below the corporate management level there exist other types of management. The general purpose kind has been variously labeled traditional, routine, or as is used here, conventional management. This type is not to be confused with project management.

Inside the boundary of all projects there always exists a level of human organizational skill concerned with the general kind of management, that of the office, staff matters, personal activity, records, and so forth [8]. The design team manager needs to have awareness of these general management principles and practices, for they can lead to efficiencies in operation of the office-type operations of the design team. By itself, general management is not sufficient.

An often-heard statement is that SE is simply another name for the older established role of project management. Indeed, they do have similarities in part; they are discussed in Section 2.4.2.

A project is formed as a number of complex activities carried out to a plan in order to reach the required system performance outcome, on time and within cost. It usually has definite start and end points. It requires skills in time and task management of the personnel involved in executing the project's intentions.

Project management is the management type to choose for dealing with such issues as producing deliverables according to the prevailing drivers. It is about setting up and tracking progress being made in project tasks assigned to people. It is less about deciding and supporting the best technical design path and choices available for creating the right paths and activities to be undertaken.

Where a precedent product or system project exists, the situation for design is largely repeating design one but with minor changes. Few technical engineering design decisions need to be made in such cases. It is a rerun. PM is sufficient here to allocate and track the staff activity tasks.

Figure 2.6 shows a model of the activities [9] and their interplay for the management of a project.

A study of PM statements [9] led to the conclusion that PM involves the following operations:

- Identifying;
- Planning;
- Organizing;
- Monitoring;
- Communicating;
- Deciding.

Each of these can be broken down into more specific task functions that can be allocated to specialist design teams. Note the similarity with the list of processes given in Section 1.1.3.

We now have reached the point where differences between project management and conventional management can be appreciated [10]. A project has several key properties that are not needed to the same extent in conventional management. These are:

- *Uniqueness*. Each project is a one-off with its own design problems.

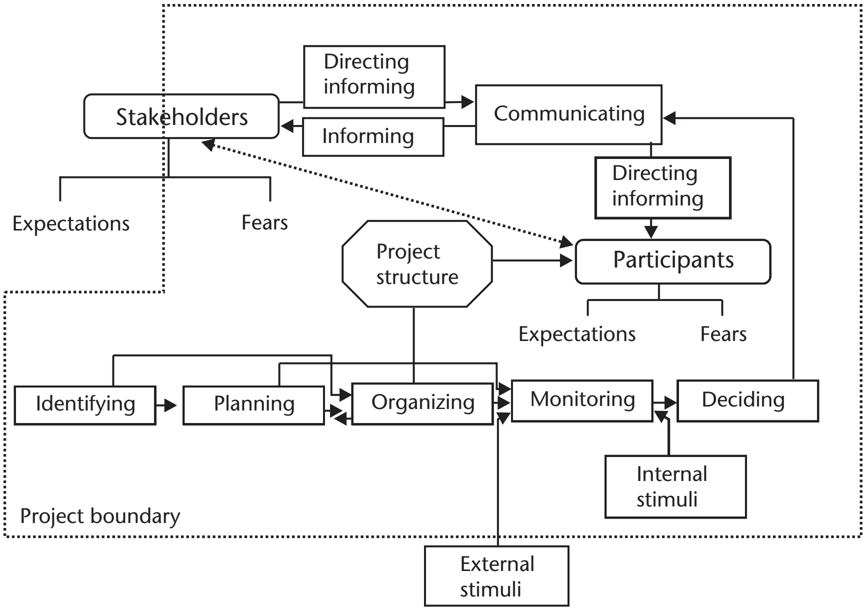


**Figure 2.6** One interpretation of the functional view of PM. (*Source:* [9].)

- *Finiteness.* The project must eventually end. It cannot be allowed to drift on toward a never-reached conclusion.
- *Interdisciplinary and transdisciplinary needs.* Designs benefit greatly from the use of ideas from numerous disciplines, not just from traditional engineering, hard sciences, and management.
- *Complexity.* Complexity, as used here, is more about the way that large numbers of factors interact than about the sheer number of interactions involved.
- *Dynamic behavior.* "Never a dull moment" sums it up. The innovative nature of a project constantly requires new solutions for new situations, along with their resultant risks.
- *Low inheritance.* Past methods may be used again but they need serious review of their applicability. Relevant inherited knowledge should carry over from former similar projects that presumably were well documented.

The planning aspect is important; it will involve:

- *Creation of plans.* These are made well ahead of time and modified to suit as time proceeds. They are widely available so that the design teams work to the some plan. Development is aided by wise involvement of those knowledgeable about the activities of later stages.
- *Forecasting and risk mitigation.* Projects rarely are able to fully meet their plans. Look-ahead activities are needed at all times to try to predict and head off problems. All managers seek a good crystal ball and know that the much-heralded "silver bullet" solution does not exist.
- *Establishing objectives.* Usually, a project has one, or at least some, customers. As they learn from the progress made, their needs tend to change. This requires careful and attentive management, as an innovative project topic is a

learning experience for many. It is imperative to watch out for instances where the organization is not working at the "best practice" and thus may not know about many already well-developed processes, techniques, and tools. A good project group establishes its capability baseline before it implements major change (see Section 12.1).

Programming and scheduling is another aspect that involves:

- *Setting up sequences of operations.* Starting from the needs statements for the project, the overall task has to be broken down to the point where the design teams can start on their own clear technical requirements. This is but one of many operational activities.
- *Replanning.* With all the best intentions, even the best-planned project will all too often fail to be able to follow its original plans. There are too many chaotic uncontrollable elements in complex projects for this not to happen. Replanning is an optional path to consider instead of pouring resources into a failing existing task that is not maturing on time.
- *Management of conflict and competing factors.* Open market competition of modern engineering has slimmed down operations to be very efficient. This means increased interteam and intrateam situations will be competing for ever scarcer resources. Conflict management, conflict resolution, and trade-off studies are able to put some degree of scientific quantitative rigor into this important issue, but generally it is more a matter of political and sociotechnical problem solving that requires skills not usually well developed in engineering designers.

The project manager is responsible for budgeting and for cost maintenance and reduction. This involves:

- *Management of different kinds of resources.* Resources come in many forms—personnel, machines, money, knowledge, tools, opportunities, and more. These all need different levels of attention at various times in a project. Their timely procurement and application must never be overlooked, as these are the elements important to successful design.
- *Assisting development of cost control policies.* Policies are considered statements expressing how to handle repetitive issues. They can be set up for all concerned to follow without need for reference to any senior staff member.
- *Setting up procedures for resource allocation and control.* While accountants can provide their skills, experience, and tools for assisting cost management, they are not trained to know the technical needs of PM or SE. Many would assert they exist to service the PM's needs. As they sign the checks and thus possess overriding control, they often assume control of situations not suited to their experience.
- *Develop organizational structures.* Usually, some standard organizational structures exist that have evolved to suit the industry in question.

Modifications of the standard structure may be needed to suit a particular project. On occasion, corporate management decides that the current state of its best practice can be improved in a major way. A fine example was the Boeing Corp. creation of a design integration center in Seattle, Washington. Many widely dispersed development laboratories were colocated into one massive purpose-built building. This facilitated successful implementation of concurrent engineering and integrated product and process development (IPPD) practices.

At the design team level, the majority of the organizational structure behavior will be imposed on the team. Some flexibility is usually available within the team structure, but changes need to be agreed on with the overall line manager, who can best judge the impact of changes on the whole organization. Section 3.5 discusses the common structures used.

Such imposts may not exist when the design team and enterprise are relatively small; in these cases, the team leader must choose an organizational structure to suit the situation to hand.

Some examples of the flexibility available are found in multiskilled staff, matrix operations, virtual presence, and the adoption of strict top-level leadership overview versus delegated responsibility.

A commonly adopted project structure today is the IPPD methodology. Figure 2.7 illustrates the activities needed at the definition, development, and deployment stages.

One key reason for tuning organizational structures is to facilitate effective communication. This is not only engendered by structure but also by staff relationships. While there does need to be a well-established line of authority (and with that goes responsibility), just how imposing this is a matter of leadership style. Some activities cannot avoid the imposition of formal rigor. Examples are annual staff

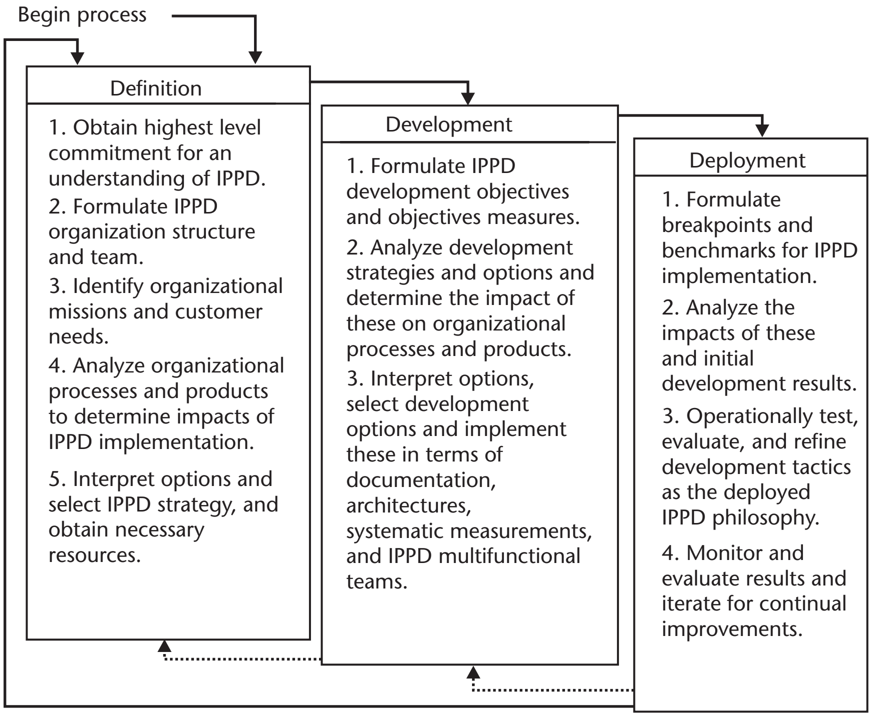


**Figure 2.7** A simplified process to implement IPPD. (*Source*: [7].)

appraisals, career progression issues, performance measurement, salary negotiations, and responsibility for such things as signing off designs.

Finally, in this brief overview of PM there is the matter of performance evaluation. For a project to meet its driver targets there is need for measures (also called metrics) to be set up and monitored. PM needs to oversee their development and maturity. Performance measures apply to many facets, as is later explained in Section 2.5.

## 2.3 Overview of SE

### 2.3.1 Principles and Practice of SE

Having given an outline of PM, we now need an overview of SE. Previous sections have outlined a top-level viewpoint of SE, showing how it stems from the more general systems thinking and how it is differently interpreted across the engineering design regime. Here is given the lower-level explanation wherein the specific tasks are outlined by mapping them onto the product or service life-cycle stages that were identified earlier in Figure 1.2. The emphasis of this account is on design team activity as needed in the stages of the life cycle.

#### Concept formation stage

At the concept formation stage, candidate solution schemas are developed. Tasks are to:

- Identify and record the client's need, which is often different from knowing if there is a technical solution, or even what is needed to provide the solution.
- Identify key influencing and limiting parameters such as political and environmental issue to move toward defining the system's design boundaries.
- Begin PM, SE, T&E, and other key plans as deemed necessary.
- Begin development of requirements, knowing that this is a most difficult and time-changing matter (see Chapter 6).
- Set up and run high-level models of the concept (see Chapter 11).
- Identify the type of system in its various aspects, such as organizational hierarchy, and the degree of soft versus hard activity involved.
- Set up integrated process teams.
- Sort out likely resource needs of the project and begin procurement planning for long-term issues such as staffing and finance. It can take many months to find and place key staff into position (see Section 3.6 onward).
- Create a concept of operations and its documentation (see Section 6.4).
- Conduct concept design reviews (see Section 8.6).
- Create the documentation process for moving knowledge on to later stages.
- Down-select two to four candidate designs for feasibility studies. Going with only one concept is not recommended at this early stage of a project.

### Feasibility Assessment Stage

At the feasibility assessment stage, tasks are to:

- Assess requirements at the operational and now technical level.
- Carry out system architecting that leads to various system breakdown structures.
- Use functional decomposition to identify design and execution tasks down to the design team level of need. Take care to ensure decompositions can be integrated later to obtain the performance needed (see Section 5.5).
- Identify SE and PM roles and needs.
- Evaluate the candidate designs using trades studies, models and simulations, and other comparative evaluation methods (see Chapter 7).
- Continue development of key SE and PM plans.
- Begin suitability and operability studies of the candidate designs (see Chapter 9). These issues were not attended to that well in the past, but now whole of life planning is in vogue.
- Conduct feasibility reviews to establish whether the candidates measure up when some realistic detail is added to the concept.
- Conduct syntheses and analyses that lead to effective generation and evaluation of quantitatively predicted performance, cost, and time metrics.
- Set up the critical issues needed for T&E planning and organize the method for tracking their maturity. Technical performance measures (TPMs) are a popular (but potentially flawed) metric method (see Section 2.5).
- Down-select, using a goodly degree of rigor, one to three candidate concepts to go on to the detailing stage. How to choose the best concept is covered in Chapter 7.

### Detailed Design Stage

At the detailed design stage, tasks and steps are detailed below:

- Carry on previous studies, but now with a greater number of teams being involved in carrying out the detailing work of selected and reticulating designs to the level needed for them to create the detail needed for manufacturing.
- Watch for the semantic difference in interpretations of requirements. Design teams work to design their subsystem to meet the technical requirements given to them from the requirements management process.
- Design team leaders act as the team's interface to other design teams, ensuring the right information flows with the least error.
- Review designs against checklists including technical performance parameters and other critical issues.
- System design is set up in a support tool system using enterprise-approved tools and internally available tool suites (see Chapters 4 and 11).
- Models and simulations are now integrated with others to form their higher-level combination.

- Documentation control and configuration management tasks are put into place (see Section 9.7).
- As it is generated, deliver required design detail to the manufacturing stage personnel for their comment and later use.

### Manufacturing Stage

At the manufacturing stage, tasks and steps are as follows:

- The design team's role is now largely over—if all has gone well. They are usually still involved in assisting interpretation, for tuning design details, and conducting changes that appear as the strictness of final reality emerges. This is really too late a time to modify designs but there may well be good reasons for changes. In general, regard rework as negative value adding. Errors are best trapped earlier in the previous stages if at all possible.
- Prepare documentation and operational detail in support of training and operator use.

### Use Stage

If all has gone well, design teams are now quite far way from the project and have moved onto another one. They have no large tasks to perform; their part is done.

Designers need to be aware of what goes on in the use stage of a system because that can impact on their design. They will need to have representation at field trials and in the use stage team, as this is where necessary design changes can be uncovered and where "lessons to be learned" are witnessed that should be passed on. Too often, however, the design team has been disbanded by this stage and little is passed back for future learning.

Placing resource emphasis into the front-end stages (front-end loading or FEL) increases early error detection and trapping. This is usually agreed to be the right way to go, but as it uses more resources with little visible results, the reality is that too many projects do not get sufficient resources to get them up and running well. The consequence is often that major problems run on until they are noticed at a stage where they are very expensive or even impossible to rectify.

IPPD working reduces the defects rate at the first prototype test. In large, low-volume products such as aircraft, it used to be common practice for the prototype to not go into service. The modern approach—the "no surprises" one—is that prototype test runs are carried out to identify whether there are few defects. Ideally, these tests are used to confirm that the design is as expected. When performance is confirmed, the prototype goes into service. This is in sharp contrast with former attitudes, where the prototype was the first practical test of the full system, run to find what emerged from design.

### Upgrade Stage

This stage is a rerun of the former processes. It is usually regarded as a new project in its own right. The original design team will be long gone. Good records from the first development can assist inheritance of design issues, but generally designers are in a restart project situation with different needs and available technologies.

The apparent simplicity of adding extra functionality usually does not materialize. There is hope in some circles that deployment of the incremental acquisition SE life cycle will help alleviate the need for complete restarts, but this flies in the face of ever-present, rapidly changing customer needs and technology.

#### Disposal Stage

Unless there is heightened interest, the design needs of this stage tend to be much neglected. By this stage, ownership of the system has probably changed hands many times and considerable time has passed. In some sectors, for instance automobiles, legal requirements exist regarding disposal of worn-out systems. The original design team would need to have these long-term needs in mind as they execute the original design. Some industries, such as nuclear facilities, have serious and difficult disposal needs. They need to be addressed all through the life cycle, starting at concept generation.

### 2.3.2 Hardware and Software Domains

All systems developments will have varying degrees of hardware and software in the design solution. Hardware manifests itself as the mass/energy component of the tangible physical aspects.

Software, however, is developed in the IT information domain, where reductionist thinking rarely is that effective. In general, engineers think and act as reductionists and software people make use of thinking somewhere between hard to soft attitudes.

Some projects themselves are almost solely about software in their design activity, but even there the software will be working with existing hardware for which its behavior must be understood. Software design should never be carried out in isolation of the hardware, for the hardware places bounds on the system's performance characteristics.

It is widely observed that hardware and software aspects are not always given due attention as a codesign activity, with the result that system failures occur. A major space rocket once failed its first flight because the software was being reused without recognition of the fact that a critical control flap design had been changed. Examples such as this are all too easy to find.

Part of the problem is that people tend to prefer one or the other of these two aspects. They each seem to suit a different type of person. Computer system engineering courses may well give good coverage to both aspects yet most students will gravitate to the keyboard programming topics.

Another issue here is the apparent ease of modifying software compared with hardware. This is a fallacy when a holistic viewpoint is applied. Knowing that hardware is not as easy to alter as software, there is likely higher emphasis given to getting the hardware right early in the design cycle. Software, on the other hand, has so much flexibility available that is appears anything can be done with it to make it work. The fact is that a design change in software can be a nightmare. Each single binary bit change may have to be worked through the entire environment to assess its impact on the systems operation. Regression analysis and change control are major activities in projects with extensive amounts of software.

The design team leader must be constantly on the watch for sound integration of hardware and software in a project.

## 2.4 Comparison of the Roles of PM and SE

### 2.4.1 Bodies of Knowledge: PMBOK and SEBOK

The Project Management Institute (PMI) has developed what it calls its project management body of knowledge (PMBOK).

While a BOK seems to be a sound concept, just what to include is a matter of debate—and BOKs are a relatively new concept.

INCOSE is developing a BOK for SE, called SEBOK. The International Standards Organization (ISO) is also developing one for SE.

One way to define the content of a BOK is to set up a list of competencies needed by workers in the field of interest. Competencies are brief one-liners of a definable activity that can be taught, learned, and assessed. An example in the SE regime is, "Explain how integrated logistics support and logistics support analysis are applied within the systems engineering process by the integrated product and process development team." Some competencies require lengthy training, others a mere hour or so. One either can or cannot carry out a competency. Performing the activity of a competency often requires special knowledge in its execution.

A study of the sets of competencies for SE and PM has found considerable overlap in their listings [9].

Such lists are useful to a design team because they provide checklists of things that might need to be done. They also provide a yardstick for setting up staff appraisals and staff hiring and selection (see Chapter 3).

### 2.4.2 Relationship between PM and SE in a Project

It is the degree of technical know-how and how it is used that distinguishes between SE and PM. Recall that PM is about time control and that it does not deal with the numerous technical functions that form the body of knowledge of SE. Competencies are rarely found to be unique to one or the other of these two. Some 30% are PM led with some 20% being SE led [9]. The rest are common to both.

SE is predominant in the areas of organizing definition and creation of the product, and in enhancement of the outcome. It will be involved in almost all processes, the exceptions sometimes being seen to be in contract matters, negotiation, and detailed administration, in value analysis, and in budgeting of resources. PM is at the fore for planning and organizing the project, monitoring progress, and making key decisions.

So the general differences are not so dominant. Debate continues about ownership of these territorial duties in a project.

The situation of the design team leader is clear. Both PM and SE are valuable and provide idea-packed sources for assisting a design team to be effective.

## 2.5 Role of Quality and T&E in Systems Development

### 2.5.1 Role of Quality in Engineering Design

Quality has always been a strong driver in design so it is covered in more detail in Chapter 9. For now, in this discussion of holistic considerations, it needs to be stressed that the term quality has many interpretations. In the holistic design space this is a key factor that needs to be put into its various perspectives as design is executed.

One common and generally accepted definition is that quality is about the developed system being "fit for purpose." This has two aspects: that of being suitable for its task in the operational sense, and that the design results in a system that has the level of "esteem" associated with it as is expected.

One strong quality improvement initiative has been that of raising the design performance (and other roles) of a developmental or service-offering enterprise. Published standards on quality, such as the ISO 9000 series, give guidelines on how to ensure that quality operations exist in an organization. They also facilitate independent audits that can be provided as third-party assessments.

It is often overlooked that an organization with a good quality ranking has certainly matured its own methods to a known quality level, but that capability alone does not necessarily indicate they will be able to convert an idea into the product or service required. Simply stated, they may well be able to make the best widgets available but they fail to satisfy a need if they make the wrong thing.

Another related strong following exists for what has been termed the Capability Maturity Model or CMM (© Software Productivity Consortium). These evaluations are used to baseline, improve, and certify that a supplier organization is capable and mature in its sphere of activity to a stated level of accomplishment.

This practice is useful for improving the capability of an organization. However, the quality movement is still incomplete. For truly best practice to be in place, the activities of all three of the principal groups involved in a systems development—customer, supplier, and user—need to follow the same maturity self-audit and self-improvement path as the contractor/supplier group is now expected to adopt.

At present only the supplier group makes use of the CMM concept. The customer and user groups do not have to carry the same level of responsibility for best practice in their own roles. A poorly developed client can be a real stumbling block as it may not be skilled or knowledgeable enough about their need to be able to give sound instructions and advice.

As overall project performance relies heavily on all three being simultaneously and continuously excellent, it seems reasonable to expect, at least in large projects, that all three parties be subject to maturity development processes. As this is not the case, the engineering designer has to live with a less-than-perfect situation.

Another interpretation of quality is the general appreciation of it in a mass-produced items context. This is in the domain of the quality control department who apply statistical methods in order to sample output for final inspection purposes. In this situation, it is common for this inspection operation to be a stand-alone check stage for which results are not always fed back to the design team.

The operational suitability aspect of a project is most important (see Chapter 9). A system that does not perform as required is far less tolerated today than in previous times. Major designs that fail to satisfy all of their required regimes are, however, still commonly encountered.

The various interpretations of quality all need to be considered in design activity. In the medium to large enterprise there will almost certainly be quality directives and support for improvement and audit. Maintaining and proving that one is capable of quality performance is an expensive overhead. Decisions need to be made as to the financial benefit of obtaining quality certification and to what level it is to be taken.

The design team needs to be familiar, if not expert, with the various quality issues, for they introduce requirements that restrict design freedom. In addition, most important, obtaining quality in design has it roots in the concept, feasibility, and detail design stages. It becomes increasingly more expensive to add after those stages.

### 2.5.2 T&E in Systems Development

As they are always set up as a matter of normal practice, it is reasonable to assume that the cost and time management processes will be in place for a project. Management of performance control, however, is often left to the design engineers to implement on an ad hoc informal basis (see Section 1.4 for an overview of T&E practices).

It is now appropriate to discuss how performance maturity and system appropriateness might better be executed at the holistic level.

Three main planning needs of a successful T&E program are:

1. Ensuring that scarce test resources efficiently address the project's critical issues. Every possible system parameter cannot be tested; there are far too many of them.
2. Ensuring that those who need to know can observe how well the critical issues are maturing according to well-thought-through expectations.
3. Providing information on the plan and its maturity to all who need to know about these issues. For example, those who plan the use of test resources need considerable lead time for organizing availability of test objects, observers, test equipment, test suite programming, and so forth.

Figure 2.8 shows the main stages and activities that the author considers [11] necessary to set up a performance maturity management system for a project.

Working through the steps of Figure 2.8:

1. A relational database is set up for tracking the target and current value, and the estimated uncertainty, for all of the system's critical issues (CIs).

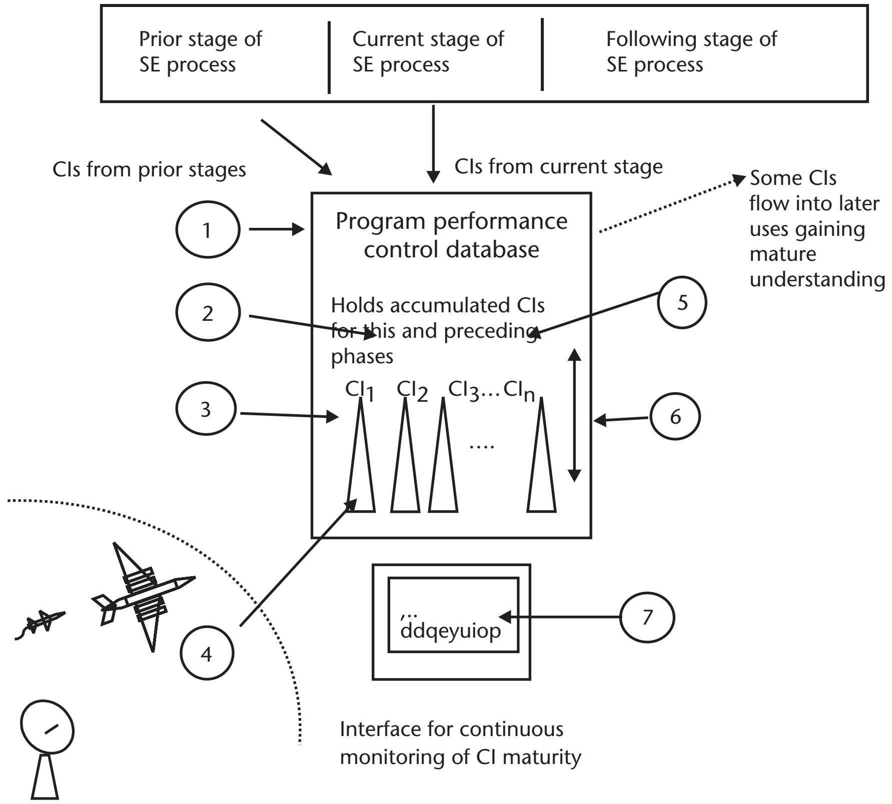


**Figure 2.8** Setting up a T&E performance maturity management system for a project.

(Unfortunately, as is the case for many terms used in SE, the term "critical issue" is also used to indicate something that needs to be resolved/defined in requirements management to complete a set of requirements. Here it is used in the context of the T&E of systems, as defined in U.S. DoD documents.)

2. CIs, often called show stoppers, are identified from project documents and investigation within the four specific classes of project regime. The CIs are found by asking what show-stopping issues will arise as the bracketed questions below are asked. The four classes of CI are as follows:

   - *Operational requirement*. (What is the system intended to do?)
   - *Suitability for purpose*. (Will it perform where and when it is needed, and continue to do so?)
   - *Political and environmental needs*. (What nontechnical impacting issues exist that influence matters of design?)
   - *Program execution regimes*. (Will the way the project is organized facilitate efficient development all through its life?)

   Generated CIs are each assigned initial present-time values along with their crudely estimated uncertainty levels.

3. Create the many "measures trees" that result from breaking down each CI into successive layers of different types of measures as shown in Figure 2.9.

It is important to remember that to obtain traceable "truth" for the maturity assessment process, the CIs must trace down and then back up from the measured TPP data. It is only the TPP data that is obtained by strictly performed scientific investigations—the physical tests. All other measures will be subjective if they are not founded on a base of scientifically conducted measurement data and thus can be problematic and less reliable indicators. Mapping the levels upward gradually introduces increasing uncertainty.

4. Obtain TPP data. By applying the sound method of scientific investigation of the selected tests, it is then possible to generate CIs values (see Section 11.6). Data to populate the various measures trees can also be obtained from prior tests as long as the test through which it was produced was for the same set of conditions and equipment under test. Note that an individual TPP test can often be used to feed other TPP parameters in the set of measures trees.
5. Set up calculations for converting TPP data into the stated CIs. These are used to form management system maturity indicators. Other performance parameters may be needed that are generated from appropriate combination of various measures trees data points. These are traditionally called technical performance measures (TPMs). However, in many cases generation of TPMs is not done traceably upward to defined CIs.
6. As data is obtained, perform automated calculation of all CIs by upward mapping of the various TPP data values into smaller sets, as per the combinational rules set by the tree structure. This will usually require estimated surrogate TPP data to get the system going and to check that it is working satisfactorily.
7. Create a user interface for the performance management system to display and report on the needed CI and TPM parameters. This interface is also used as the tester's data entry medium.

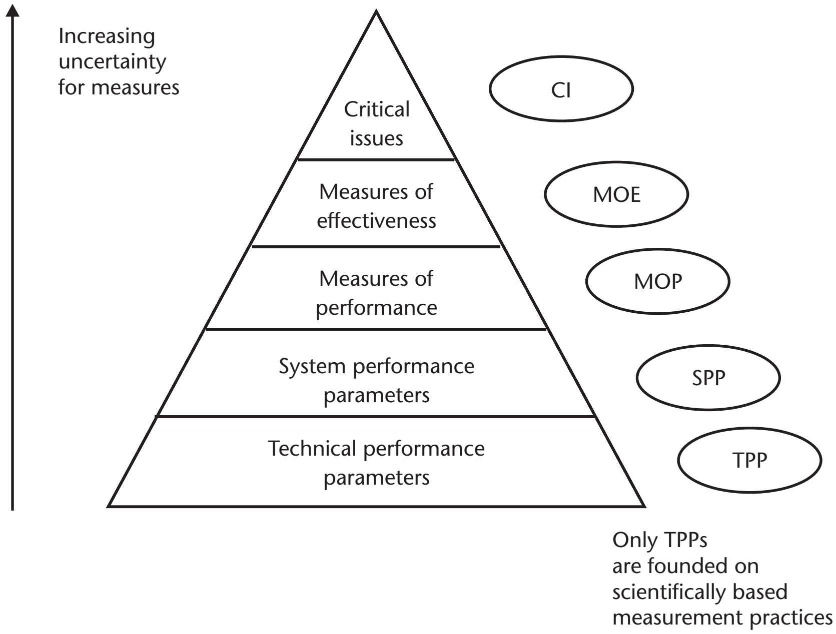


**Figure 2.9** Measures tree layers formed as CIs are converted into TPPs.

As development moves through its stages, the CI determinations should, by tight design control, gradually trend toward the target with their uncertainties reducing to acceptable values by the required time.

With such a system available, the project managers and design team leaders can see how the CIs are maturing toward their goals. Time trend graphs can show the current state of performance maturity compared with the target value. Severe deviations can then be given more attention to bring a particular CI back on track. An openly observable system such as this exposes error early where it can be less expensively corrected.

Openness of trend data also means that the designers are not overly compromised by bad results because the error is occurring early where it is not at a career-threatening magnitude. It is a well-proven fact that the project manager or team leader often keeps severe performance shortcomings hidden in the hope that more time will allow local action to rectify them. Late reporting of problems is a common cause of system failure and one that is hard to detect and manage.

The above performance management methodology addresses the three key T&E questions given in Section 1.4.1. Successful implementation of this process depends on many factors. It should be adopted fully or in part to suit the project size, type, political environment, and cultural attitudes of the organization.

Too often T&E is not allocated the appropriate amount of resources, nor addressed early enough. Not having well-planned T&E in place is a saved cost but only if all goes well! It is akin to taking out insurance, but additionally if done properly, it is a powerful design support tool in its own right.

## 2.6 Integrating the Hard and Soft Aspects of System Design

### 2.6.1 Qualitative Regimes

It has been explained that both hard and soft thinking approaches need to be used in a design. Before progressing, let us explore how you, the reader, view systems with a technological content. Take a brief look at Figure 2.10.

Do you instinctively see the figure as a technological system about which you are already analyzing its usefulness and functionality, how is it constructed, and if the various structural members are adequately strong and well connected?

Perhaps, instead, your first thoughts were about its artistic metaphor, as a vision, or a portrayal of a thing of abstract beauty?

Most design engineers would see it through the eyes of a reductionist. This long-trained, well-ingrained, hard approach often gets in the way of clear thinking about problem solving in design.

Despite the strengths of working in the hard science domain, in engineering design there are times when one can only make progress using the less certain qualitative kinds of thinking. A serious error, however, would be to stick with qualitative methods when powerful quantitative methods exist that will solve design needs very efficiently.

**Figure 2.10** Hard versus soft thinking; a self-assessment test—see Section 2.6.1.

So how does one recognize when soft or hard thinking is needed? Some clues are usually available that will help decide between the two alternatives.

The first clue to identifying which is appropriate is to establish whether the problem to be solved is concerned solely with the behavior of physical matter or energy and can be bounded to give a closed boundary design situation. If so, then the quantitative methods will work well, although it is still necessary to weigh up the effort needed to apply them if little prior work has been done to develop a good starting foundation.

Another clue is to decide whether the problem concerns nonphysical entities—information and knowledge. If this is the case, it is important to separate out the quantitative from the qualitative areas. For example, information theory is about the statistical properties of known messaging quantities arriving intact; it offers little for understanding the properties of the meaningful nature of the information in the message.

A third clue is to assess if a formal model is possible. In many situations it will be apparent that a set of rules of thumb (called heuristics) can lead to solutions for situations where qualitative methods cannot be implemented.

It is an interesting philosophical issue as to whether heuristic-based thinking is actually the first step toward quantitative formal understanding.

The observed fact is that people are able to solve many difficult problems without developing strictly formal mathematical models. It certainly does not seem that the human mind solves problems by setting up formal mathematical equations to obtain solutions.

Heuristics can be a very powerful basis for problem solving. Management uses them all the time. Engineering tends to berate them as not being quantitative enough! Systems engineering uses both.

As the design engineer has to make best use of scarce resources when developing a system, the use of heuristics may well be the most efficient, indeed only, method to use.

Another powerful clue for deciding to go hard or soft is to establish if people are dominant subsystems in the whole system. If so, then assuredly qualitative methods will have to be used in the main. If any significant degree of soft features exist in the design then one can be reasonably certain that formal methods will not work well, despite the appearance to the contrary.

Soft situations can be recognized if the following issues apply:

- Where systems concern cognitive (those pertaining to the human mind) aspects of design development, such as in the early concept stage that involves formative thinking about solutions.
- Always soft for the software program regime, not so much in the coding itself but in the construction of the program architectures.
- Where human activity is involved, such as design team behavior, requirements generation, design innovation, and synthesizing design elements. Less appreciated is the fact that the very roots of hard science about the real world are based on coefficients and heuristics that make the equations fit the uses.
- When resources do not allow formal methods to be developed, such as when insufficient time prevents a fuller degree of solution generation.

### 2.6.2 Quantitative Aspects

The most comfortable design thinking mode for engineers is undoubtedly the hard methodology. It is founded on a tight and rigorous scientific discovery process. Findings are proven from unique sets of facts that apply over the range of circumstances for which the method has been found to apply. Its formal nature is certainly attractive; it has one unique method of representation.

In some fields, such as the highly formalized and very powerful computational fluid dynamics, this methodology has supported great advances in design. In electrical networks, formal methods also work well and they have been usefully extended into the nonlinear, network problems covering hydraulic network behavior.

These successes might well imply only formal methods are respectable. The reality is that they are not always applicable, they can use far too much resources at times, or they cannot be applied for lack of availability of the physical constants and coefficients needed to solve models for specific situations.

There are, in fact, many places in the engineering design process that do not lend themselves to classical linear, or even extended into nonlinear, mathematical description. An obvious area is software development. Formal methods have been tried to support software code development, the hope being to realize designs that can be automatically processed for error detection, correction, and verification. In the main, however, they have not yielded the level of pragmatic usefulness expected. Formal methods have been investigated for measurement systems design, the conclusion being that there are just too many issues that cannot be handled formally.

Modeling of the SE process life cycle has similar difficulties. Trends appear and are followed for a while, but the pragmatic needs of engineering—to obtain the best use of resources and an optimal design—often can find solutions by using soft thinking approaches far faster than can formal methods.

These remarks can only be an indicator. Be aware that trends and conservatism can trap designers into sticking with accepted methods, potentially leading to lack of competitive solutions.

## 2.7 Setting Up SE Activity for a Project

### 2.7.1 Guidelines for Establishing an SE Approach

There is no singularly useful set of recommended rules for using SE methodology to plan a project. The difficulty is that each project is likely to be unique in many ways. The various SE standards, such as EIA-632, can be used by tailoring their listed issues to suit. This section gives some key activities that need to be considered early in the design cycle.

#### Teams and Their Communications

Clearly, the design team has to be established with the right mix of expertise to suit the assigned task (see Chapter 3), and be supported with modern IT (see Chapter 4). This usually has to be as a compromise.

Communication needs must be met by provision of appropriate methods. Figure 2.11 illustrates the two different paths of communication that can take place between two people using design support tool systems as part of their system development. The data path arises when information is transferred using tools such as spreadsheets, requirements management, and office sets. Passing a computer file over to another person may not pass on the message expected. This problem occurs early in the life cycle when requirements begin to be generated. There is a need for carefully controlled terminology lest the message changes, as it does when a simple message is whispered from person to person in the well-known party game.

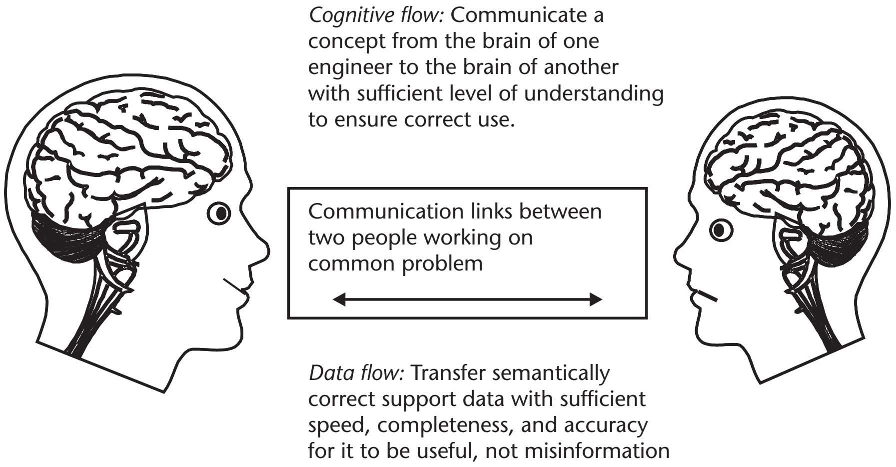


**Figure 2.11** The two essential means by which designers communicate design information have very different properties. (*Courtesy*: D. Harris.)

At the present state of computer-interconnected working, the semantics associated with the cognition of words, images, and sounds are such that these media cannot be guaranteed to pass on design detail with a high certainty of interpretation.

Support tools do lead to greater efficiency, and used carefully can add value to a project. Standards are needed to ensure integration of data at each end of the link. Such standards are emerging but are still in their infancy.

To minimize error of communication, it is recognized that there is a need for considerable face-to-face discussion between those concerned. Virtual operations, wherein groups and individuals work in relative isolation communicating over IT networks, can be used but they have been shown to not adequately replace colocation of staff, especially in very complex design situations (see Section 4.5).

### Familiarity with the Best Practice

A wealth of information exists for obtaining guidance about the "what to do" activities of systems engineering. Far less is published about the "how to do" aspects.

SE standards are essential reference documents to have at hand but they usually have to be purchased from limited sources; sometimes by Web site download with or without charge. The INCOSE Web site (www.incose.org) offers useful documents to members, many free of charge. Essential basic SE documents are:

- EIA 632–1999, which describes the processes for engineering a system [12];
- ISO 15288, which is the latest (as of April 2003) standard to describe life-cycle processes [13];
- MIL-STD-499B, which is a long-standing prescriptive and lengthy document that, while generally considered out of fashion for being waterfall process oriented, is a good source of detail on many of the practices needed [14];
- *Systems Engineering Handbook*, which documents consensus thinking [15];
- Textbooks with practical application of material on the engineering of systems, such as [5];
- Major reference work on systems engineering and management [7] that gives considerable detail of the activities and their scholarly foundation;
- The organization's own proprietary SE process handbook, if one exists;
- Recent overview of perceptions of SE, such as [16];
- MIL STD series of standards [17].

Some of the above material is available from intranets of organizations or from the Internet. Some of the documents used by an organization are seen as valuable company assets and thus are only available to authorized personnel.

### Key Process Studies and Implementation

The following list outlines the main activities that need serious consideration when a project begins:

- Sort out and identify what kind of project is involved in organizational terms.
- Decide the SE life-cycle process type to be used.
- Decide and set an integrated database ready to accept project documents, support tools, support handbooks and procedures, project management, and financial records.
- Develop a concept of operations (ConOps) for the project. This is also known as the operational concept.
- Set up a sound systems engineering management plan (SEMP) that tells what, when, and how the various SE activities will be managed. This is called the through life management plan (TLMP) in U.K. Ministry of Defence (UKMOD) practices.
- Set up the T&E and acceptance master plan. (A suggested better title is project performance maturity assessment plan, or PMAP.) A variation of this is called the integrated test and evaluation and acceptance plan (ITEAP) in the UKMOD.

#### Staffing Issues

Some key staffing issues are:

- Ensure all staff are well trained into, and accept and act within, the ways and culture of the project in order to work toward strong coalition organizational thinking and to work with efficient interfacing lines of communication.
- Look ahead and carry out hiring of appropriate staff (see Sections 3.6 and 3.7).
- Ensure concurrent engineering is being practiced. This is assisted by adopting integrated product and process development (IPPD) methods, and through intercontractor practices such as teaming, where trust and transparency are key factors required between competitive contractors.

This list can go on! How far one goes with implementation and formality depends on the size of the project and the design team leader's level of influence and background on the senior staff responsible for overall SE support. Unfortunately, in many situations one has to live within often-inadequate practices of the larger whole.

## 2.8 Summary

In this chapter, we covered how the ubiquitous system differs in understanding with the discipline concerned, and that each interpretation may be useful to the designer.

The differences between systems engineering and its related discipline of project management were discussed, showing that considerable overlap exists between their respective tasks. This overlap is not important as long as it is recognized that they both offer useful techniques to the engineering designer.

Knowing how well a design development is going requires a clear strategy for testing and evaluating the delivered system not only when it is completed, but as it is being developed. A formal, whole of project, T&E process can provide a vital tool for monitoring maturity of the performance issues of a system as the project passes through its life-cycle stages.

Efficient integration and appropriate use of hard and soft thinking styles is essential for overall management of projects. The wise designer is able to recognize what kind of problem solving metaphor to use and what kind of thinking approach to adopt to implement a sound solution.

To complete the mind-broadening introduction of this book, this chapter ended with a discussion on how to generally implement SE and PM practices.

Using the material presented in this book, we can now begin to deal with specific techniques and practices that can be used to improve the practice of engineering design. It will be seen that the above principles and concepts find use in numerous ways.

## References

[1] Bronowski, J., *The Ascent of Man*, London: British Broadcasting Corporation, 1973.

[2] Bollay, W., "University Projects in Systems Engineering," *Engineering Education*, April 1970, Vol. 60, No. 8, p. 805.

[3] M'Pherson, P., Academic Contributions to Support Systems Engineering, Proceedings of Academic Forum, INCOSE. *Website Record of Academic Forum, Annual Symposium, INCOSE*, www.incose.org, Melbourne, July 2001.

[4] Buede, D. M., *The Engineering Design of Systems*, New York: Wiley, 2000.

[5] Blanchard, S. B., and W. J. Fabrycky, *Systems Engineering and Analysis*, (3rd Edition), Upper Saddle River, NJ: Prentice-Hall International, Inc., 1998.

[6] Hitchins, D.K., *Putting Systems to Work*, Chichester, West Sussex: Wiley, 1992. Free download version available from www.hitchins.org/prof, April, 2002.

[7] Sage, A.G., and W. B. Rouse (eds.), *Handbook of Systems Engineering and Management*, New York: Wiley, 1999..

[8] Heller, R., and T. Hindle, *Essential Manager's Manual*, New York: Dorling Kindersley, 1998.

[9] Bottomley, P., et al., "A Study of the Relationship of Systems Engineering to Project Management," *Proc 4th Systems Engineering Symposium*, INCOSE UK Chapter, Hendon, U.K., June 1–2, 1998, p. 113–124.

[10] Stretton, A. M., "Distinctive Features of Project Management: A Comparison with Conventional Management," *Gen. Trans. IE Aust.*, 1983, p. 15–21.

[11] Sydenham, P. H., "Methodology for Integration of Evaluation Systems in the Engineering of Large Systems," *Proc. 3rd Int. Conf., Measurement 2001*, Smolenice, Slovak Republic, May 14–17, IMEKO, pp. 7–11, 2001.

[12] Electronic Industries Association, *Standard EIA-632. Systems Engineering*, 1999.

[13] ISO, *ISO/IEC 15288 Life Cycle Management—Systems Life Cycle Process,* International Standards Organization, Geneva: 2002.

[14] MIL-STD, *Military Standard MIL-STD-499B-1992 Systems Engineering*, Washington, D.C.: U.S. Dept. of Commerce, 1993.

[15] INCOSE, International Council on Systems Engineering, http://www.incose.org, March 2002.

[16] INCOSE. *Website Record of Academic Forum, Annual Symposium, INCOSE*, www.incose.org, Melbourne, July 2001.

[17] USDoD MIL documents, 2002, http://astimage.daps.dla.mil/quicksearch/.

CHAPTER 3

# Design Team Formation and Staff Selection

Staffing is the most costly and valuable asset used in carrying out effective engineering design. This chapter deals with staffing issues of importance to the design team situation. It explains:

- Why financial issues impact new appointments and why they can take so long;
- Skills needed of a design team and selection of an appropriate team member;
- How a new start gets underway and the kinds of support needed to operate a design team;
- Handling resignations and retirements;
- Organizational structures that the team will meet;
- Staff appointment processes, staff selection, and settling new staff into the team environment;
- Staff development and performance assessment;
- Quality methods likely to impact on staffing activity.

## 3.1 Team Requirements: An Example Start-Up

Having made the case that implementing sound systems engineering depends heavily on the people involved, this chapter explores the staffing aspect of the design team. This is a topic not usually taught to engineers; they sense what to do from experience, which can be a rather protracted way to learn the ropes. Content given here is intended to provide a crash course in staffing matters.

Before we delve into the particular aspects of staffing of an engineering design team, it is appropriate to run through the makeup of a typical situation. While the actual situation varies according to the size of the organization at the design team level, there are close parallels of need. An imaginary case study, for the start-up of a small technical business enterprise, now puts these needs into perspective.

An opportunity has arisen for a large organization to develop and supply instrumentation systems needed to support large-scale hydroponics farming. This involves growing vegetables and fruit in specially built enclosures that do not use soil. All plant nutrients are provided under tight automatic control using mass-produced stalls and controller units that feed the nutrients and light.

The host company is a large instrumentation group. In order to give the start-up organization the speed of operation it needs, it is set up under a separate trading name. A project manager is appointed to coordinate the start-up from within the organization. This is the only appointment at this stage; other staff will follow as needs became clearer. To obtain finance and other planning needs for the operation's start-up phase, a detailed business plan [1] is prepared using consultancy assistance.

The business plan facilitates procurement of the necessary start-up loan to float the operation for its first 3 years of operation, that being the predicted period needed to reach self-sufficient flows of income.

A business entity is set in place using an already registered shelf company to allow a formal creation start-up in the minimum time. Hydroponics Corporation is registered as the trading entity.

Premises are needed to house the team and its support staff. The requirements for this are given in the business plan. As hi-tech start-ups are notoriously uncertain in terms of needs and speed of growth, the project manager has chosen to rent premises in an incubator business park (Figure 3.1). This gives them a good business address, access to centralized secretarial and office equipment, meeting rooms, refreshment facilities, and even potted plants, pictures for the walls, presentation equipment, a parking lot, and grounds that are tended on behalf of tenants. More important, there will be space available as they grow.

The location of the park selected is decided from a compromise of variables such as the proximity to land on which to build the hydroponics development facility, staff availability, local relevant skills, profile of the business park, and conditions of occupancy.

**Figure 3.1** Example of a typical business park accommodation.

Incentives available for taking a place in the park are negotiated to sweeten the operation.

In parallel with location selection, staff are progressively selected and appointed to suit the stages of the business plan when their skills become needed. Accounting, banking, and legal support are appointed on a part-time basis from the start.

Activities then commence to obtain patents, the trademark, and to register a product name, these all needing little engineering input, but already using up budget. Trade accounts have been started, making use of extended payments where possible to help the poor cash flow situation.

A core team of designers is formed to cover the electronic system design, manufacture of controlling equipment, and general operational issues. It is yet not seen that a full-time hydroponics expert is needed so a consultant has been retained.

After around 6 months, commencement designs are ready to prototype, and a small research and development laboratory is being built. The company is just about ready to commence growing limited amounts of vegetables and fruit to test the systems being developed. By this time technicians and more designers are being appointed.

While there is still no certainty that the venture will be successful, it is necessary to produce publicity and promotional materials to help the effort along. As well, it is now emerging that exporting equipment systems might also be a profitable extension along with developing proprietary local grower operations.

After a year from the start-up, the first crops have matured and data from the test facility has been used to firm up elements of the business plan, which by now needs serious revision for much had been learned over the first year. Some things have fallen out of favor, new issues have emerged, and confidence has increased. This looks like a winner!

It is now the time to progress into developing a commercial growing facility that takes the design ideas from the prototype to full-scale operation. Starting up that kind of enterprise is not appropriate for the initial R&D team, so another new company is created, taking appropriate staff out of the development company to assist its run up.

After 2 years, the original start-up has become the ongoing R&D support arm for the expanding commercial operation.

Each start-up follows a similar path but always with variance in the what, when, and how issues. Considerable business skill is needed to make the best of this situation. More details of starting up and operating a small business enterprise are available [2].

## 3.2 Staffing Aspect of the Design Team

### 3.2.1 Financial Issues

Staffing is the most important asset of a project. For a design type organization it will usually be found that staff costs constitute from 70% to 95% of the total turnover.

Staff brings innovation, expertise, and experience; without them there is obviously no activity.

Despite its obvious value-adding importance, too often this seems to be a facet of leadership responsibility that those with an engineering education are less than ready for.

Direct costs arise with respect to:

- Locating potential applicants;
- Selecting and hiring an appointee from a list of applicants;
- Relocating the newly hired appointee;
- Helping the appointee settle in for the first few weeks, possibly providing accommodations and a car;
- Providing ongoing daily support for the appointee to perform their work (office, cafeteria, salary management, etc.);
- Carrying through a position termination or a resignation (office refurbishment, departure records, termination payments, signing back-issued resources, and taxation issues).

Along with a salary, the employer is also required to provide so-called "on-costs" of a position. These vary widely but will usually include:

- Various leave entitlements (recreation, sickness, paternity and maternity, long service, bereavement, etc.);
- Pension arrangements (superannuation, etc.);
- Other company-provided benefits that may be included in salary package (health insurance, fitness club, car, phones, etc.);
- Insurance (public liability and professional indemnity);
- Salary inducements that are paid in addition to the stated salary.

On-costs added to salary can amount to a minimum of 30% of gross salary, and they are often even higher.

Having now accounted for the directly attributable costs of a person, add to this what are called overheads for the support of staff to perform their jobs efficiently. These include:

- Office space, which will be owned or rented;
- Office furniture;
- Office tools;
- Office support staff;
- Administrative staff;
- Records management;
- Training;
- Security clearances;
- Travel on business;
- IT computing equipment;

- Communications, including phones, faxes, and networks;
- Insurance for buildings, supplies, and equipment;
- Expense accounts for entertaining customers, and the like.

The general overhead needed to support a professional designer can be in the range of 100% to 400% of gross salary. Some professions also include the cost of other staff supporting the charged-out person's time.

When all of the above costs are lumped together, it is not unusual for the charge-out rate for design work to be from 2 to 5 times the gross salary with travel costs still to be added if out-of-office visits are needed.

Thus, putting in place a new staff appointment can be the most costly decision ever made by a manager. This comes as a surprise to many staff members, who may not realize the magnitude of the impact on the overall long-term performance of their team.

A staff appointment also needs to be seen in the light of a recurrent salary, continuing for possibly many years, and how it often influences the overall path of development for the team and the organization.

### 3.2.2 Role of Staff in a Team

Staff members are employed to add value to operations. This value-added component is not easy to calculate in a detailed way for design activity. However, the concept of adding value, and of preventing or reducing rework can be applied in the general sense for helping to make staffing decisions.

Poorly matched, inappropriate staff can all too easily add negative value! The team leader is seeking to form a well-oiled, coalition thinking set of experts (see Section 1.3.1.) The team will not function well if any one of them needs to be coerced to do the job at hand.

### 3.2.3 Commitments by Employer and Employee

Staff members are not inanimate objects in a production line. Well-treated people usually respond in kind. The converse applies; poor treatment results in dissatisfaction that yields negative value added, errors that show up later, and time lost in modifications.

In addition to handling programmatic aspects and overseeing the design activity team, managers also must attend to:

- Staff development;
- Working conditions;
- Mentoring staff in the technical aspects of their work;
- Pastoral care of staff in difficult personal times (which must be done with particular care and caution).

Large organizations will usually have staff appointed to assist these functions. Staff members, however, often need to be encouraged, indeed compelled at times, to make use of this kind of support. It is an observation that these services often follow a trend, peaking at various times with compulsory attendance at training sessions and then fading away as top management move to address other issues. The team leader and members should keep these issues active in their daily roles; they are important to being successful.

In the smaller organization, the team leader will need to assume these roles. These functions are necessary regardless of the size of the activity.

### 3.2.4 Time Constants of Staff Appointments and Replacement

Finding and settling in a new person can take unexpectedly long times to achieve. In one instance, it took 3 years to finally set up a senior leadership position; two rounds of prior appointment attempts failed at their invitation points!

Why can it take so long? Numerous kinds of delays can be encountered. These are generally longer in the large organizations unless some form of fast-track appointment process is employed, which usually means greater expenditure. There may be several slow-moving committees to pass decision-making through. Long, deliberate nonapprovals are also common practices to release money for other purposes.

An employment agency is often used to assist in developing the requirement and to confidentially headhunt staff. These agencies have special expertise and connections that can potentially speed up the process and find the best person.

Delay in making appointments can arise due to delays taking place in the many processes that have to be performed sequentially. Sources of delay are shown in Figure 3.2.

Some principle reasons for slip, with likely times, are as follows:

- *Defining the job requirement and getting internal approval* to proceed is a managerial decision that is part of organizational overall resource

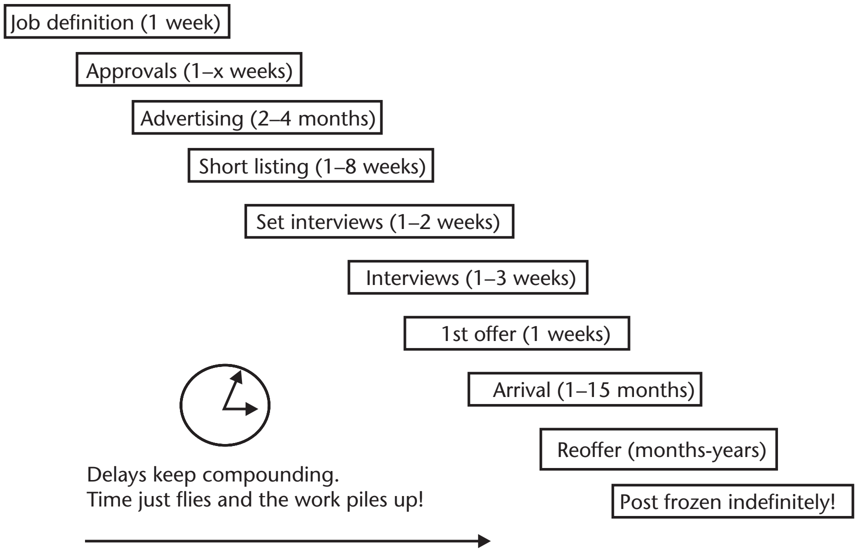


**Figure 3.2** Sources of delay in appointing staff.

management. If the position is still filled it may not be possible to proceed until it is finally vacated. (1–4 months, even years at times).

- *Advertising* will be needed to attract applicants (1–4 months).
- *Selecting a short list* can take several meetings (1–8 weeks).
- *Setting interview dates* can require quite lengthy time frames to fit them into the availability of all the involved candidates and interviewers (1–8 weeks).
- *The interview period* will vary to suit the availability of the candidates and the style of interviewing used; some are simple face-to-face, one-time meetings; some take place over 1 to 2 weeks of events (1 day–3 weeks); it is not unusual for some appointments to hold as many as eight interviewing rounds to gradually filter out the applicants!
- *First offer and time to accept.* E-mail communication can get the job offer to a person within a day or so. Letters can take 4 to 14 days to be received. Some candidates reply immediately, while others get into extensive negotiations before finally accepting or rejecting the offer (1 to 3 months).
- *Taking up the position.* Many different reasons exist that determine the time to actually start in a new position. A common reason for delay is an existing contract with a notice of resignation condition. In some professions it is required that the person to be appointed does not work for a competitive company for 6 months prior to hiring. Serious delay in arrival can also arise when a work permit is required for nonnationals (1–15 months).
- *Reissuing an offer.* If the person to whom the first offer is made declines the position, it may be acceptable to offer it to the next person ranked on the short list. Worst still is having to traverse the full process cycle all over again (months–years).
- *Infinite delay!* Organizations can change their hiring policy at any time. If serious delays have arisen the position might well be frozen due to quite separate events taking place. The dilemma of taking a poorly matched, just appointable candidate, with least delay, as opposed to waiting for another round of applications, can be a hard call that a team leader will sometimes need to make.

As well as being street smart about making appointments, the team leader will need to be equally smart with terminations of staff contracts. These may arise in harmonious circumstances such as resignations, but sometimes they are a trauma for all involved.

Staff dismissal in the latter situation requires skillful handling of an appropriate process. Getting advice is highly recommended in these cases because the situation can easily backfire for procedural reasons, leaving a person in place who does not fit the position and who may be highly resented by the rest of the team.

A termination clause in the appointment contract will spell out the conditions for departure, usually requiring either side to offer a given number of weeks of notice. Usually the employee will need to take the rest of any remaining allocation of recreation leave and other outstanding leave entitlements within the remaining period. This means a position can be left unfilled for several weeks, leaving a gap in staffing deployment. Labor hiring agencies and consultants can be used to fill gaps, but at a premium price.

Termination clauses are usually negotiable. In some circumstances it may be to the employer's advantage to accept a shorter resignation period than the contract requires, to save costs and facilitate faster replacement.

There was a time, mostly but not exclusively in large government organizations, when staff could earn tenure of employment. This gave them a job virtually for life. Today, that privilege is all but gone to any employee. Even obtaining permanent employment status does not give a guarantee of lifelong employment anymore.

Many current staffing agreements allow an employee to be dismissed under a redundancy termination provision. Redundancy terms can be quite complex and are found in the contract of employment from the human resource (HR) department or staff employment union.

Redundancy is generally valid if the need for the position no longer exists. Another person cannot be appointed to the same position after the redundant person has left. (Organizations often get around this by reengineering the structure to create new positions with different duties.) The redundancy payout is usually based on a given period of notice being served by the employer, compensation being set in terms of annual salary and years of service.

The selection of who is declared redundant usually begins by inviting those who are interested to apply for it first. Personnel in key positions often have their applications for redundancy declined.

Being dismissed under a redundancy clause is a very common occurrence in larger organizations. Despite a slowly fading stigma that was once associated with it, being declared redundant usually has no basis in staff member lack of competency but is more a matter of high-level management expediency arising where there is need to shed operating costs or reorganize operations.

Appointment of staff can, therefore, take from days to years. In larger programs, it is not uncommon for companies to start the process of hiring staff well before they are needed, in anticipation of winning a contract.

At the other end of the time-scale spectrum, it is sometimes possible to locate and appoint a person in a matter of days. However, care should be exercised in such cases to not allow haste to cloud sound decision-making because of the pressures of an existing project's need. It is usually far harder to terminate employment than it is to make it!

There are two tempting-to-use poor practices that are often not dealt with at all well in small companies: first, allowing staff to start without a contract being set up and signed, and second, not having obtained budget approval or verifying that a position can be supported. These practices should be avoided.

On occasion a person may be hired without an adequate position description. This also is poor practice, for it can lead to many difficulties if the match is not well made. It pays to dot the i's and cross the t's very well in the form of a written and agreed contract giving the job description, time of start, conditions of appointment, and termination arrangement for both the organization and the employee.

### 3.2.5 Skills Needed in the Design Team

The nature of engineering design calls for a wide range of skills, and a well-formed team can cope with the variance needed. However, skill supplementation is often needed.

Construction of a T diagram (see Chapter 2) will assist development of the breadth and depth aspects topics likely to be required. Figure 3.3 shows a T diagram constructed for an engineer specializing in sensor and data acquisition systems aspects but who is not required to be an expert with the software side of design.

Having a set of these in place for the team will assist the leader in recognizing what the team can and cannot do.

It is often felt that a quick survey of any special knowledge needed in a project can be filled in by one of the team. Generally available knowledge is usually somewhat stale by the time it becomes widely available. As such, it rarely includes the trend and current emergent thinking that is driving progress. It is often the case that an external expert can bring to the operation that deeper knowledge. Whether a consultant is called in for special needs depends on:

- Level of impact the specialty has on the project outcome;
- Time available to make a decision;
- Whether funding is available to hire in services;
- Whether such an expert can be found who really does have the skills needed;
- How easy it is to explain the problem situation;

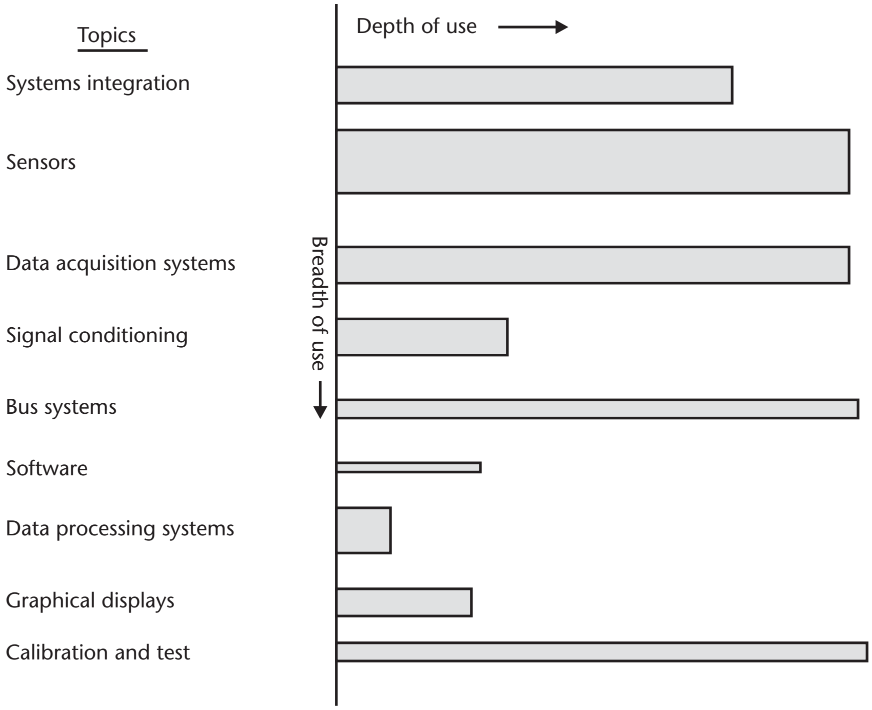


**Figure 3.3** Example T diagram for a design team member.

- The depth of understanding needed.

A committee can be formed to decide the need but this way of proceeding can be lengthy in its deliberations. Use of think tanks and other information-gleaning processes are certainly useful (see Chapter 7).

Another way to obtain skills in a team is for members to be given time to attend training and to improve their educational qualifications. There are pros and cons with this. Increasing skills can make staff more portable inside the industry but it can also reduce staff turnover. An often-vaunted reason for management to not support skill upgrading is that the staff in question cannot be released as they fill key positions. Some large organizations support a small amount of paid hours per month for staff to undertake specially constructed in-house personalized courses. They might also support flexible hours working to help staff undertake upgrading education on a time lost recovery and perhaps tuition fee recovery basis. It is usually the case that significant staff development is a personal commitment made in one's own time.

### 3.2.6 Determining the Overall Staffing Requirement for a Design Project

Core staff needed includes enough scientists or engineers to develop the design detail and supervise prototype manufacture and testing. They will need the support of skilled technicians or engineering associates. Modern engineering of systems is a complex task. It can require a wide range of skills. A checklist chart can be used to assist broad identification of the skills that may be needed as a project passes through its life-cycle stages. Figure 3.4 is one way of presenting many of those skills for easy comprehension.

It is essential to decide:

- Mix and depth of skills to meet project needs over its duration;
- Support for the staff to help them do their job well;

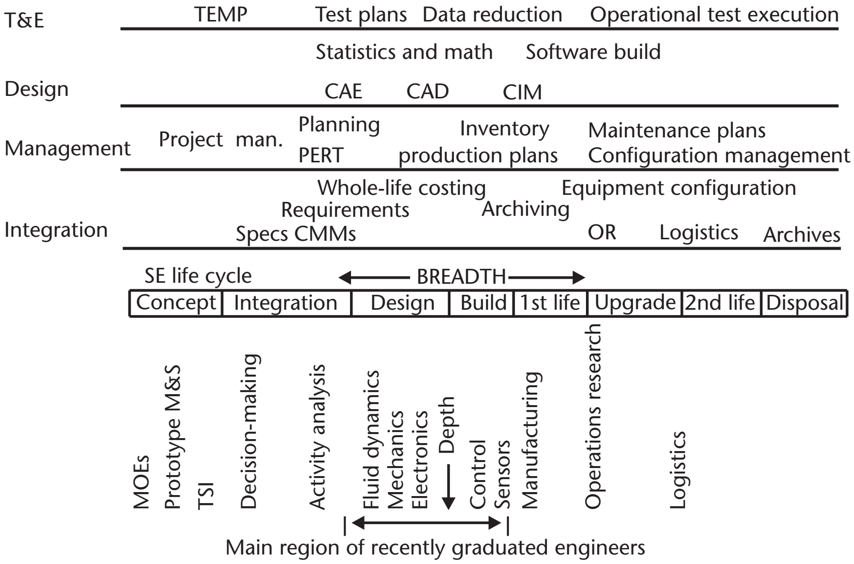


**Figure 3.4** Mapping of disciplines onto the SE life cycle.

- Interfacing needs with each other and with other design teams;
- Envisaged future needs;
- Legal aspects of staffing;
- Accounting and financial aspects staffing.

The team leader, depending on the project size and organizations management structure, may be nominated to carry out many of the tasks. It is unlikely that the team will need much marketing and promotional skills as they are usually provided by the organization at large—and engineers are not usually good at these anyway!

After analyzing the project and deciding on the staffing mix required, consideration is needed for:

- Delays of arrival of new staff and selecting and contracting consultants;
- Time for new staff to settle in and learn the local organization's policies and practices.

Finances need constant management. In the smaller enterprise, that task will be carried out by one of the trained staff using the services of an accountant and auditor on a part-time basis. A large organization will be able to support a central accounting group. A team leader will have to control the team budget.

A considerable amount of record keeping, filing, and correspondence always exists. Office secretarial services will be needed, perhaps on a part-time basis. Use of computer-based office operations reduces but does not eliminate the need for a traditional style of secretary who can type. The secretarial role has changed over time to be one of general administration by an administrative officer.

Regardless of size of the operation, there will commonly arise a need for external consulting services. These would include such tasks as carrying out market research, preparing publicity material, maintaining the computing system, printing business cards and reports, and so on.

A first step to deciding what staff will be needed is to list the skill areas that the business plan or project outlines suggest. Listing the topics needed and then rating them by time and depth will assist in deciding the need. This may seem to be a time-consuming way to approach things but it does pay off and give data for use in reports and proposals. Obviously, the activity must be scaled to suit the resource size and time available.

Some factors of possible help in framing the team requirements include:

- Breaking down project tasks into the hard and soft sciences kind. Establish the kind of disciplines needed for each and the effort time envisaged for each.
- Consider the experience that was needed for a relatively similar project.
- Use records of earlier projects and discussions with former leadership as a source of lessons learned.
- Apply both systematic (process used) and systemic (holistic attitude) thinking to the problem. Develop an operational concept for the project, as this will tease out the staffing need once the operational events are isolated and described in a process.

- Take care not to force existing staff into poorly matched situations. Learning can take quite a while!
- Be prepared to compromise—the perfect team is a rare thing.
- The leader should be cautious with his or her own enthusiasm and expectations of what a team can actually do in a given time. Managers invariably underestimate the time taken to do things and the breadth of skills available.

Figure 3.5 indicates the various paths for building up the skills and knowledge of a design team.

### 3.2.7 Selecting a Staff Member

With the overall team requirement now better known, the next step is to create more detail for the individual staff positions. A useful checklist follows:

- Obtain a job description of the position to be filled from the previous person or the organization's HR records.
- Decide the integration level and skills of communication needed for the position.
- Determine the work tasks expected for now and the near future. Developing a T diagram for each person is useful.
- Obtain a set of job task competencies for similar positions and prioritize them for the particular position. These are often only available as company proprietary intellectual property (IP) lists so it may be necessary to develop your own set for the project.
- Determine what peripheral tasks might be required of the person, such as being a member of a standards committee that the company supports.
- Decide the professional or trade qualifications that are appropriate to the position, remembering that education has its general aspects and people usually

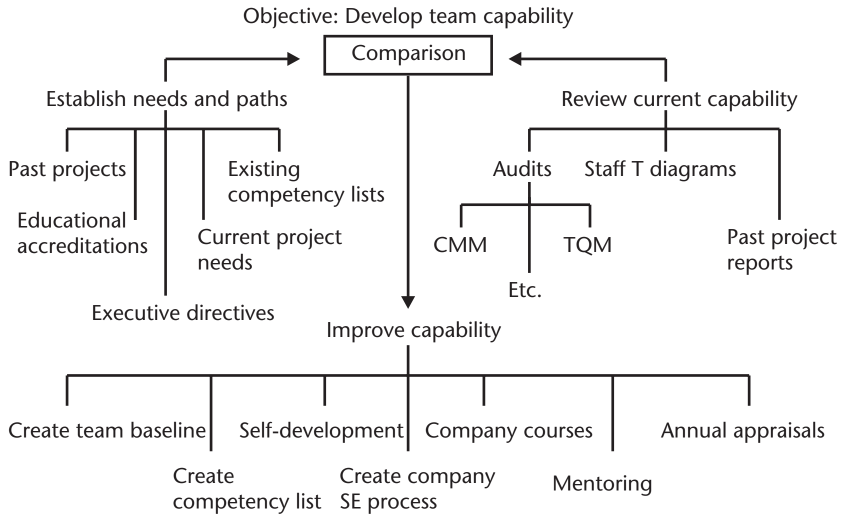


**Figure 3.5** Strategy for developing the skills needed for a design team.

widen their skills over time. It is said that you cannot tell what basic area a person was trained in 5 years after graduation.
- Decide the type of practical experience needed to supplement any paper qualifications.

The appointment process will require much of this information. A documentation effort done with some degree of formality will motivate doing the right research and asking the right questions. Such investigations are too often only conducted in the head of the team leader.

Support for the following will usually be needed for a new appointment, which is done in strict confidence as these are considered personal issues where privacy must be preserved:

- Developing the hiring contract, including statement of duties, conditions, perks, salary package, and termination;
- Salary payment method (cash, check, direct deposit to a bank);
- Salary packages to offer (salary, salary sacrifice options, pay increase plans, perks such as serviced car and gas, health insurance, phone, accommodations);
- Statement of growth potential;
- Terms of appointment (tenure, contract, permanent, permanent part-time, part-time, or probationary);
- Travel and resettlement allowance details (including any arrival accommodations and car);

### 3.2.8 Legal Aspects Concerning the Hiring of Staff

As we have discussed, hiring a staff member is a complex, costly, and lengthy set of activities. The nature of the tasks and agreements usually require legal support. Legal issues are introduced in Chapter 10. Larger organizations usually employ a company lawyer or retain the services of a law firm; small operations, often to their regret later, will ignore legal needs because they are costly and can delay matters far too much.

Staffing matters of potentially real impact in legal terms for an organization include:

- Contract of employment that is signed when accepted by the employee and employer;
- Confidentiality agreement for nondisclosure and possibly noncompetitive rehire time if the employee resigns;
- Pension schemes offered by the organization;
- Work agreements with staff unions;
- Freedom of information control;
- Permission to use personal details in a public arena;
- Equal opportunity statement;

- Occupational health and safety statements and safety of designs;
- Patent and other trade protection issues;
- Records of IP brought into the position by a new employee;
- Health examinations of a compulsory nature, such as retinal mapping in laser-based working situations and radiation screening;
- Setting assignments of copyright and other IP components;
- Environmental laws and regulations.

Suitably experienced lawyers are needed to give the best protection from the numerous litigious situations that can arise without warning.

## 3.3 Premises and Equipment

A written report is worth preparing for both premises and equipment, as that clarifies the mind. Premises will be often provided, according to some kind of bidding process, in the larger organizational situation. The smaller operation will generally need to locate suitable premises. Options for accommodating the project include:

- Renting an office and industrial space;
- Using a multitenanted incubator science/technology park facility (office support centralized for tenants);
- Purchasing premises (this is often a sound long-term choice but requires valuable start-up cash for the deposit and purchasing fees);
- Building premises (rather too slow for most situations, but nowadays a small factory can be built in weeks. Obtaining building permissions is likely to be a significant delay factor!).

Premises will usually need:

- Electronics or other specialized laboratory space;
- Suitable equipment (purchased or hired in);
- Environmental test plant;
- Development and test equipment areas;
- Testing area;
- Storage and use of project-related customer plant or equipment;
- General storage for stock and tools;
- Staff amenities;
- Parking spaces;
- Loading area;
- Library and records area
- Meeting area for client meetings and reviews;
- Computer or hard-copy drafting facility;

- Security system level, as dictated by type of project (company, police, military);
- Office space for group leader and group administrator;
- Space for consultants on visits;
- Telecommunications (phones, fax, intranet, Internet, ISP, or proprietary server, broadband connection);
- Office support plant (server, computers, printers, copier, report binder, stationary supplies).

When moving into new premises, minor building alterations are usually needed. Incubator accommodation normally provides large open areas that are partitioned off with reusable walls and power and IT cable runs. Allow at least 2 to 3 weeks for building alterations and any internal installation. It can easily take 1 to 3 months for a relatively stable routine operation to be put into place. It is an exciting but very demanding period; there will be many peripheral activities to be dealt with.

## 3.4 Managing Staff Turnover

### 3.4.1 Factors of Staff Turnover

Once an operation is set up, some of the appointed staff may well wish to leave for a variety of reasons. The rate of staff turnover needs control in the design situation, for replacements are not as easy to find as in those jobs where prerequisite knowledge is minor and training time is a few hours.

High staff turnover is costly and very disruptive in project development. A high rate might be an indicator of poor management or staff conditions, but not necessarily so. This phenomenon is complex in nature. Factors affecting staff turnover rate include:

- Alternative employment opportunities;
- Geographical relocation distance limits;
- Agreements on the length of notice needed to terminate;
- Career prospects on offer within the organization;
- Management style;
- Staff development support;
- Local rumors about the long-term survival health of the organization;
- Interest level of projects;
- Employment conditions in general;
- Parity with similar jobs;
- Enticements offered (such as shares in the organization's stock).

These are all double edged. Skillful use of inducements to stay can play a large part in reducing staff turnover.

### 3.4.2 Minimizing the Impact of a Resignation

Any employee might resign at any time. This point seems to be lost on some managers.

Suppose all of the inducements that can be offered have not worked well enough and a good designer has decided to leave your services. What can be done to minimize the impact of this situation?

It may well be a serious setback but the aware team leader will have already set up contingency plans. The staff resignation situation is common and always seems to occur at the worst times. The team as a whole will feel the impact of a missing person in doing extra work, so it is important to move rapidly to fill a vacated position.

It is important to have sound, ever improving plans in place that might well attract staff to stay on and also to find and entice replacements to sign on.

When a resignation is becoming apparent, have alternatives ready that will allow you to match the external offer made to your staff member.

Work hard and consistently to keep staff turnover down, as it can feed on itself and cause panic in a workplace. Many staff members are satisfied with their situation more by default than analysis. A noticeable exodus may well cause them to consider their situations and begin to explore their alternatives.

Speedily remove disruptive and negative value-adding staff because they can impact significantly on a healthy work environment. Using the "golden handshake" can be the cheapest and fastest way to reorganize staff, as it is often more expedient to incur a short financial loss than go on paying a salary in the hope that the matter will resolve itself.

Notice of resignation is the trigger to commence the reappointment process without delay. Where feasible, maintain a list of likely candidates. It is wise to plan for overlap of the position to allow the outgoing person to help the replacement settle into the job.

In cases where it is clear that a person will be retiring or is about to be promoted. a wise team leader has succession planning in place. The draft hiring documentation can be prepared and a sensitive ear can be at work, listening for names of suitable candidates who might be interested in joining your organization when the time comes. A good way is to retain a small team of consultants and other part-time staff as a pool of potential new staff.

Maintaining a watching brief with an employment agency can turn out to be useful in speeding up replacement.

All this being said, it is only possible to give pointers for managing staff. Experience and direct wisdom are valuable commodities in this soft aspect of design team life.

## 3.5 Organizational Structures Used in Different Kinds of Businesses

### 3.5.1 Place of Organizational Structures

This section will assist designers in understanding the structure in which they operate.

Three dominant organizational structures can be identified in team operations—military, flat, and matrix. Each has it pros and cons and none provides the ideal situation.

A design team typically comprises 4 to 10 members. They have to communicate their design progress to each other and their collective work has to be interfaced to other teams and to higher management. The type of structure in place can have significant influence on team efficiency.

Engineers are well known for pulling together at the design team level. Left without a purposely-designated structure, team behavior will usually sort itself out into a sound coalition of people working within a combination of all three structures given below. Some decision-making and responsibilities need clear, well-defined, organizational structure; others do not.

The personal style of the team leader will largely dictate which is used, as will higher organizational dictates coming from such working practices as IPT operations.

The following sections give the pros and cons of each type. Figure 3.6 gives the structural model for each.

### 3.5.2 Military Hierarchy

Military hierarchy has evolved from large hierarchical organizations such as that of an army—hence the name. Its characteristics are:

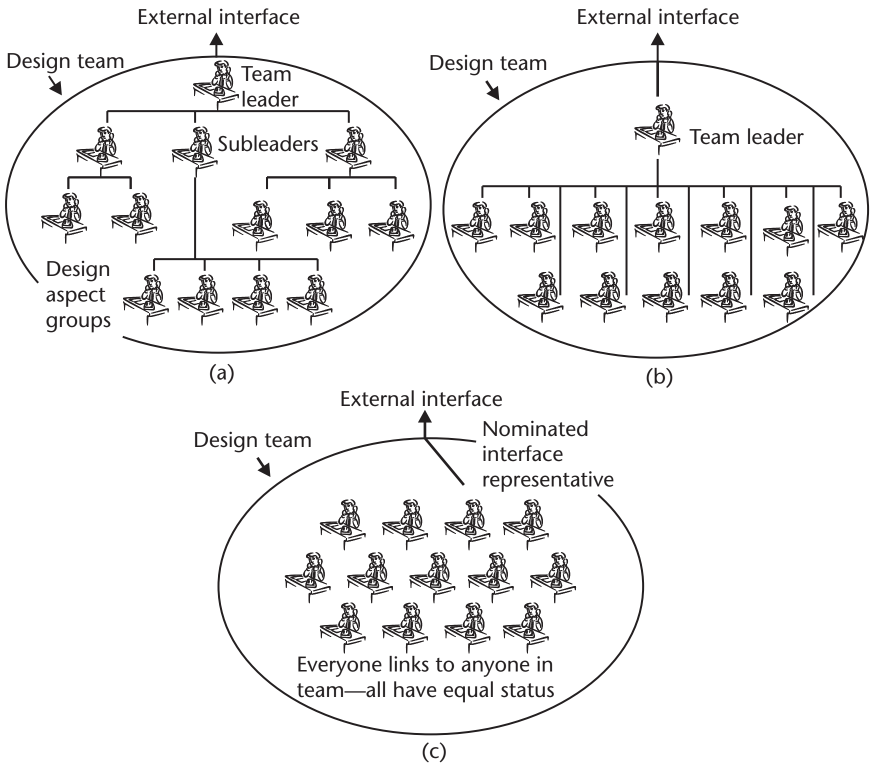


**Figure 3.6** Common organizational structures for a design team: (a) military framework, (b) flat structure, and (c) matrix operations.

- Clearly defined lines of decision-making exist, can be identified, and are expected to be used exclusively;
- Slow response compared with the following flat and matrix methods;
- Can be intimidating to lower-level staff;
- Accepted as sound practice for large organizations;
- Should have only three to six reporting relationships at each level of the hierarchy;
- Does not easily engender innovation, as personal action is not always encouraged;
- Can become politicized at its various levels;
- Has negative performance parallels for getting things done that equate with the deficiencies of the previously covered waterfall process;
- Can suffer from bureaucratic attenuation as messages rise up looking for a response;
- Messages can easily lose their original content where the number of levels increases.

In the design team situation there is usually only a small number of staff, so using two to three levels is sufficient to ensure the reporting relationships are within realistic limits. The second layer will also include a deputy leader to give continuity of operation at all times.

Design activity can be split into three or four areas, each reporting to the leader. These areas will often comprise the same staff operating in different roles. Clear status and position relative to the team leader is evident.

### 3.5.3 Flat Structure

In the flat structure model, all team staff report to the team leader. This model is often used. Its features are:

- Might have too many reporting relationships for the leader to effectively manage;
- If strictly adhered to, queries need to pass through the team leader, who is probably overloaded due to the large number of people who report to him or her;
- Can work well in smaller teams (up to say 10 staff members) where the team leader is highly experienced and able to work in this mode for the common good;
- Can, however, permit a dominant leader to overpower staff decisions and innovation.

This is a typical way of working in small teams. It gives the leader definite status, responsibility, and decision paths are clear.

### 3.5.4 Matrix Organization

To conduct rapid and tight design development, it is advantageous to let all team members work up their own contributions with direct lines of communication with other team members.

The pros and cons of this method are:

- Has fast lines of communication, as all staff can refer directly to the person needed.
- Leadership is less well defined in status terms.
- Staff can find this situation unsettling because it is unclear who is in charge. They often need time to feel comfortable with the less-obvious higher management.
- Is typical of IPT operations.
- Has strong use of design concurrency, which can make it more efficient.
- In terms of organization behavior and assuming all projects of any substance are in the "complex" organizational group, this structure works well with a coalition environment but is likely to fail if the team spirit is coercive in nature.

All members enjoy similar status and that can be more acceptable because team members are each a specialist in their own right. A defined team leader is still needed to oversee relationships and duties and to provide the management interface with other teams. In some cases an administrator kind of leader is used. This can be a disaster because the leader does need to be familiar with the technical aspects of the project. An administrator is a useful position when it supports the team and leadership with those necessary, but time-consuming, routine duties such as budgets and annual report preparation.

## 3.6 Staff Appointments

### 3.6.1 Human Resource Management

We have previously touched on the problems of finding and retaining staff. Here we go deeper into hiring practices.

The importance of human resources to the success of an enterprise has led to the older idea of a simplistic staff-hiring department being upgraded and expanded to what is now usually known as the HR department [3]. HR functions are:

- Control staffing levels and suitability;
- Support the location and appointment of staff;
- Give staff support in the implementation of organizational HR policy in such matters as hiring conditions, staff development, and equal opportunity;
- Give support in legal aspects of staff matters;
- Arrange staff development programs.

Where the organization is large enough, the HR department will support the design team leader for most of the staffing issues that arise. In this case the team leader has to follow the organization's requirements, making it imperative that he or she becomes quite familiar with stated policy and practices. It is so easy to be caught short by not following them—with subsequent rework and anguish, perhaps even getting involved in protracted legal matters.

Smaller organizations will require the team leader to carry much of these functions as part of his or her duties. The general practice of HR management is well documented, but its specific application must be established from local documents and practices.

### 3.6.2 Documentation Involved in Hiring Staff

We have already seen how it can take an unexpectedly long time to find and place a new team member. To keep delays to a minimum, it pays to give quality and timely effort to preparing the materials needed to support finding, attracting, selecting, and appointing a person. This section provides an awareness of that documentation.

Many variations of an organizational hiring process exist because different labor laws exist from region to region. The required documentation presented here illustrates the materials that might be needed.

The general points of setting this process up, conducting interviews, and assessing applications are well covered in [4]. Figure 3.2 illustrates the mileposts of the hiring process. Each step has associated documentation.

An appointment committee oversees the process. This is usually set up according to organizational recommendations. Typical members will be:

- An expert interviewer as the chairperson;
- Manager of the team leader;
- Present position holder (if appropriate and available);
- Team leader;
- Member of team with relevant expertise;
- HR representative (to service the activity and ensure the rules are followed);
- Equal opportunity representative (where required);
- Representative of one or more from a closely related other team(s);

The team leader and HR representative will usually develop the necessary documentation.

There are many documents required, and preparing them may seem to be somewhat overdoing things. However, each document helps to reduce the risk of making a less-than-optimal appointment. It is wise to keep reminding all concerned that a few weeks of activity and several short meetings can help to ensure that staff appointments, which may have great influence for years, will be sound commitments.

Documents needed are:

- Position description or duty statement, including a T diagram.

- Organization's description showing relative place of the position in its structure.
- Description of the working environment of the position.
- Details for forming an advertisement (this is eventually composed by others).
- Interview strategy and small set of well-thought-out interview questions (in some situations only these predetermined questions can be asked at the interviews).
- Details of any presentations, or other tasks to be performed by interviewed candidates.
- Terms and conditions of the position.
- Draft letter of invitation.
- Timetable with optimal milestone dates. Key dates to set are for placement of the advertisement, closing date for applications, interview timeframes, date the decision will be finalized, and date of notification to unsuccessful candidates.
- Date of notification of an offer to the first ranked person (this person sometimes declines so be prepared to make subsequent offers).
- Envisaged commencement date.
- Text of letter for notifying unsuccessful candidates and statement of process for such (a standard letter that is personalized in use).
- Candidate application review sheets. These are usually created by HR staff with the key points listed in a table for assessor comments to be added alongside. The criteria arising out of these for an applicant to be judged as "appointable" must be clearly stated. Subjective and unsubstantiated exclusion of a candidate is not permitted in best practice appointment processes, as it does not provide grounds for nonselection when asked for by the applicant or for use in any appeal process.
- A frequently asked question (FAQ) list of expected questions with answers; answers may be company confidential, or at least not for general release.

Upon receiving an offer it is not uncommon for the invited person to require considerable negotiation regarding the terms and conditions of employment. The result of this negotiation may well see the person decline the offer. To this end, the documentation listed above should try to second-guess likely questions and provide information for ready access.

Cases are also sometimes encountered where people accept the offer and then procrastinate, finally pulling out.

Typical negotiation points that arise in finalizing an appointment offer can include:

- Terms of appointment such as job title, office accommodation, perks, and performance targets;
- Premium payments for cost of living at the job's location;
- Relocation costs and provision of some initial personal living accommodations;

- Unavoidable external issues such as transfer of superannuation and pension rights, work permits for overseas appointments (for example, a green card in the United States), and unexpected illness;
- Family requirements, such as transition of children's schooling and term dates.

### 3.6.3 Tailored Processes

Individual staffing situations can be so different. The above process should be tailored to suit local practices. In some cases, the organization may hand over operation of the hiring process to a management hiring agency.

It may well seem attractive to cut corners in order to speed up the process. This can, however, be counterproductive if not carefully controlled.

## 3.7 Staff Selection

### 3.7.1 Finding Candidates

It is often said that there are many more people seeking employment than there are job vacancies. This suggests that dozens of candidates will offer themselves for your position. The reality is that by the time the various constraints for your new position are applied to that large set of people, very few actually match the need. In systems engineering, the supply situation has been poor for a decade or more. As time is usually of the essence in replacing staff, the wisest strategy is to make a sound job of seeking candidates.

It is sometimes compulsory in an organization to ensure that a position's availability is widely publicized to seemingly ensure that the "best available candidate" is appointed. It is often also organizational policy that an internal company transfer be first investigated.

Methods for finding candidates are many, and all need various amounts of time to explore. They include:

- Placing paid advertisements in local, regional, national, and international newspapers, and researching advertisement deadlines and any legal requirements that have to be satisfied for publication;
- Advertising in professional magazines (this often requires 2–3 months notice);
- Advertising in Web-based appointment services, often allied to newspapers;
- Checking the above sources to see if anyone is offering their services;
- Notifying a suitable set of groups by a selected e-mail drop;
- Using market intelligence to find out whether people are becoming available (for example, a corporation collapse that will be placing people in the job market);
- Using an employment consulting firm;
- Using government social welfare job-placement agencies;
- Word-of-mouth broadcasting of the position;
- Informal discussions in personal situations or at professional meetings;

- Using already cultured relationships set up in anticipation of a position becoming vacant.

The advertisement has to be prepared and await the next publishing opportunity. This can take from a few days to many weeks. The specialized nature of design positions may not suit the use of local or even national newspapers. Advertising in these places can be a waste of money and time.

Using Web-based appointment services is certainly attractive as it is fast method for getting the notice to the public, cheap to carry out, and can reach wide target audiences. Some services will also list people seeking positions.

Many of the larger organizations, as well as professional societies, have their own employment support services. For example, the U.S. Department of Defense has a touch screen computer-based service for finding jobs that is located in the foyer of the Pentagon shopping center.

### 3.7.2 Interviews

The general points of interviewing and applicant selection are well explained elsewhere [4]. This section supplements the basics of general best practice with additional discussion points specific to the engineering design team situation.

Career progression is an important issue to most applicants. A surprising number of engineering design positions employ relatively static SE processes. Staff in these positions will find it hard to progress up the promotion ladder or be able to change positions if they need to do so. The employer must have good answers to questions on staff development opportunities for such staff.

Designer's positions will usually have a quite specific role at the time of appointment. This, however, will come to an end at some time and the tasks will change. Candidates will need to have some idea of their future work.

The totally electronic office may not really have arrived but many of its elements are routine. Expect questions about office e-systems used (Microsoft® Word, Lotus™, etc.) and the extent of tools proficiency needed to service the position.

Some candidates will say they can do everything asked of them. Software is a good example of how easy it is to be fooled by a candidate—they can use tool X or write in Y code—but how well? Penetrating questions are needed to probe their depth of knowledge and skills because there is no easy way of calibrating these competencies reported on a CV. A guide to good CV preparation [5] is also useful for examining those received as well as preparing them.

Mention of CVs is appropriate at this stage. It is wise, sometimes obligatory, to check the validity of qualifications by consulting the registers of the award-granting organization. Sighting a certificate supplied by a candidate is not always a guarantee. There was once a case of an engineering appointment of a person with a sound CV including two engineering degrees from top-level western campuses. It later surfaced that the whole CV had been made up!

Past positions of an applicant are easy to talk up. Probe the length of time held and the kind of work undertaken. Ask to see some results of the work, such as photographs of equipment, circuit sheets, and articles. Have some probing questions ready about these materials.

Another testing question that rarely gets a good reply but tells a lot about a candidate, is to ask the candidate to state where they reasonably expect to be in 5 years' time. Look for a person who will not only perform the current tasks needed but appears to be leadership material. Finding good designers is hard enough; finding good design team leaders is very hard.

Staff members need to constantly update their knowledge and skills. Look for evidence of this in an application.

Some positions call for considerable travel, often to countries with a degree of instability. A candidate may not be able to accommodate this need due to a range of valid personal reasons. If travel an essential part of the job, it should be explored with the candidate.

A similar situation is the need to work long hours at often inconvenient times, especially near to delivery and commissioning milestones.

There are numerous issues that could need discussion to ensure the candidate matches the job. They are usually all self-evident—after the event! Quality consideration is a must to be sure the right things are asked in the advertisements and answered during the interview.

### 3.7.3 Appointments

All has gone well. A person has been appointed and is about to start the job. There are many things to address to make him or her feel they have made the right decision and to get them settled with speed.

A first consideration is that the person has probably made a major lifestyle shift. This can be a most vexing and unsettling time as there are numerous issues—work and personal—to attend to.

Large organizations usually offer an induction process that introduces the person to the organization at large, to its policies, and to a range of those common, but always done a little differently, general administration issues. It is also the time to meet key senior staff.

At the team level, the person will benefit if there is in place some well-thought-through commencement support.

An appropriate member of the team should assist with:

- Issue of keys, passes, and passwords;
- Computer equipment and access line;
- Stationary and materials supply paths;
- Parking permit;
- Approval procedures and the chain of command;
- Accommodations;
- Personal issues, such as finding schools for children and setting up banking;
- Organizing office space and initial setup materials;
- General office routines such as working hours, review meeting times, and other relatively regular events;
- Making the necessary introductions.

Some organizations run a mentoring scheme that provides assistance for more complicated technical issues. An informal gathering is a good way of introducing the new person and family.

This all comes down to finding the time to welcome and genuinely assist a new coworker settle in rapidly and successfully. Taking time out to read a book on staffing can help to accomplish this [6].

## 3.8 Competency-Based Methodology

### 3.8.1 Principle of Competency Assignment

Employers want to know what staff can do. This calibrates a person allowing task matching and staff development. One method for doing this is to list and briefly describe the small tasks that together form a total capability of a team. Each task is known as a competency.

A competency profile describes the basic levels of competence that a person can be expected to handle. It also represents the needs of an employer. Profiles can be assembled as defined sets that indicate a specific job title or grade. They can also be used to design training courses, degree awards, and the necessary work experience.

The European SARTOR route to registration of graduate engineers, an example of a large education standards agency, defines the competence of an individual as including:

- General knowledge, understanding, experience, and skills of the individual appropriate to the level of accreditation;
- In-depth understanding and mastery of one or more engineering specialties as required by the level of accreditation;
- Ability to perform satisfactorily in the accreditation role;
- Possession of the needed supervisory, management, and personal skills to be effective in both expected and unexpected situations.

At the trades or craftsperson level, an example competency statement will usually address a particular technical skill. An example might be "be able to make a satisfactory soldered joint." A training time for achieving this will usually be stated.

In the professions, competencies often relate to more abstract capability, for example, "Explain the basic contents of, and need for, a systems engineering policy statement."

Vocational assignments of ability do not always harmonize well with the foundational educational paths supplied by academia, which prefer to educate and train people on fundamentals, not specific skills. Competencies are little used in academia as a basis for program construction so large organizations usually need to provide additional in-service training.

### 3.8.2 Examples of Competencies for SE

A sample of the tabular entries of an emergent list of competencies for the systems engineer is given in Table 3.1.

**Table 3.1** Extract of the Set of SE Competencies Prepared for INCOSE

| *Subject* | *Item* | *Competency* | *Profile* | | | |
|---|---|---|---|---|---|---|
| | | | I | II | III | IV |
| 1. Systems Engineering Discipline Category | | | | | | |
| 1.1 | .0 | Systems Engineering Process (SEP) | 2 | 4 | 5 | 6 |
| | .1 | Define and explain the basic systems engineering terminology | 3 | 4 | 5 | 6 |
| | .2 | Explain and the difference between systems engineering and software engineering | 3 | 5 | 6 | 6 |
| | .3 | Explain the basic contents of, and need for, a systems engineering policy statement | 1 | 2 | 4 | 6 |
| | .4 | Identify and describe the basic process areas within an SEP | 3 | 4 | 5 | 6 |
| | .5 | Show how the basic SEP processes relate to the software development and integration processes as contained in the SW-CMM® | 3 | 4 | 5 | 6 |

Engineering Classification Level
I = Systems engineering practitioner (bachelor's degree)
II = Fully qualified systems engineer (degree, plus time on the job)
III = Senior systems engineer (master's degree)
IV = Certified systems engineer (mature reflective engineer)
Required Cognitive Levels (Based on Bloom's Taxonomy)
0 - No competency required
1 - Basic knowledge, recalling of specific bits of information
2 - Comprehension of the subject matter but without application
3 - Applying the information in new situations
4 - Analyzing, evaluating, or breaking down the information
5 - Ability to synthesize the information to form an original result
6 - Applying the information in both expected and unforeseen situations
[*Source*: Bob Tufts.]

In the example given above, a competency is classed in terms of the cognitive level of understanding needed in the designated grades of practitioner. These examples are taken from emergent work by Tufts [7]. His prototype table has some 300 competencies listed. At the time of writing no published, ready-to-use, competency list seems to be openly available in the public domain for systems or design engineers. The difficulty is that those organizations that have prepared them regard their competency list as valuable IP and do not usually allow them to be published.

Some will argue of the competency grading method, that it cannot embody and delineate the wisdom element of the good professional worker. However, it is a useful methodology to employ for assisting selection, grading, and development of design staff capability.

## 3.9 Staff Development

### 3.9.1 Staff Appraisal Methodology

A number of reasons exist why staff performance needs to be assessed:

- Success of a design team depends much upon the capability of its members;
- Individuals need to know how their personal development is going;

- Reclassification of staff requires a method for assessing if it is time for promotion;
- Management needs to know if their organization has adequate capability to undertake, and be seen as suitable to undertake, contracted tasks;
- Management needs short accounts of activity to assist their task of guiding the whole project.

Two recurrent aspects of personal ability arise:

- Staff appraisals for personal development planning;
- Annual assessment or fitness reporting for employment extension, possible promotion, and also for personal development purposes.

*Staff appraisals* are intended to give a staff member peer support as a sounding board and are not supposed to be used as a possibly punitive process. The person being so appraised prepares a statement of goals for the upcoming year, these being expressed in terms of activities to be carried out. An appraiser is appointed by mutual agreement of the appraiser and the appraisee.

They discuss the report, comparing it with that of the previous year to reveal where improvement should be possible to advance the person's capabilities and overall performance.

They may well write into the plan some training, professional work experience, and short-term location elsewhere in the organization.

This report then goes on file with the person's supervisor seeing only that the appraisal has taken place.

For the appraisal method to work, a clear statement has to be issued that senior staff cannot assert punitive action on a person as the result of this process. Senior management is expected to support the needs of the appraisee to meet reasonable development goals.

*Staff fitness reports* are somewhat similar to staff appraisals in what is documented. However, they are definitely concerned with finding out if restorative and employment continuance issues need attention.

Without care in their application, these can easily become contentious, breaking down the necessary coalition atmosphere of the design team. They are often seen as threatening by the staff themselves. They have, however, become very much the norm in larger organizations—this is, after all, the age of audit!

Both processes will involve the following elements or issues:

- Long-term objective setting;
- Upcoming-year objectives setting;
- Comparison with previous year objectives and their outcomes;
- Report style and length is short, with clearly stated performance issues and quantitative targets, and metrics that can actually be measured;
- A record is made of who sees report and where it is filed. All parties involved are given copies that are agreed on in writing by both the employee and the employer.

Overall, the objective is to discover and record the accepted key capability factors of the person's work that add value to the team's operations and to the staff member's personal development.

Key questions to consider include:

- What specific design activity parameters are of importance?
- What skills are to be upgraded?
- What are the relevant educational qualifications?
- What are suitable professional society memberships?
- What is suitable committee work to be undertaken, such as serving on a standards working party?
- How will the person support implementation of best practice, such as setting up and running a quality activity?
- Would it be helpful to install and apply a new tool set or other generally useful activity in support of team operations?
- What are the appropriate professional journal papers to publish?

Some of this process can be streamlined by use of standard proforma reports that require indications in boxes to be marked, to which are added a small amount of textual replies.

Annual performance systems are commonplace in the larger organizations. In such cases, the HR department will issue procedures to follow. When they are not mandated it is still wise to conduct annual audit of staff and team performance, as this assists in raising the competence of staff by establishing baselines and targets to shoot for. The process need not become, or be seen as, adversarial if used with care.

### 3.9.2 Personal Development Maturity Plans

Staff members often regard the appraisal method as a waste of their valuable time, as it is being done at inconvenient times and they feel a lack of ownership for it. They do not wish their work to be so closely questioned by a second party, and worse, see it recorded.

This does necessarily not mean they wish to ignore the need for high performance; it is more a matter of being shy of having to give account in this manner. They also have difficulty seeing that it has merit; they would rather get on with the next challenge.

An alternative method of staff development and reporting is the personal maturity plan (PMP). In this method, the staff member sets up a personal plan according to a guidance process and records outcomes as the year passes. Random audits are used to encourage accuracy. This method suits the person who is outgoing and highly self-motivated.

It is common for the various methods to be offered for staff to nominate their preference for their performance audit. It may be necessary to explain to them that this is a necessary task of employment for the reasons given above.

A guide to self-development for managers provides a deeper look at this subject [8]. Section 12.4 discusses the issue of personal development by a staff member in conditions of change.

## 3.10 Team Culture

### 3.10.1 Overview of Methods for Evaluating Team Performance

For best results, the team needs to enjoy a coalition kind of operation. All members have a different role but work toward the common goal of satisfying a need given to them by the organization. Thus, there is need for a design team and its leaders to develop the right culture, that of being customer-centric.

It is a general observation that young graduates generate solutions to design problems by leaping into applying a solution framed in commercial-off-the-shelf (COTS) component terms. They heavily align with the bottom-up approach, wherein their newly acquired basket of known items is rummaged through to find a seemingly appropriate response to the current design problem. Their work output may appear to be better than expected because they are able to rapidly identify items.

The more correct approach is to work top-down, starting with a customer need that has been broken down to the point where appropriate "bottom" building blocks are selected. Mature designers will, therefore, follow the top-down path and for this reason often seem to be taking too much time to get to solutions.

The characteristics of the quality of engineering design are covered in more detail in Chapter 5. For now, where we are covering staffing considerations, it is those customer-oriented aspects of a person's career development that are that are of interest. These are now introduced to illustrate the kind of quality attributes to look for in new staff appointments and to work on in team development.

Three key methodologies exist that are related to being customer-centric. They are usually grouped under the following headings:

- Quality processes according to the ISO 9000 standard;
- Quality function deployment (QFD) and the house of quality concept;
- Capability Maturity Models (CMM®).

Each of these requires considerable staff training after completion of academic studies. This training is usually provided by the larger organization when it develops its certification for ISO and the CMM audit. As these schemes have been in place for over a decade, it is to be expected that mature appointees will have experience from previous positions.

When it has not been provided, as in the small to medium company, then it is up to the team leader to decide which elements of these can usefully be applied in their local situation.

In general, the purpose of these exercises is to:

- Clarify the performance level of the team within the whole organization in terms of unified parameters;
- Define the current level of capability to external bodies, such as customers;
- Assist set paths of activities to raise the level of maturity.

### 3.10.2 ISO 9000 International Quality Standard

By the 1990s, organizations gradually accepted the importance of truly seeking to satisfy customers. This may seem to be a trite assertion, but even today it is still possible to identify organizations that let their own internal activities dominate how they service their clients.

Great improvement resulted from the introduction of detailed records for standardized processes of all needed activities. Thinking and emphasis changed from the management of quality to quality management.

At first glance, taking valuable staff time out of project time to set up these recording processes appears to be counterproductive. Deciding what the steps are in performing an activity and then having to constantly make reports as the work is performed is a major overhead that surely must add negative value to the organization's performance! In reality, adoption of quality management methods has led to significant improvement, as explained below.

A U.S. study has reported that adoption of the main quality registration path, via ISO 9000, resulted in improvement of many business factors for 20 top companies [9]:

- On-time deliveries up 4.7%
- Errors reduced by 10.3%
- Cost down 9%
- Customer complaints down 11.6%
- Market share up 13.7%
- Increase in sales per employee up 8.6%

Registration by an organization with the ISO 9000 certification means they have established a framework for going about their operations in a manner that ensures they will meet accepted quality levels for their kind of activity.

Well-organized methods are instituted for determining needs and matching design and production to those needs in a purposeful and recorded manner.

However, successful registration does not guarantee that the right things will be designed, as it is more about doing things right. A top team can still produce failures if given tasks that are not well constructed.

As stated in [9], the ISO 9000 standards have three elements:

1. Say what you are going to do (that is, what process you are going to use), and show that the process meets the standard.
2. Do what you said that you were going to do.
3. Be able to prove that you have done it.

Its process is summed up by the following attitudes [9]:

- If it moves, train it.
- If it does not move, calibrate it.
- If it isn't documented, it does not exist or didn't happen.

Staff need to be aware of the importance of quality certification and be able to adhere to its processes.

### 3.10.3 Quality Function Deployment

The overall quality issue is dealt with under the umbrella of Quality Function Deployment (QFD) [10]. In essence, this ensures a holistic approach is set up for a project, that the necessary interfaces are established to deliver the system or product correctly by hearing the "voice of the customer."

It is easily understood using the much-used "house of quality" analogy. Figure 3.7 shows this house as metaphorical rooms existing under one roof.

Customer needs are compared against engineer's solution and the competitor's factors via a set of matrices. These matrices have weights assigned to the respective matrix coordinates.

The customer's need generates "whats." These are compared against the "how's" of likely solutions that are generated by the design team. The competitor's room yields constraints that impact on the design choices. Once the respective matrices are filled in, they can then be analyzed to find missing information and best paths.

The key reason for the discussion being given here is to prompt questioning to establish whether staff can use these processes to optimize and track design effectiveness. At its root is acceptance of these ideas by the design staff. Quality of design itself is the subject of Chapter 9.

### 3.10.4 The CMM® Concept

Problems in software systems development in the early 1990s led to the development of the Capability Maturity Model (CMM®) approach by the Software Engineering Institute (SEI).

In 1995, the SEI published a variation of its first CMM, the Systems Engineering Capability Maturity Model (SE-CMM). The impact of this CMM was to extend the formalism used for evaluating an organization's software engineering capability out to the wider field of systems engineering at large.

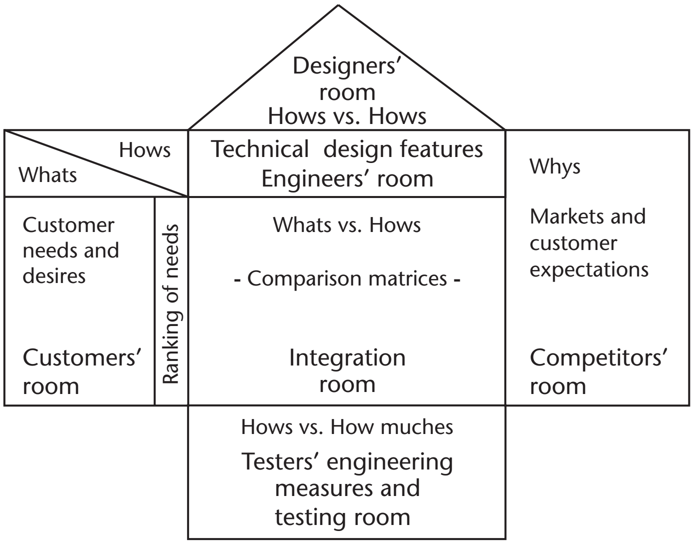


**Figure 3.7** The house of quality is built as rooms for the key players. (*Source*: [9].)

This is similar to the ISO 9000 thrust in that it is about giving a third party a sound indication of the performance of an organization to carry out an activity. Additionally, it allows levels of capability to be assigned.

Initially, CMM® was intended as a tool for an organization to baseline its performance in order to fill in holes and mature its performance to higher levels. It was not constructed to be a mandatory requirement imposed by the customers; but this is what it has become.

CMM is a process for assessing capability at performing. It does not indicate that specific products made by the organization will be suitable; it is a measuring stick for the capability of an organization in its chosen activity. The six attainment levels of the original CMM have been briefly described as [9]:

*Level 1:* Initial level. Ad hoc methods may achieve success through heroic effort; little quality management; no discernable process; nothing to expect other than perhaps the intensity of heroic effort; results are unpredictable.

*Level 2:* Repeatable level. Successes may be repeated for similar applications; thus, a repeatable process is discovered that is measurable against prior efforts.

*Level 3:* Defined level. Claims to have understood, measured, and specified a repeatable process with predictable cost and schedule characteristics.

*Level 4:* Managed maturity level. Comprehensive process measurements enable interactive management.

*Level 5:* Optimization level. Continuous process improvement in place for lasting quality that tracks the best practice.

Many design organizations are still at level 1. The goal is usually level 3, for that satisfies most customers and is seen as a good investment to make. Going higher is very costly for an organization, so few will choose to reach capability higher than level 3.

The systems engineering variation, SE-CMM, has five levels that address the maturity of the SE process:

*Level 1.* Process performed informally.

*Level 2.* Planned and tracked process.

*Level 3.* Well-defined process.

*Level 4.* Quantitatively controlled process.

*Level 5.* Continuously improving process.

Because a single project could easily be using several versions of CMM, a need for integration arose. This led to another wave of activity under the title of CMMI® (I for integration).

Staff cannot be expected to be experts at implementing such schemes, for they are complex and need the support of specialists. However, staff may have been involved in their implementation in prior appointments, bringing a useful asset to their new employer.

## 3.11 Summary

Staffing is the most valuable asset for carrying out effective engineering design. This chapter has dealt with staffing issues of importance to the design team situation that are not covered in texts on general management.

After justifying the need to give staffing issues high attention, the time taken in getting new staff into place and the difficulties of termination started off discussion of a succession of issues that the team member and leader are rarely given training in, yet find themselves having to manage.

Skills needed of a design team, and some pointers for assisting selection of an appropriate new team member, were then discussed.

When a new team, or team member, arrives, they need many kinds of support to assist them in their work. A typical hi-tech start-up example began discussion of that collection of issues.

Staff turnover is a reality that must be faced and plans must be set up to lessen the impact of a member not being available. Lists of important issues were provided for guidance.

Teams members will need to operate in a variety of organizational structures. These were discussed in terms of communications and team efficiency.

It is normal for members of a team, and especially the leader, to be involved in staff appointment processes, in staff selection, and settling new staff into the team environment. Some general background was given.

Staff development and performance assessment are always needed to keep up performance and to assist guide management. Appraisals, fitness reports, and personal development methods were outlined, showing the variety of approaches that are employed.

Today, design teams are required to consistently provide quality outcomes. The main methods used from the design team's staffing perspective were reviewed.

## References

[1] Barrow, P., R. Branson, and D. Storey, *The Best-Laid Business Plans: How to Write Them, How to Pitch Them,* Virgin Publishing, 2001.

[2] Burstiner, I., *The Small Business Handbook*, Prentice Hall, 1992.

[3] Armstrong, M., *Human Resource Management Practice,* Kogan Page Ltd, 2001.

[4] Heller, R., and T. Hindle, *Essential Manager's Manual*, New York: Dorling Kindersley, 1998.

[5] Jackson, T, and E. Jackson, *The New Perfect Resume*, Main Street Books, 1996.

[6] Soat, D. M., *Managing Engineers and Technical Employees: How to Attract, Motivate, and Retain Excellent People*, Artech House: Norwood, MA, 1996.

[7] INCOSE, International Council on Systems Engineering, http://www.incose.org, EMWG pages, 2002.

[8] Pedler, M., J. Burgoyne, and T. Boydell, *A Manager' Guide to Self Development*, McGraw-Hill, 1998.

[9] Sage, A. G., and W. B. Rouse, (eds.), *Handbook of Systems Engineering and Management*, New York: Wiley, 1999.

[10] Blanchard, S. B., and W. J. Fabrycky, *Systems Engineering and Analysis*, (3rd Edition), Upper Saddle River, NJ: Prentice-Hall International Inc., 1998.

## CHAPTER 4

# IT in Support of Design

Staff members need good information technology (IT) systems to perform well. This chapter deals with the IT aspect of the design team's work. It explains:

- What IT is and what it can do;
- Hardware and software used to support the design activity;
- Features of tools;
- Office and management tools;
- Specialized design tool systems;
- Use of the Internet for design team working;
- Key terms.

## 4.1 The IT System of the Design Office

### 4.1.1 Introduction

If the reader is already familiar with IT systems then the early part of this chapter can be skipped. This material is intended to assist those making the transition from the traditional paper-dominated design office to the so-called paperless office environment, to get the best from tools and tool suites, and to explain how a design office introduces tool systems, or moves to the use of centralized intranet or Internet operations.

The Oxford Dictionary defines information technology as: "The study or use of processes (esp. computers, telecommunications, etc.) for storing retrieving, and sending information."

Addressed here is the role of IT in supporting the operations of the engineering design team.

In becoming efficient with this aspect of design activity, there is no substitute for a small amount of formal learning combined with a great deal of keyboard practice. Fortunately, IT methods and techniques can be quite forgiving, with the more easily detected office work errors usually being discovered and corrected.

Becoming proficient with design support IT is best approached from its functionality—by using it to do those things normally done during the design activity. Once the general techniques of file handling and management have become second nature, it becomes increasingly easier to master new applications, because they mostly use the windows concept and relatively similar function commands. Commonly used routine office uses of IT are not covered here.

The complexity of IT systems can be overwhelming. An IT system will perform the following functions for handling and processing information:

- Inputting;
- Processing, including sorting;
- Storing;
- Displaying;
- Printing;
- Recording.

IT is ideal for supporting the engineering design processes over all of the SE life-cycle functions, as is explained in this chapter. Indeed, it is hard to imagine how an office could be efficient without its widespread use.

### 4.1.2 The Computer and Its Peripheral Devices

#### 4.1.2.1 Hardware Parts

The main tool of the modern design office is the ubiquitous personal computer—the PC. (A workstation computer used to be somewhat different than a PC, with that term being used more for intranet-connected PCs because they had different software suites. The distinction has become blurred and "workstation" is becoming the normal term to use for any personal computer.)

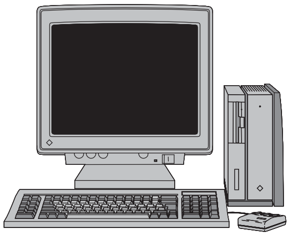
A personal computer, regardless of its builder, uses relatively standard critical specification parameters to describe it.

Figure 4.1 is an example specification extracted from sales store literature from April 2003. While the parameters are stable, the quantitative data will change toward greater performance in as little as 6 months. Figure 4.2 shows how the various parts are assembled to form the stand-alone PC.

The parameters stated in Figure 4.1 are now covered with some hints that may assist selection.

*PC form.* This refers to the case used to hold all of the parts of the computer together. They come as a desktop assembly for placing flat under the monitor unit, or as a standup tower unit that has a smaller footprint on the desk or floor. Some makers integrate the whole into a fashionably styled unit (such as the packaging of some Apple® computer systems).

*Processor.* This is the computational heart of the system. Operating speed is crucial, as this ensures faster file opening and task processing. This speed is being increased continuously, so go for as close to the best as possible at the time of purchase. Avoid the very fastest specification, as the cost increment may not be worth it given that it will become the norm in a matter of months, at a much lower price. The speed given is that of the frequency of the digital clock that paces each step of the binary system onto the next state. Generally, the higher the speed, the faster the operating response time.



Note: Specifications for computers change rapidly!

| Item | Specification |
|---|---|
| Form | Slim desktop |
| Processor | Processor name, 2.0 GHz |
| HDD | 20 GB @ 7,200 rpm |
| RAM | 256 MB DDR |
| LAN | 56K v.90 and 10/100 LAN |
| Video | 32 MB |
| Sound | Maker's name, with turbo |
| CD-ROM | DVD/CDRW combo unit |
| Monitor | 17″ CRT |
| Warranty | 3 years RTB |
| OS (operating system) | WinXP Pro |
| Catalog number | xxxxx.xxxx.xx |
| Price | $xxxxx |
| Rental | $xx/wk |

**Figure 4.1** Typical PC specification.

*HDD (hard disk drive).* This is the main medium for long-term storage. As the computer operates, its data is shuffled between the HDD and the faster but smaller capacity, random access memory (RAM). HDD capacity of the past was rather small and filled rapidly. Today, HDD capacity is not usually critical because large sizes are standard. Go for the highest speed and size, but it might be wise to avoid the very latest offerings as they are much more expensive per unit of storage added. These drives can be upgraded as long as the operating system is able to support expansion in a useful manner.

*RAM.* This is the read/write electronic memory that does the work. It is used to process data shuffled with the HDD. Some applications require an unusually large amount of RAM; it can be upgraded easily and affordably by simply plugging in extra memory chips to a memory board already provided inside the computer case.

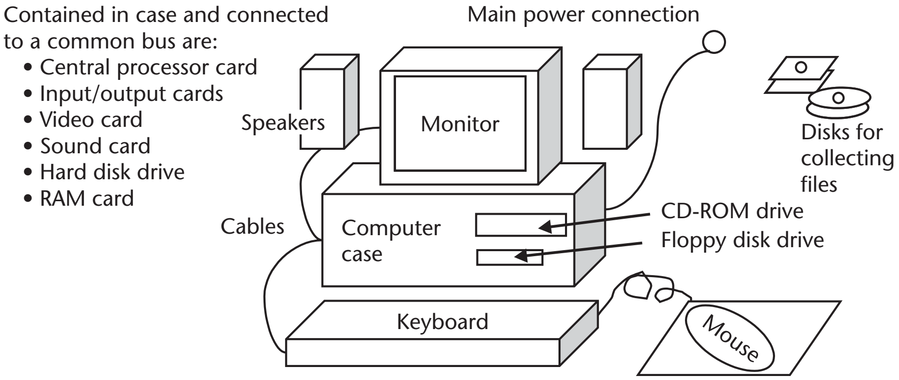


**Figure 4.2** System diagram for a stand-alone PC.

*LAN (local area network).* This facility is necessary for fastest interconnection time between computers. It is not needed for single-person use over a telephone line connection. A card is required to connect a network to a computer. This is added as a credit-card-sized module in laptops. An IEEE Fire-Fox connection port is needed for wireless networking, the current method that is finding wide application. Networking requires some special training to install. In large organizations, a computer systems administrator is usually available to set this up along with password registration needed to protect access to your work from the network. Protected access by use of different individuals can be set up on single PC. Each person can then have secure files and their own desktop icon set up.

*Video.* This is a dedicated circuitry board for driving the video imaging system. Video is reasonably standard but watch for compatibility with unusual video system players and recorders. Most PCs will support playing music CDs by using a virtual player window found in program accessories, but less so for videos unless a DVD drive is fitted.

*Sound.* Another board is required to drive audio systems. Again, these are reasonably standard. Where sophisticated speaker systems are needed it is necessary to check for compatibility with that audio system's characteristics, such as power handling. These come in different audio quality levels.

*Compact disc–read-only memory (CD-ROM).* The CD-ROM drive has generally replaced the floppy diskette drive as the medium for storing and passing files into and out of the computer. DVD drives are now common. Provision of a combo drive (CD-ROM and DVD combined) is becoming standard in laptops. The CD-ROM holds around 700 MB of data compared with 1.2 MB of the earlier floppy diskette. They come in two forms for file handling—read-only (CD-R) and read and/or write (CD-RW). When only one floppy drive is provided, it is possible to add an R/W CD-ROM as an internal or external unit. When image files (40 KB—5 MB each) are involved, a CD-RW drive is essential for file transfer and storage.

*Modem.* These units are used for communicating with other computers over telephone lines and links. They are sometimes fitted as an external box but it is more common for them to now be built in. Modems need the speed capability and must be compatible with the communication medium being used. Typical maximum communication speeds for dial-up connections are:

- Dial-up telephone line: Up to 56 Kbps maximum; check with the telecommunication provider that the local exchange and street cabling are set to allow for the best speed.
- Broadband cable: 6 Mbps.
- Broadband wireless: 11 Mbps.

Broadband communication is slowly being accepted for domestic and small business use, but it is not always available at a location. A company will usually subscribe to an optical fiber link to obtain the speed needed for efficient business use.

*Monitor.* The display monitor is made in one of two technology forms. The older form, stemming back from origins in the 1930s, is the cathode ray tube (CRT) system. This is still the cheapest but it is bulky, not that flat across the screen, and liberates considerable waste heat.

The modern solid-state replacement of the CRT is the plasma flat screen unit. These are thin, have excellent screen properties, and use far less power than the CRT. They are slow to be widely adopted for general PC use because their price is around three times that of the CRT (at the time of writing). These can be expected to replace the CRT monitor unit in future new purchases.

Screen size is measured across the diagonal dimension. The smallest used in desktop units is 14 inches (35 cm), with 15 inches (38 cm) and larger being the basic professional norm. Larger screens are used for situations requiring many large images (CAD applications, for instance) and for multiwindow use. In some computer installations, several display screens may be provided for one computer.

*Warranty.* Computers are generally very reliable. It is their mechanical parts in the disk drives, keyboard, and connectors that can give trouble. Look for a useful warranty that lasts for a sufficient time. However, service contracts can be a waste of money because problems are rare and the cost of return and loss of use time is often excessive. Provision of a support help line by the supplier is good to have, but sometimes the wait time for the call service center can be very long and frustrating, even if it is a free call.

*OS (operating system).* Microsoft Windows® is the industry norm. Use of any other system can leave you out in the cold due to interface problems with applications. MS Windows has gone through many transitions: WIN 95 (not advisable to use now as it is limited and cannot accept some commonly used applications), WIN 98 (still widely used but not able to support many new applications). WIN 2000 was short-lived, and was replaced by WIN XP as the latest generally used OS in professional offices.

Be warned that a user usually takes time to settle into the new functionality when upgrading the operating system. Upgrades of the operating system are a fact of life that occur at around 3- to 5-year periods. Today, WIN XP has automatic, continuous upgrading of its application in place—perhaps lengthening the time to the next upgrade!

The version used (educational, home, or professional) requires careful selection, because some needed features may not be available for a specific user. Licensed use has been tightened up over the years, making it necessary to register use of an application.

*Laptops.* These are a definite requirement for those who need to work in many places. Laptops originally were regarded as less effective than a desktop unit but today they are often the best unit to use. Their specification is now largely the same as a good PC.

Features to consider are the screen size and type, and the system total carrying weight. Screen types can be of the cheaper passive or dearer active kind. The former is hard to see clearly on an angle and is not recommended for use when several people view the display together.

As a laptop has to be carried, its overall weight is obviously of interest. Going for slim cases and low weights can, however, come with other parameters reduced in performance and at a much higher cost. When assessing the carrying weight, do not forget to add in that of the essential accessories needed: the battery charger, additional drives, converter plugs, cables, and possibly a mouse if you prefer not to use the built-in touchpad or force button.

#### 4.1.2.2 Software Parts

Software is always needed to operate and use an electronic computer. New PC systems will usually come with some common software applications. An acceptable office tool suite that covers word processing, spreadsheets, database, e-mail, networking, and diary functions is essential.

Software can be a bargaining point at the time of purchase but take care to get the type really needed. Try to buy a system with most of the basic software already installed. It takes a lot of time to do this and the inexperienced person can make heavy weather of it.

Installation of additional applications and peripherals is usually straightforward. Most applications now provide for plug and play use. Here, connecting most new hardware peripheral devices to a PC system will automatically be recognized and set up ready for use.

There are the times, however, when full installation is needed for peripherals not in the database of the operating system. In such cases, follow the installation instructions given by the CD-ROM, as it takes the user through the steps. If in doubt about the questions posed as it progresses, use the default options. Make sure all applications are closed when loading new software.

Never remove an unwanted application by deleting or dragging its folder into the recycle bin. The Uninstall tool provided must be used. The reason for this is that many applications place their files inside other applications for interactive use; it is all too easy to leave stray or old version files in the system, which can lead to incorrect loading of the new application.

Three main levels of software exist in a computer; they are used in succession to get an application running:

1. *Boot software.* The computer hardware system is set up initially with its own limited amount of permanent memory residing in a silicon chip. This program will boot up (i.e., start) the unit, ready to accept other software programs added from external sources. The action of resetting or rebooting a computer (for instance, when its operation freezes) usually takes it back to this level of program to start it all up again from scratch.
2. *Operating system software.* When the PC is started up, the permanently held machine code program starts up the main operating system. Operating systems today tend to be the Windows® and Unix® systems but there are also many specialized ones. It is the commonness of their use that has allowed third-party software to run on most makers' machines. It has allowed

machines, and other hardware and software of different brands, to communicate with minimal interfacing problems when plugged together.

3. *Application software packages*. Running the operating system permits the starting up of application packages such as the MS Office® suite of software, games, and computer-aided design (CAD) packages.

#### Virus Checker Advice

A virus is a devious program developed by irresponsible people who create files that can enter computer systems to destroy all or part of the computer's functionality (it is a criminal act!). An absolutely essential application to have, from the first time the system is run, is a good computer virus detector, barrier, and cleanup tool. A single, once-only installed virus detection tool gives some protection but it is not sufficient. New viruses appear at daily intervals! When a virus gets into the computer system, it can take days of work by expert technicians to clean it out without destroying existing files, and to reload your applications, which are often not at hand. Usually many files will have to be deleted, and thus lost.

Viruses can certainly be avoided by never accepting files from other sources on disks or from incoming e-mail and Internet, but this is rarely a workable way to use a computer.

A virus detection tool alerts the user via a notice to indicate a virus has been detected and corrected, or instructs the user to go to the file and delete it. Viruses are mostly held in attachments to e-mail messages and go about their destructive work only when opened. Consequently, never open a file from a suspect source, or if the virus checker advises that the file is infected. When a file is suspect, immediately delete it from the attachment folder of the e-mail system. Do not forget to empty the recycle bin, because a deleted file is usually held there until the bin is emptied. Again, DO NOT OPEN IT!

Some viruses sit on the server, not your machine. They appear to be in your machine when connected but they cannot be found. They can be deleted with special knowledge.

Virus checker applications are best purchased as an annual subscription service that initially provides a full version of the application. Update files are added when the maker issues them, by downloading them automatically or when prompted to do so by an e-mail message. Installation of upgrades takes only few minutes. A good checker can upgrade at around two to three times a week!

### 4.1.3 Linking Computers

It is essential to be able to pass data files to other users and to receive data and messages. One way to do this is to save the file on a suitable portable storage medium, such as a floppy diskette or CD-ROM, loading it into the next machine that is running the same application.

A more efficient way is to get the computers to communicate together. For fastest operation, connect them to the same computer digital communication "bus."

Where the computers are too far from each other to make direct computer-to-computer bus linking practical, or when there is only the occasional need to communicate, they can be connected via some form of communication medium. This can be a copper wire telephone line, coaxial cable, fiber-optic cable, or a wireless channel.

File transfer between users is easy using e-mail attachments over links, but this method is limited to file sizes of some 2 to 3 MB maximum for the lower speed telephone links.

The Internet—the Web—is a vast system of interconnected computers that allows a user of any kind of computer to connect to any other in the network to read or use its data. Figure 4.3 shows part of a networked system of users. Intranets are fast links using dedicated local area links of similar architecture to this.

While the basic ways of using any computer system are much the same, there is always a strong and vigorous element of change associated with use. The concept of how it all works remains much the same, but the basic computing processor, operating system, applications, networking speed, range of tools available, and connected peripherals all have a limited useful professional life of 3 to 4 years. They do not wear out as such but become inferior in performance, or run out of sufficient compatibility with applications and peripherals.

The modern IT-based design office cannot avoid the need to spend a considerable amount of time and money upgrading systems to keep up with best practice. Upgrading can be avoided for only so long. Messaging will have problems handling files coming from more modern applications, new applications will not load properly for lack of sufficient storage space, image storage will run out, the slow speed of general operation will become irritating, and so on. It is clear when an upgrade is due!

When considering an upgrade, little of the current machine will be reusable, so buying new machines is the only way to go. Proceed with installation of new software, and even more so upgrades, with great caution lest the task lead to a system failure that can take days to unravel.

The secure way to upgrade PC capability is to set up another, newer, computer from scratch. Load in the new operating system. Check it out. Then load in the main application suites. Set up the Internet and networking applications.

When that all seems to be settled and operating properly, progressively transfer files across from the older unit using a CD-ROM. Make sure the new system still

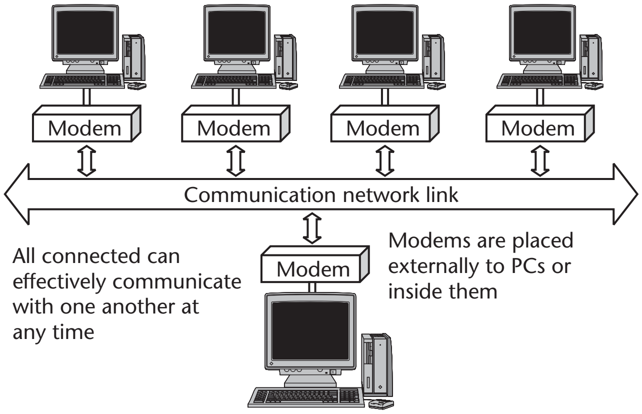


**Figure 4.3** System diagram for a PC working in a distributed bus network.

works as each application is added. Keep the older unit operational until it is clear that everything is operating properly on the new machine.

For security reasons, clean out the old machine's HDD before it is passed on. Wiping files into the desktop recycle bin and deleting them does not necessarily delete them from the HDD. Skilled technicians can recover them! To be sure it is clear, reformat the hard drive(s).

### 4.1.4 Getting Started

Getting started with a PC can be a tough, especially if you are new to computers. If this is the case, then do not try to set it up yourself for it will be most frustrating and you will usually still need assistance.

Once operating, it is a matter of gaining sound "flying hours," so be prepared to make mistakes that take time to correct. One learns much when making mistakes because it takes the user over paths not normally traversed.

There will always be a situation when a ridiculously simple problem stumps you. Finding the truly real "expert" is often difficult, for those with lots of experience (but not enough for your problem) will usually rise to the challenge—on your expensively paid time!

As already suggested, go for a computer specification that is near but not at the highest level available. Set budgets to replace the computer system at intervals of 2 to 3 years. Upgrading key components can be helpful but there is usually no business case for a full upgrade compared with purchasing a new system.

It used to be that software was chosen first and then a computer obtained to run it. Due to their wide acceptance, PCs are reasonably standard these days, and thus all software can reasonably be expected to run on one. Make sure it has the connections and hardware elements needed.

Most PC system suppliers will build specials to order using building blocks from a catalog. Be aware of the possible malpractice of reusing secondhand parts in so-called new PCs.

Look out for the right kind of connections available. Universal serial bus (USB) connections are now common but many of the older peripherals cannot use them, meaning a new machine may also need some new hardware items.

It is advisable to "stick with the crowd" when selecting systems. Being out on a limb through use of an unusual PC or software system can give rise to significant problems of support. If the system is special then be prepared to pay dearly for sound, fast, and reliable support. When estimating the cost of computer support, make allowances for designer time if PC support is not part of the budget.

When several people are to have new systems or major software changes, it is necessary to provide training and job release time for them to become familiar with the changes. It can take from hours to months for staff to master new systems.

A necessary need is access to a help-desk service that is immediately available for use when things go wrong. Even with such help, it may take lots of time to recover a situation.

To minimize downtime, be sure to maintain sound and reliable archives of key data files and applications on separate storage media. Rapid access to a second machine will allow the current task to be carried on from the archive files while the other machine is being fixed.

When calling on a help desk about connection and Internet problems, use a separate phone line for the spoken link so that the PC can be run and toggles changed as the help technician suggests.

Help advice can be obtained, via e-mail, Web connection or telephone, or from within the PC software, through the following sources:

- PC supplier's phone line or Web site.
- Peripherals supplier's phone lines or Web site.
- ISP phone line.
- Tool vendor's phone lines or Web site.
- Company IT mentors, tool support staff, and computer administrator.
- Company general help-desk line.
- Chat rooms on the Internet.
- Other team members.
- Within the operating system software.
- Within the application.
- Hard copy manuals, which are usually copies of the computer help function, but are harder to use as they cannot be searched or show on-screen walkthroughs for selected functions. They are becoming less commonly available because they are expensive to provide, bulky, and harder to use than e-file forms.
- Texts, which are available at all levels of complexity. The larger volumes covering specific applications will provide much deeper knowledge and knowledge that is not always given in the software version of the help function. Mainstream book and computer stores usually have many books and CDs to offer (see comments on books in the reference list).

## 4.2 Tool Features

### 4.2.1 What the Designer Does with a PC

IT activities make most effective use of tools to perform tasks that involve working on data. An example is the now very sophisticated word-processing tool that makes the task of writing and wordsmithing easy and far more efficient than by the traditional manner.

The designer's most basic tools are paper, a ruler, pencil, printed tables, drawings, and a pocket calculator. When tackling a design, that basic capability is extended using tools for such aspects as:

- System concept development;
- Requirements extraction;
- Architecture generation;

- Functionality charting;
- Behavior characterization;
- Board layout for electronic systems;
- Circuit simulation.

Providing appropriate computer-based design tools allows those functions to be combined with respect to:

- Logical considerations;
- Structural integrity;
- Traceability of activities and paths taken;
- Calculation, where needed;
- Visualization through interfaces;
- Database handling of interrelated information;
- Simulation of performance;
- Speed of operation, and slowing down or speeding up of simulations;
- Reporting outcomes of design detail, simulations, and decisions taken.

Members of the design team, via their own computers, will often have their work integrated with that of their colleagues to form a cohesive system development.

Computer tools sometimes appear to possess intelligence but at their current state of development they are only a means for performing well-defined, routine, trivial tasks. It is still the human engineer's brains and actions that add the greatest value by providing the thinking process, intelligence, innovation, and cunning needed to carry out effective design.

Tools assist those activities where human methods are slower or less capable than a computer can be. Computers are slaves for reliably doing routine hackwork. They are especially good at checking logical things; searching; sorting; indexing; and archiving; and in showing things such as images and text.

Figure 4.4 shows some of the many classes of tools that are available in support of the systems engineering aspect of a development. Figure 4.5 gives a similar diagram for tools used in electronic systems design.

Let us now explore the main reasons for using CAD tools.

Most important is that CAD tools can save time if put to the right uses, such as number crunching, and searching and sorting files, words, and strings or symbols.

Next, they can be error minimizing in operation. Much of the routine operational parts of the design process can be automated, helping to ensure that essential issues are addressed.

Rekeying data such as lists and text is much less error-prone by copying and pasting. When many kinds of keying errors arise—those not involving semantics—the user will usually know because the computer generates error messages and warning sounds.

Humans have poor memories for exact things; computers, however, are very exact in their operations. Design capability is enhanced by the rapid pace and automatic aspects of computing applications. They facilitate tool integration across

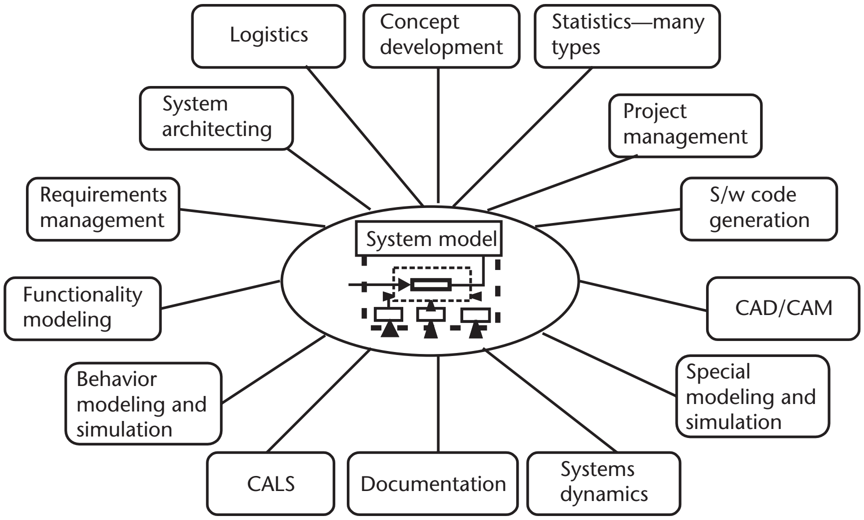


**Figure 4.4** Systems engineering tools.

large team activity and enable concurrent engineering practices to be used via centralized intranet and Internet operations.

Tools can be classed according to their main use. Some support the modeling of a system through the generation of coherent, executable models. Others are concerned with system integration and management of requirements and specifications, including interface specification.

In simulation tools, they can be used to evaluate the function and behavior of man-in-loop (MIL) and hardware-in-loop (HIL) developments well before parts

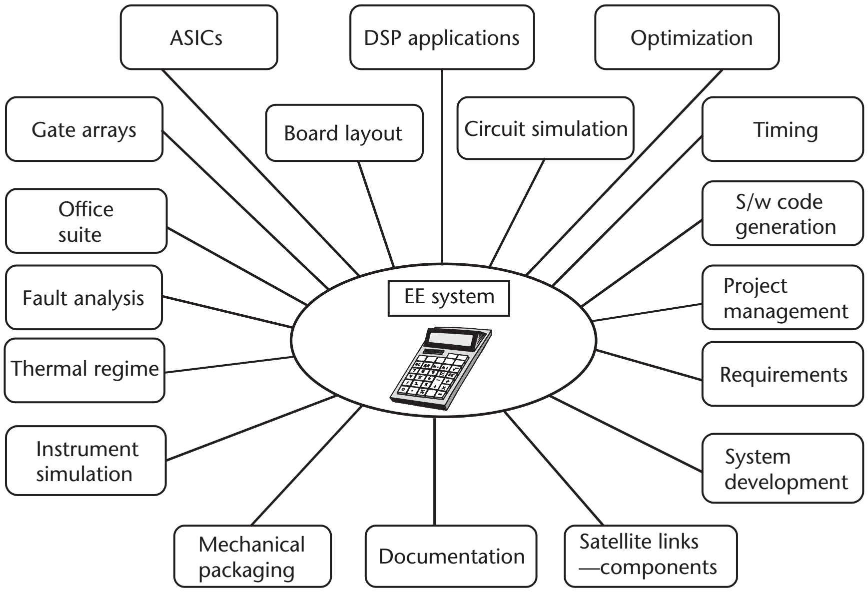


**Figure 4.5** Electrical engineering design tools.

need to be manufactured. In HIL applications, the model representing the design gradually transforms into the real system as the design work progresses.

Some areas of design activity that are well supported by CAD tools are system functional architecture, system behavior, requirements management, integration, software code generation, database management, office and administrative tasks, plus a host of special purpose functions.

The heart of a tool is the metaphysical model contained within its structure; this represents the design function it supports. An example of a tool model is a fault tree for a safety aspect of a design that has been set up in a database. This might be embedded into a spreadsheet within its grid of cells, their operations for manipulating the cell data having been set up to operate in a dynamic manner. In design exploration iteration, the tool user changes variables in the model to carry out "what-if" investigations (design analysis), observing the outcomes.

In order to get fast and correct uptake by new users, the design model in a tool must be easily and readily understood. The best way to learn about the capability of an unfamiliar tool is to use it to support successively complex designing functions.

No tool seems to give all the functions a project might need; but many a vendor will suggest theirs does. Major tools take from weeks to months to select, install, and train staff in their use.

Tool vendors have developed requirements tools in virtual isolation of each other. There has been no one-time research and development (R&D) project to decide a consensus of requirements. Their kernel model has usually started out as a good idea of an experienced practitioner, embedding that working experience of the situation. These tools have settled to offer similar functions that do not always operate in the same way or use the same terms. Expensive and time-consuming additions of considerable amounts of extra software code are often needed to interface them to existing customer systems packages. Selection of these tools need careful study. Some features to consider are:

- Number of requirements that can be accommodated;
- Interfacing to other tools feeding from their outputs;
- Networking operations;
- Software code used;
- Computing platform needed;
- Long-term availability of support for tool;
- Ease of input, file handling, and report preparation;
- Analysis support available;
- Database type;
- History of development and application;
- Type of graphical interfaces provided;
- Archiving methods;
- How its traceability works.

Tool use requires wise and sound research of their capability statements.

### 4.2.2 Tool Characteristics

Clever development of tools can make them into killer applications (i.e., those that are just so right to use, and give such powerful performance, that all other alternatives seem puny in comparison).

The data structure reveals a lot about how a tool is built and operates. A key parameter is the representational schema used—the model. Explore this in terms of human factors as well as a theoretical formal description. Does the user see easily how it is built and operates? Does it have a commonly used modern appearance, and operation? How does it get data to and from other systems?

Critical features to consider for a tool are outlined below.

*Functionality.* When selecting a tool, this relates to its usefulness. Ask the question, "What is it intended to do to add value to a design operation?" Functionality covers the use needs and defines the functions that are provided. These are expressed in terms of word descriptions and mockup demonstrations of the functionality required or supplied.

Communicating required functionality can be difficult if the features are new to the field. When investigating new situations, an existing tool can be used as a baseline specification from which to prepare a statement about the additional functions needed. Analogous functions in other tools can be used to illustrate a need.

It is also important to ensure tools will provide the data and formats needed for related aspects of design to which they contribute. All functions should link into other applications in a traceable manner. If not, serious misfit errors can arise, with often very expensive, late-error remediation rework being needed.

*Behavior.* This pertains to the way by which the functions are carried out. Tool suppliers usually provide educational demonstrations and animated tutorials to show this. When evaluating tools, ensure that they follow existing norms of tool operation as that provides "fast to learn" tools, an essential feature for successful adoption. Timing and speed of execution need to be checked out by exploring the operation through use of carefully crafted test simulations that adequately exercise the tool.

Getting a tool to work in an integrated manner can depend on whether it has good interfacing characteristics. Many early tools, and still some specialized ones today, need middleware to get compatibility. Setting up these transformation interfaces takes considerable effort, especially if there is need for software code to be generated.

Tool vendors get lots of business setting up interfaces! Watch out for unwanted emergent properties as tools are interfaced. New mixes of yet unconnected systems are likely to do unexpected things when a new system of systems is formed—for good or bad!

*Requirements handling.* The basic management function in any design project is how well it supports the handling of its requirements.

Some questions to ask about tools are:

- Are all requirements needed for the task listed?

- Is each requirement linked to a stated functionality?
- Is the linkage coherent?
- Does it have traceability from requirement right through to a test?

Key functions then become clear:

- Does it make the task easier to do than without it? (This may appear to be an obvious thing to ask but some tools actually add negative value.)
- Are operational mistakes hard to make when using it?
- Does it archive and update data changes automatically and accurately?

*Code generation.* Another function of many tools is the generation of computer software code for such items as:

- To extend its capability (e.g., macros for spreadsheet-type tools);
- Simulation modules (e.g., setting up a model to investigate a control situation);
- System operating software (e.g., installing a feature);
- Operational needs (e.g., carrying out a disk management procedure).

*Model representation.* This is how the design model is internally represented in the tool. Is it easy to work out? Has it been externalized in reports or in the application? For example, a decision-making tool may seem to do a fine job but if it does not reveal the computational methods used internally, the results must be used with caution because the way the decision matrix is calculated can greatly change the result. Tools used in safety assessments must be verified for every step they take. For this reason, safety projects may chose to develop their own tools; a proprietary one could well be creating a fault condition within its operation.

Examples of model representation are:

- Hierarchy in a tree structure;
- Causal chain of events triggered by other events;
- State machine;
- Hyperlinked text.

It is necessary to know which is used, because in design data transfer between tools, differences in representation can lead to serious design error that is not detected early.

*User interfacing.* A good interface is needed for a tool as that affects how well it can be used. Windows-based working is now very common and users are usually experienced enough to know what to look for. The structure of the tool operation is represented using buttons, block diagrams, pictures, and charts. The design engineer controls the design model layout in this form and is working, importantly, in much the same way as he or she is mentally imaging the task at hand.

Text-based interfaces are sometimes needed in applications but it is hard to use large sets of numbers in tables. Images presented in terms of charts, histograms, trend curves, and the like are often a better method of communicating overall information.

*External interfacing.* This concerns how the tool has access to giving and receiving data for related tools. Although this is a major issue in tool use, it is still often very limited. Some tools provide no external data path, relying on provision of report files and hard copy printouts to make the link. Some provide only an import interface. Tool selection or purchase should address this feature, not only from the point of view of current use, but also from how the tool might need to be integrated at a later date.

### 4.2.3 Control of Tool Use

If design aspects are undertaken using different tools, the resulting design data will not always interface correctly when parts of the design are integrated. If tool use is within a relatively small project, those involved will usually be able to cope with any errors arising and correct them en route.

If, however, the project has many people involved, especially with subcontractors, then tight control of tool types and versions is absolutely essential for efficient development. Failure to set up project policies and standards for tools can all too easily result in considerable and very costly late design errors. It can take 3 to 4 years for such errors to finally show up in a systems development!

A tight support tool control system will:

- Have a tool policy in place covering what applications are allowed, how they will be added, and who will support them;
- Have written or adopted recorded standards for connection, operation, and integration of tools;
- Allow use of only approved, tested, and certified tools;
- Provide support to users through appointment of tutors chosen from staff who are using the tool in a major way;
- Set up an approval process for adoption of additional tools;
- Provide tool software from a centrally controlled software files library;
- Make available, on demand, support for use information;
- Control the versions and their introduction;
- Allocate adequate archiving and server file space;
- Set up training for design staff and others using the system.

The detail of integrated tool systems can be valuable IP to a commercial enterprise, so information on their experiences is not readily made available to other organizations. Information is available from the Develop New Products (DNP) system of the Jet Propulsion Laboratories (JPL). This integrated tool system was set up around 1999 to support 40 or so space projects. It covers all stages of the SE life cycle as an almost fully integrated tool system.

Vendors also offer integrated suites that are customized as needed. They can show how a development process can be created and are able to assist in setting up a new tool system. Tool suites may also include an enterprise process improvement package that tracks and extracts the performance data needed for that task.

Staff will not all easily accept tight tool-use control, for it tends to slow up the short-term needs of a designer and imposes an initially unproductive learning load. Careful introduction is needed to have the system accepted with the least difficulty.

## 4.3 Major Software Tools Used

### 4.3.1 Office Tools

All computer use in a design office will need general office operating functions. Integrated sets are needed. Microsoft® Office is the most used, but certainly not the only one available. Ensure that any new system addition is compatible with the existing office norm.

Functions usually needed are (with some example product trade names given in brackets):

- Word processing (Word, WordPerfect);
- Spreadsheet operations (Excel, Lotus);
- Database (Access, Perfect Filer);
- Presentations (PowerPoint, CorelDraw, etc.);
- E-mail (Outlook Express, Eudora);
- Internet browser (MS Internet Explorer, Netscape);
- Virus protection (Vet, Norton);
- Personal diary (Outlook);
- Help files (at operating system and application level);
- File handling and structural visualization (Explorers, etc.);
- Peripheral drivers.

Also useful are the additional support functions that are applied to all of the above, such as:

- Drawing, using binary input commands (i.e., each keystroke or two makes a change to a diagram being drawn);
- Spell checking, with choice of spoken language and version of that language available on selection;
- Grammar checking, with choice of spoken language and version, such as English in U.S. or U.K. forms.

A wide range of books is available ranging from the simplistic to the most complex (see the reference list). Support help sources are covered in Section 4.1.4.

### 4.3.2 Management Tools

A wide range of tools that support all manner of managerial tasks for project activity is available.

MS Outlook®, for example, includes a personal diary system that allows members of a team to view permitted parts of the diary entries of others and to propose a meeting time to the team. These work well for people who are permanently interconnected, as by a company intranet. They are less useful for those connected by the external Internet, for response times can then be long and uncertain.

Groupware is a tool system concept that facilitates communication, coordination, and cooperation. It combines the power of e-mail, word processing, the database, the diary, time planners, and more. With this system, staff can keep in communication in an efficient manner. It is an extension of normal e-mail services, providing proformas for all manner of things, such as a notice of meetings and minutes. It can track actions and prompt their completion.

A range of groupware products exist. Lotus Notes®, for example, provides e-mail, message tracking in terms of events and documents needed. Their Web site states that:

> It is an information manager software tool for workgroups. People can share information across a computer network even if those people are in different parts of the world. It can collect information from a variety of sources and store text, tables and graphics. It organizes this information in a database so everyone can quickly find what they need.

The concept of groupware is sound but unless the full organization uses it, problems can arise with connection to other systems and from users not sticking to the rules. It can also be overly good at never letting an action item be overlooked; practical operations need a certain amount of inbuilt "action attenuation," for in the heat of meetings it is all too easy to set up tasks that are later realized to be unnecessary.

Real-time meetings can also be set up using the Internet by groupware products such as Netmeet® and Facilitate®.

To manage the scheduling of small projects, tools such as MS Project® fit the bill. These are based on PERT charting techniques. Once the tasks are named and times to complete and sequence have been entered into the tool's management interface, it can create the overall flow chart, calculate the critical paths, and support various kinds of scheduling analyses and reporting needs.

It is possible to make use of spreadsheets to sequence events and carry out tasks. These also enable a model of the process to be set up to carry out "what if" investigations.

In fact, spreadsheets can be set up to perform numerous design support functions. They tend to be used so much because they are very familiar tools.

It is frequently observed that engineers often go down the path of building their own tools instead of taking time to find out what is already available. This can often be counterproductive, for they are not making use of the extensive inherited experience and application development offered in proprietary tools. The cost to purchase and time taken to become proficient with an off-the-shelf tool must, however, be weighed against the pragmatic needs of the project to hand.

Where the need for a given task is clearly repetitive in operation, serious adoption of tools is supported. Continuing to use old, primitive, and naïve ways for routine operations is a certain way to be permanently left behind in market competition.

Tools, appropriately selected and used, definitely lead to improved efficiency but need time to select and master.

## 4.4 Specialized Software Tools

### 4.4.1 CAD/CAE Systems

Today, most engineering design is done using a range of computer-assisted tools. This began with the use of primitive electronic computers to support the routine operations needed in engineering drafting (i.e., the line-drawing process; hence the original name of computer-assisted drafting, which was also called CAD).

To this foundation were added libraries of design data, a calculator, models for tolerancing part sizes linked to dimensional standards information, part lists, plus extension out from the two-dimensional (2-D), three-view projections of traditional engineering drawings into other ways of visualizing form and shape. Such tools then became worthy of the more modern term computer-aided design (CAD). Progress has been relentless in this field and is not expected to slow [1].

Sophisticated engineering design tool suites can now cover the following stages of a development:

- Sketching;
- Idea development and innovation management;
- Decision-making support;
- Concept development with bubble charts and the like;
- Requirements extraction and management;
- Detailed systems and component modeling in 2-D and 3-D as both wire-frame stick and solid, rapidly rotating, graphics imaging;
- Materials and stress optimization based on analytical and finite element methods (FEM/FEA) of analysis;
- Parts lists and parts data;
- Manufacturing detail, including automatic tolerancing of parts sizes;
- Preparation of assembly drawings and exploded views;
- Environmental grading of a system to International Electrotechnical Commision (IEC) standardized methods;
- Preparation of CNC programs for materials handling, machining, joining, placing, setting, and inspection;
- Painting spray head routing;
- Assembly management;
- Technical handbooks;
- Reports and more.

Tool systems, with equally as great sophistication, are available to support the electronic development activity (EDA) of electronic systems.

With sufficient investment and learning time, tool suites can now be integrated into a relatively seamless, key-only-once system.

Special input and output devices are available such as large screen and multiple displays, large bed-sized plotters, and laser-based prototype maker units that transform the inner areas of a tank of special liquid into a solid part for "rapid prototyping." The list of available computer-based tools is endless. Figure 4.6 shows the many kinds of functions that can be now be supported with computer-aided tools.

### 4.4.2 Tool Directories

Finding out what tools are available to suit a specific need is not that easy. A good start is to use Internet searches based on one or more of the following generic search approaches:

- Functionality needed (e.g., an event-planning tool);
- Principle used (e.g., Monte Carlo simulations);
- Product name (e.g., Stella®);
- Application kind (e.g., gate array design);
- Field of use (e.g., electronic engineering system design);
- Trades study of a "suitable wording" (e.g., trade study of gate array tools).

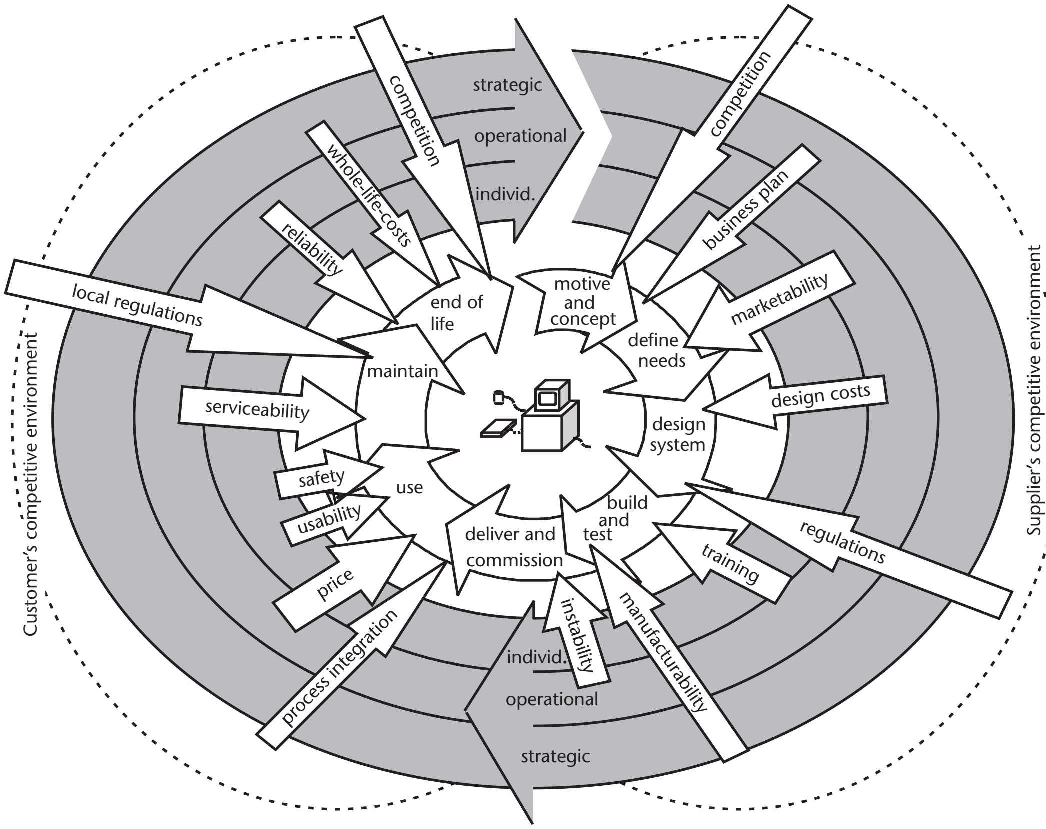


**Figure 4.6** Complex design issues needed in production have tool support.

When available, make use of tool databases to locate needed tools. One of the largest studies of tools relevant to engineering development and design is that of the International Conference on Systems Engineering (INCOSE) [2].

This database of several hundred tools is openly available and can be searched on the basis of:

- Taxonomies of the life cycle, as published by three leading SE organizations;
- Name of tool;
- Vendor.

Tools located there are linked to their vendor's Web site for procurement of more information.

Vendors usually offer a range of assistance for learning what their applications can do. A good start is to download any tutorials they offer from their Web sites, or try out limited versions of applications. When the need is serious and large enough, vendors will often provide on-site demonstrations, and perhaps free entry to regular training courses for their products.

Before using a demonstration, set up a list of what is needed; this assists crisper understanding of the capabilities offered. Considerable effort is needed to properly evaluate a complex tool suite.

Surveys are also available in the INCOSE databases that compare the functionality of given tools.

Bearing in mind the vendor is after a sale, it is always a matter of ensuring the information offered is verifiable. In the tool study situation, it is easy to misinterpret each other's meanings when both are learning about the opposite's situation. Tool vendors seem, unfairly, to be the brunt of overly negative jokes about their honesty on what their products can do. The simple fact is that many companies operate their tools and without vendors there would be fewer tools and less inheritance of know-how. As with any purchase, the buyer needs to be smart about the need and apply quality thinking and research on what is needed as negotiations proceed. The INCOSE database is aimed at SE needs and does not cover manufacturing stages that well.

Queens University in Canada maintains another major tool database [3]. It covers, in the main, computer-assisted software engineering (CASE) tools and lists information on over 1,000 tools from 300 vendors and research groups.

Internet searches will reveal hundreds of suppliers of tools.

## 4.5 Internet Application and Other On-Line Operations

### 4.5.1 Centralized Internet Working

The Internet needs little introduction in its personal use form: it is ubiquitous for finding information, conducting business, and making purchases. Less known is its usefulness in supporting projects where the team members are not colocated [4–6]. This section gives an outline of that aspect.

When several people are involved in a project they start to trip over each other's actions if they need to use electronic means of design. For example, consider a database used by several people to add and change information as a common activity. If the database is held on one person's PC then each must wait until the current user has finished a change before they can have access. If they are close together, this can work by going to the PC in turn. This is fine for operating, say, the catalog of a small library, or a parts store listing but it is not satisfactory where dynamic interactions are needed.

If users are situated at a distance from each other, each person has to send data to the database user to insert. They also have to ask for the latest data to be sent to them when they need it. This approach slows to being unworkable as the project size grows.

The obvious way forward is to network them with a LAN or other network solution. Project information of common need is then held in a central PC server unit. Users access the information through their intranet connection.

The computer system multiplexes user operations to avoid clashes. To the user it seems that they are the sole person on the server—until the system demands a large number of simultaneous users, in which case operation slows down.

This methodology is now in widespread use by commercial companies. Banking, telephone accounts, airlines, travel, and the like use this centralized methodology over the Internet. As an example, a major international software developer manages globally located development teams this way.

Many tool products are available to support this kind of cooperative working. Figure 4.7 show an illustrative system diagram for central operation. It lists, in three groups, the many kinds of activities that can be handled centrally.

For this to work well in a fast-changing, multiperson development, organizations need to have wideband access services available.

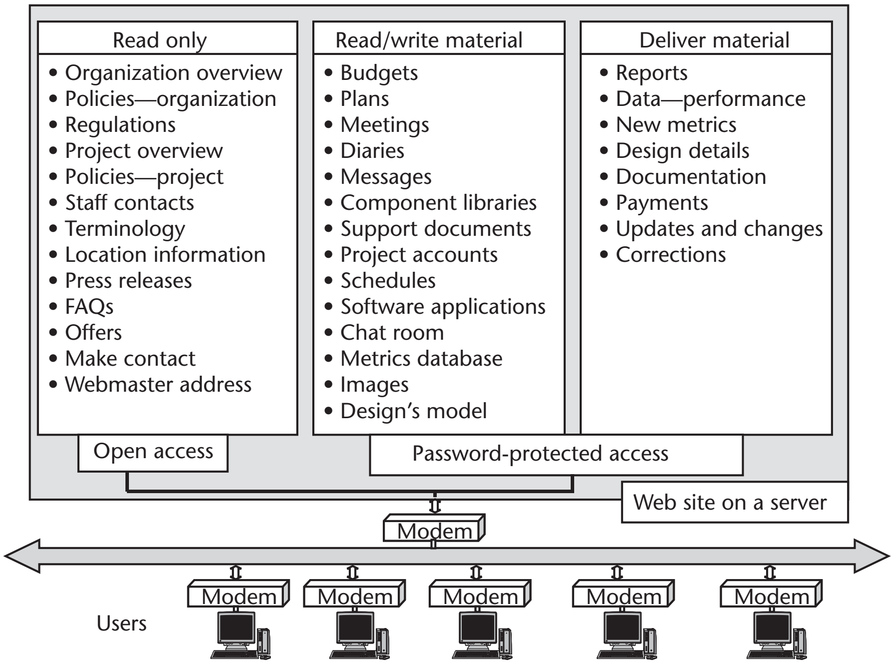


**Figure 4.7** Illustrative system diagram for central Internet operation.

### 4.5.2 On-Line Web Working by Detailed Design Teams

The center of this collective operation will be a major relational database, plus files of the Web and the necessary interfaces. Such systems need to be built by expert Web-site builders with this kind of experience. As users call for information, the necessary data is pulled out of the central server database and compiled into the forms of report needed for transmission to connected users. Users can also feed data into the system from their "outstation."

The following list gives some of the main design domain items that can be delivered to users from a central support Web site:

- Policies;
- Staff conditions;
- Heath and safety documents;
- Proformas;
- Software;
- Records;
- Design and company standards;
- Application notes and other design information;
- Databases and libraries of engineering design information;
- Budgets;
- Accounts;
- Staff contact lists;
- E-mail message storage and use;
- Terms and dictionaries;
- Meeting notices and records;
- Schedules;
- Inventories and delivery details;
- Staff availability;
- Visually inspecting other locations, as in area security or machine operation.

Internet sites can be developed using relatively easy-to-use Web-site building tools such as Dreamweaver®. However, major sites are built at the code level to get the optimum usefulness out the service. Office tools contain tools supporting Web site use.

Updating data on a Web site is relatively easy provided information is held in separate stand-alone files. Given that users have access permission and a simple uploading tool, the old file can be replaced with the updated one as an uploaded file transfer.

Dropout, downtime, and loss of data for phone line connected systems are relatively rare events today but they can still be frustrating. Data can become corrupted in transmission due to coding and decoding incompatibilities. Comparisons are using fax or phone communications are sometimes needed to confirm that subtle differences are not happening to formats by the transmission system.

Uploading files to a central location using file transfer protocol (FTP) is more likely to be error-free than are files sent as e-mail attachments.

Setting up a Web site based operation needs care in its design. Its functionality and behavior are critical design features. Get these wrong and users, who expect excellence in operation, will soon be ignoring the site. For example, when the author was investigating sites for finding how to locate, learn about, and purchase engineering components, two extremes of suitability were experienced. One was a joy to use in that every keystroke and page that was downloaded was adding considerable value to the pathway to a good solution—that need came easily and efficiently.

The other site needed numerous keystrokes and long waits for screens to fill. with each stage making little progress toward an outcome. It was so irritating that is was easy to give up on the search.

### 4.5.3 The Virtual Office Mode of Working

The so-called paperless office has been put forward as the ideal for some years now. Replacing the mountain of records and communications that are on paper should save major amounts of storage space, allow easy access to materials, and let document and design reuse become a normal practice. The ideal is to remove all need for hard copy paper in the office and project. Some projects and administration systems have almost achieved the paperless goal. Advantages are clear. However, good reasons exist for using paper.

One reason is that of legal requirement. Officially binding legal documents are still only generally recognized in hard copy form with an original signature. Widespread use of a legally accepted electronic signature is far from common practice. Thus, many documents of a design development must still be held in paper form.

Users often find the printed form more useful than looking at a screen. PCs cannot be provided to everyone at meetings, or be fast enough in supporting all kinds of meeting activity. Mathematics needs very large screens to show the detail of equations. When using e-files it is often necessary to browse several files at once; hard copy is still better for that need.

Many computer users still have to make the transition to using e-file information alone. It requires a certain amount of self-discipline to make this change and that takes time to become routine. Here, project leaders need to be patient with staff and to appreciate the human issues and forces at work.

Virtual working; that is, where the staff members are not colocated, becomes possible where the electronic office is available. At first sight the benefits of working this way, as and when it is needed, are very clear. These are:

- Work almost anywhere;
- Save travel time to work;
- Work in pleasant circumstances, like at home or at meetings;
- Take the work to the application;
- Do the information part of the job as matters proceed;
- Office site overheads are greatly reduced;

Those who work in a virtual office environment soon learn it has its downsides:

- Work done that way is often less appreciated by senior staff;

- Valuable person-to-person interaction in decision making is lost;
- Social interaction is missing and that can allow relationships and group politics to suffer;
- Numerous distractions from work;
- Work effort is not easy to measure;
- Work effort may not be so easy to manage;
- Valuable records may not be made properly, or at all;
- Information of value to others may reside on a virtual worker's computer that may not be available when needed.

On balance, virtual working needs careful evaluation to ascertain that it is at least as effective as conventional colocated office methods. In sophisticated design situations, colocation of design staff is still much preferred.

## 4.6 Some IT Jargon

For ready reference, here are a few terms that are commonly encountered.

*Application.* General name given to a software program used in a computer to carry out a specific task. Examples include word processors and office suites of various kinds of applications bundled together and integrated to work between each other.

*Browser.* Software application for using the Internet. It supplies the means to download material from the Internet, organize connecting files for rapid recall, and support searches of the Internet's millions of computers using externally provided search services. It does not make the actual connection but will connect to a modem to do that function. Examples include Netscape® and Internet Explorer®.

*File.* The electronic data file that represents its subject in digital data form. A computer will easily have 10,000 to 20,000 of these files when in full operating state for normal office use. Examples include file of a letter, a spreadsheet table, and files forming an application.

*Groupware.* Software application enabling team members to communicate and also use information stored in databases. Examples include Lotus Notes®.

*Hard copy.* Paper record form of information. Examples include photocopied or typed pages.

*Hardware.* Physical parts and units of IT systems. Examples include disk drive and display units.

*Middleware.* This is a special software and/or hardware system placed between two computer systems or programs to make their operations compatible. These are specialized and are often need to be custom-made in nature.

*Operating system.* The software program used to make the computer work. Examples include Windows® 98.

*Plug and play.* Way of operating IT systems whereby a new piece of hardware or software application can be added to a computer system with most of the installation task being hidden and automated.

*Public domain software.* Software available for anyone to use, usually downloaded from a Web site or provided on free CD-ROM. Examples include Adobe® .pdf file page reader.

*Shareware.* Software that is made available for shared use, usually for no charge. Examples include Eudora® e-mail application or Adobe® readers for .pdf file documents.

*Soft copy.* Information in its electronic file form. Examples include the file of a document formed in a word processor on a hard disk unit and placed in a portable medium such as a floppy diskette or a CD-ROM optical disc.

*Software.* Computer code forming the program that tells the IT system what to do and when. It is usually in electronic file form and is always present but normally is not seen by the user when being used. Examples include operating systems, word processors, and Monte Carlo simulation application packages.

## 4.7 Summary

This chapter covered the IT aspect of the design team's work. An introductory description of the hardware and software that is generally used has placed IT into perspective. Use of tools in the support of design was outlined, along with reasons for using tools. Tool functionalities have been listed and described. Use of the Internet to support design from a central location has been explained, leading to its use in a paperless office and virtual working by staff.

## References

[1] Kunwoo, L., *Principles of Cad/Cam/CAE Systems*, Upper Saddle River, NJ: Addison-Wesley Publishing, 1999.

[2] INCOSE, 2002, www.incose.org/tools/. This lists tools useful to support systems for many, but not all, engineering aspects of systems development.

[3] CASE tools database. www.cs.queensu.ca/Software-Engineering/toolcat.html.

[4] Levine J. R., Baroudi C., and Levine Young M, *The Internet for Dummies*, New York: John Wiley, 2002.

[5] Lowe, D., *Networking For Dummies*, *6th Edition*, New York: John Wiley, 2002.

[6] Tanenbaum A. S., *Computer Networks*, Prentice Hall PTR, 2002.

## Selected Bibliography

Books on basic computing are numerous and easily found in mainstream bookstores and Web site e-bookshops.

The "In Easy Steps" series of books give a good overall guide to the main tools (Computer Step, U.K., www.ineasysteps.com).

Other similar style series of books are the "Idiots Guides," "Teach Yourself," "Easy Way," "For Dummies," and "Visual Quickstart" series.

Microsoft Technology commissions its own "Running" Series of books. These give comprehensive information on applications in one large softcover volume. Volumes are grouped under user training, user reference works, professional, and developers series (Microsoft Press. www.mspress.microsoft.com).

Books on design support tools are less easily found. The AutoCAD series on design tools has built up over the decades by mustering the many efforts of individuals to develop and market their own programs to given standards of operation and integration. Today they are possibly the most widely used CAD tools.

CHAPTER 5

# The Design and Development Task

Given the task of creating a major project, just how can so many issues be handled and innovation applied? This chapter covers the process of design. It deals with:

- Where design fits into the life-cycle process;
- The types of design that are practiced;
- Nature of the design process;
- Multidisciplinary systems;
- Application of design fundamentals;
- How large projects are decomposed into smaller problems;
- Functional decomposition practice.

## 5.1 Life Cycle from Need to Delivered System

### 5.1.1 Overview of the Stages of Design

The activity of design is essential in all phases of the life cycle. It has been a topic of study for decades, with a key foundational work published in 1968 [1].

In each stage of the SE life cycle, much the same process is used to obtain specific outcomes suited to each stage.

It comprises the following activities:

- Establish the need in terms appropriate to that phase;
- Decide the technical requirement;
- Find a design solution to that requirement;
- Design the parts of the design solution;
- Model and test the solution;
- Build the solution;
- Tidy up the administration of the solution;
- During this process, iterate inside the “egg” to find satisfactory solutions.

Some call this whole process the systems engineering process (SEP), or simply the egg. Detail of SEP is shown in Figure 5.1.

The work starts with activity between the designer and a customer to establish the need, which is the input to this process. This need is then used as the reference and driver statement for carrying out requirements analysis. If the egg is in use for a

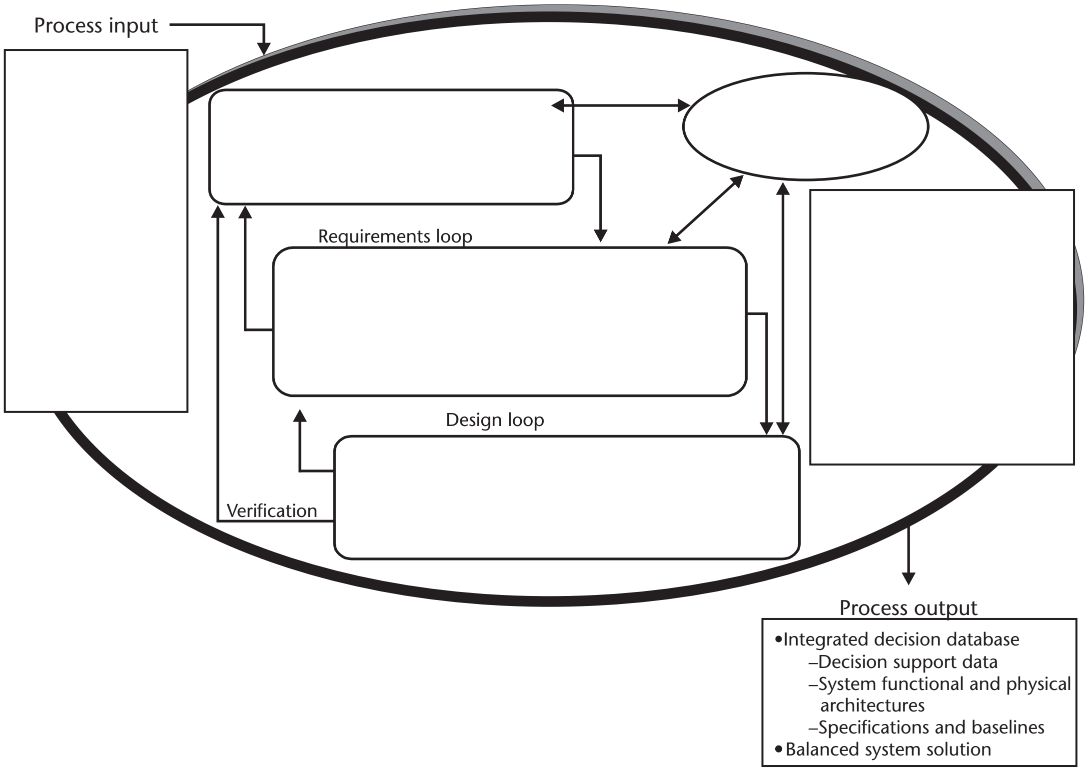


**Figure 5.1** Internal steps of the design process, often called the egg.

later stage of the life cycle, the needs statement will come from sources within the project.

With a reasonably sound basis to work from, the next step is to break down the task until its constituents become clear. This is the requirements analysis step.

The situation is then ready for application of idea generation to synthesize potential solutions that, on the face of it, seem to be sound solutions.

Experience tells us that what may seem satisfactory here must be analyzed carefully to check that the plausible solutions really are suited. Very often, this step shows them to be unsatisfactory and the loop has to be traversed again.

Iteration will be needed around several loops; as shown in Figure 5.1, these are:

- Requirements;
- Design;
- Validation.

As this process may well involve many designers, it is necessary to have some overall control of the whole activity; this is also seen in Figure 5.1.

This is actually akin to the conduct of the scientific process of discovery and so it is to be expected that design, in this engineering detail sense, is the pursuit of a solution (the hypothesis) that is generated by an investigative process, just as is the gathering of knowledge in science.

### 5.1.2 Nature of Design as an Intellectual Pursuit

Design needs a considerable degree of innovation and self-motivation. Setting up the design activity requires a certain degree of tenacity and flair to decide the starting point. Then it needs skill in discovering the right issues to investigate and in obtaining the data needed to make the various design decisions.

Synthesis of design solutions is very much an intellectual exercise, one that is hard to teach as it concerns the cognitive operations of the human mind. Experience with previous situations is needed for best results.

Analyzing a potential design solution needs good logical thinking backed by a range of mathematical skills.

Putting all of the often-conflicting issues together is another kind of skill needed in design.

Too much control over a designer's thinking can make designs unimaginative and less likely to hold with time. On the other hand, letting designers have their way can be dangerous, as their outcomes can be expensive, irrational, or too much blue-sky thinking.

The team leader needs to carefully balance the degree of freedom allowed against the constraints applied on team solutions. This needs both control and guidance to get the best results.

Experts on the nature of organizational theory suggest there are several kinds of people in a healthy project development situation.

"Heroes" are the people who are able to overcome the chaos of the situation and make things work in the face of adverse conditions. They keep things moving along where many would give up.

It is the "artists" who bring brilliance to projects and can assist order issues for the better.

Then there are the "craftsmen" who follow the process, learning from experience what is the better way to carry out practices. They are unlikely to try to affect much change—which is their strength as they bring stability to the activity.

However, all of the above are insufficient without the research scientists and engineers who, as master craftsmen, are able to fine-tune the process through deductive and inductive learning and reflective thinking based on their experience.

To improve the quality of an operation in the design group, these kinds of personalities should be nurtured.

### 5.1.3 Types of Design

The term "design" has been used so far in a collectively broad sense. It is important to appreciate that three quite different types of design activity and thinking exist in an engineering project [2, 3].

Each has similar aims of developing a satisfactory, acceptable set of parameters as per the SEP, but they bring different emphases to the SEP parameters:

- Fine art design;
- Industrial design;
- Detail engineering design.

### Fine Arts Design

The main interest in the fine arts design regime is modeling such abstract ideas as the impression a concept makes in the project user's mind and forming impressions using physical models and images.

It is little concerned with the reality of creating the solution but injects needed properties by way of:

- Prestige generated by owning the product or using the service;
- Esteem gained from being simply associated with it;
- Pleasure gained from being physically near it;
- Feeling of operational value imbued from its acclaimed reputation;
- General well being attained as nice equipment that is good to use.

However, a word of caution: the existence of well-executed fine arts design features does not necessarily mean the product or service is fit for purpose!

A well-designed item will bring the best out of users. It will seem right in use and a joy to operate and maintain. On the other hand, a poorly developed artistic design can give all manner of incorrect impressions. The level of fine art design needs to match the market requirements and application.

Detail engineers have the task to create things that work; for this they instinctively can recognize if a design will function correctly. Their skills do not usually include fine arts design ability. Their own brief rarely covers the artistic aspects so, left to it, their assemblies are usually somewhat utilitarian. They also may feel time spent on adding artistry features is a waste of time. Paradoxically, artists often emphasize the engineering aspects as part of their stylistic promotions.

Today this aspect is increasingly important for customers of products like the automobile, who implicitly expect good engineering performance and now concentrate more on human factors and styling as their purchasing points.

Many engineering projects are overly absent of fine arts considerations, often to the detriment of the project's final success. Examples of utilitarian designs are seen in electrical distribution and microwave antenna towers, now both becoming targets of the public demand for better appearance.

Excellent projects will have this aspect well covered by the use of talented fine arts designers.

### Industrial Design

Industrial design takes a fine arts contribution and adds the next step toward realization of an engineering design concept. It uses mostly mock-ups that are not functional, but look like the real thing from a distance.

This level of consideration is starting to tease out the operational specification and generate limited technical specifications.

It is taught by industrial design departments, not in engineering schools. Interfacing curriculum topics that link industrial design and engineering are rarely taught. Industrial design, however, is often be associated with fine arts schools.

Detail engineers are not good at industrial design for it involves a fair amount of fine art design and special model making skills that are seen as too subjective and hand-skill filled for engineering courses.

Industrial design's physical models are made from plaster, foam, balsa wood, and other easily crafted modeling materials. The final objects can be remarkably realistic in appearance but they are largely "fake."

Industrial design, then, assists in deciding the system mix, shape, final form, and how it will look. It also covers making a choice of candidate schemas. These models allow investigation into how users will accept the end product. Industrial design also assists in establishing key requirements and how well the intended design will stand up to competitive alternatives in the human aspects.

It has its place in the concept development stage of the SE life cycle.

#### Detail Engineering Design

Taking a requirement and designing a working system that satisfies the need is what professional engineers are generally educated and trained to do. They take the operational requirement, from which are decided the technical requirements, and then progress those statements on to the actual final detail, this being in largely quantitative terms.

Detail design engineers are often spoken about in terms of the "nuts and bolts" issues they handle. This is easily explained, for it is at the detailed design stage that such definite issues must be translated into exacting decisions so that specific items can be made. The buck stops here!

The expected readers of this book are mainly of this design kind, so there is little need to dwell on the nature and characteristics of detailed design engineering as a profession. Successful system design relies on appropriate application of the three kinds of design being executed by experts. The person carrying the systems engineering responsibility needs to ensure that each is done well to the level appropriate to the project.

## 5.2 Nature of the Engineering Design Process

### 5.2.1 Open and Closed Design Environments

Two kinds of design situations can be identified: open or closed systems. These are now explored.

The ideal of there being possible a masterful design that can cope with all environments of operation is attractive, but rarely realistic. The actual system built will be impacted by many issues, and to be realized in the specific terms needed of design engineering will only be possible within a limited set of operational conditions.

Balance is needed between the generally capable system that comes with high cost and performance penalties, and the specific design that is trimmed and tuned for a given set of conditions.

These needs will become clear as the critical issues are exposed when one seeks to isolate and set down firm foundations for a design.

In the initial concept stage, the design thinking is operating in an open environment wherein many systems parameters are very influential, often changing and problematic. This kind of situation does not permit detailed design to be completed until all significant issues are closed off, and the situation made into what is called the closed environment design regime.

When a design exercise first starts there are too many issues to cover and too many solutions that could be generated. Means are needed to narrow down the options.

One issue that assists this, and must be addressed early, is setting down the boundary limits of a design activity. This refines the design situation from its initial openness, moving it toward the needed closed situation.

A sound start to closing the design environment is to construct a boundary limits diagram, also often known as a context diagram.

This facilitates:

- Limits to be developed at the breadth of inclusion seen to be sufficient;
- Records to be made that allow others to understand the thinking regarding extent of consideration;
- Development of sound appreciation of the external factors that design must address for success.

The boundary limits diagram acts also as a baseline, giving a position statement when things go wrong! It also is useful for later upgrades as the result of what is learned as the development proceeds. Figure 5.2 is an example of a thermometer being used inside a system to determine temperature. Effects such as relative humidity are shielded out to allow a closed operating environment and thus make detailed design effective.

Engineering detail design is about making the final decisions that all others involved have generally only worked on in the semiabstract state. It has to finalize actual details of components, settings, software, connections, sizes, shapes, and so forth. It must yield robust manufacturing specifications, for this is the

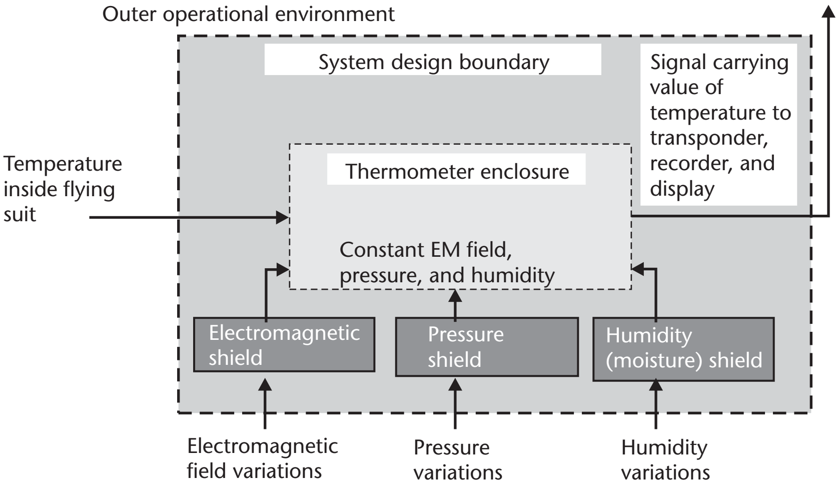


**Figure 5.2** Simple boundary limits diagram.

detail used to manufacture a system that should not need to be corrected after production.

Creating a closed design situation needs all external influences to be sorted out and controlled, or worked within. The always-present design problem is that it is not possible to entirely reach a perfect state for this need.

### 5.2.2 Multidisciplinary Nature of Design

Engineering design is about the harnessing the energy and mass of technical systems. Energy and mass obey the rules and laws of physics and thus can be handled in the strictly related terms of formal mathematical description. That allows closed design thinking to be practiced. Engineering design is also about the harnessing of information. This is not describable by the laws of physics when it concerns human communication, but much of data communication and processing can be made formal when suitable mathematics descriptions are possible.

It is the cognitive, meaningful nature of messages that defies formal modeling and therefore can be the Achilles heel in a design. Therefore, an engineering design will usually involve many different energy, mass, and information aspects, such as:

- Thermal state of circuit components;
- Acoustic and supersonic noise signal generation from components;
- Weight of circuit assemblies for aerospace use;
- Geometry to fit limited spaces such as in mobile radios;
- Seating of operators in equipment;
- Use of controls by operators;
- Fluid dynamics of cooling systems;
- The many physical regimes used in the sensor assemblies.

Checklists are useful aids for helping to ensure that all regimes are covered in a design environment study. Mature organizations will usually have such lists on hand.

### 5.2.3 Iteration and Early Error Detection

Errors are unavoidable because design is a matter of making many assumptions in often problematic situations. Waiting to find out more information to reduce the risk of less than perfect decision-making often does not work because the project must move on. Many design decisions are made in a far from perfect state of knowledge.

The two main sources of error that need to be guarded against are the slip or lapse as the result of failure to carry out an intention, and simply making a mistake in deciding the important factors of the goals and actions needed.

It is virtually impossible to totally avoid errors from occurring in complex projects; it is a human characteristic. However, there are ways to reduce their occurrence, such as by the use of well-planned prototyping (see Chapter 11).

The key aim is to remove the risk of mistakes by trapping them early enough in the project when the consequences can be minimized. Integrated project team (IPT) working is good for early error trapping because the process of decision-making is transparent to many people, taking place at a time when decisions can be challenged and corrected. A nudge about an apparent error from one person to another early in the project need not be a career-threatening embarrassment!

It has been established by a major USDoD study that a dominant reason for failed programs is that the person who discovers an error is unlikely to report it for fear of retribution to employment and career. Leaving it in place in the hope it will go away or be corrected quietly is all too often the action chosen. Error trapping needs to be rewarded, not penalized, in order to attend to them early, but beware of those who create deliberate errors in order to "find" them later.

One way to increase the error tolerance of designs is by making it easy to discover errors. This can be achieved by making actions more visible and by using effective feedback paths that allow fast correction.

Additionally, it is wise to set up operations of a design process and of the system being made such that it is difficult to make errors that cannot be reversed. An example is to require confirmation for actions such as deleting information when a delete file command is invoked. Another example is to make a person think twice before finalizing an action.

Examples of error reduction in operational processes are use of interlocking functions that force error-protecting sequences on the system user. These can be lock-ins that prevent premature action, or the opposite, lockouts that prevent dangerous paths being taken by users.

Cross checking design features and systems operation is a powerful means of error reduction, provided the checker is able to see the difference and is prepared to point it out. An example of this is the preflight check procedure used in an aircraft cockpit. The pilot and the copilot run through a checklist of control settings, each pilot checking the data with the other person.

However, it is human nature to resist pointing out errors in this kind of situation for fear of embarrassment at not really understanding the situation, or as has already been mentioned, for fear of retribution.

The rate of expenditure on projects is recognized to have a large bearing on project outcome. High front-end loading (FEL) is recommended (Figure 5.3). If a greater degree of resource is effectively expended in the early stages of the life cycle, then more errors are likely to be discovered and corrected before they flow through to generate a disastrous state of affairs at delivery time. Larger FEL expenditures are, however, sometimes misused and still end up with system failure.

Despite this well-recognized wisdom, many projects do not get the right degree of effort in their early stages. There are many reasons for this.

First, it is natural for those controlling the purse strings to feel that overgenerosity with funds at the early stage can lead to inefficiency and waste when the project parameters are still very uncertain. The fact that good systems engineering can use the funding well is not always appreciated.

Second, high-level leadership would rather see several start-ups in place than one much larger effort. It looks grander and more promising; thoughts of project failures are far away at their starting time.

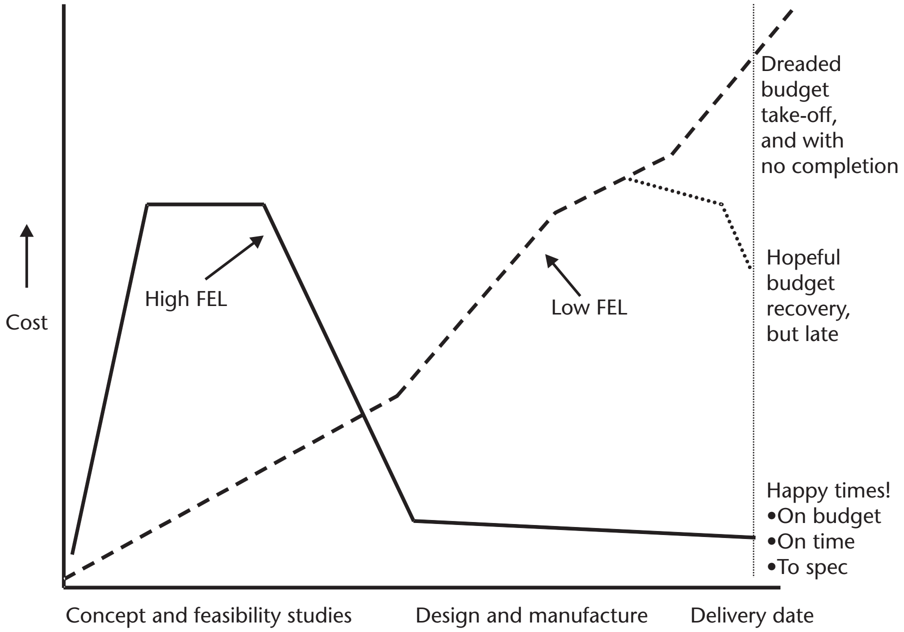


**Figure 5.3** Comparison of FEL spend rates on project outcomes.

Third, it is often hard to get the higher budget amount needed at that early stage due to conservative thinking for what is still a risky project. Large commercial projects appear to understand this need, and, while they are reticent to disclose their spending profile, do pour in the resources up front. Publicly accountable programs, on the other hand, such as those that are government funded, do not follow this wisdom well at all.

Fourth, even though the effort and intellectual resources have been allocated to give a sound FEL budget, they are often stripped away to keep another project going that has fallen behind its own budget.

### 5.2.4 Design Process Flowcharts

Many flowcharts exist for the detailed design process. They express much the same sequence of events but use different terms and number of stages. The steps traversed are:

- Decide the need;
- Break it down into manageable subparts;
- Develop a design solution for each part;
- Validate that the design is within all limits;
- Analyze each candidate design alternative for adequacy of all factors;
- Analyze sets of subparts in ever-larger wholes;
- Test the design before manufacture;
- Iterate any needed design changes before final manufacture;
- Declare the design;

- Document the design and its foundation.

The design flowchart given in Figure 5.4 has more detail than many that are published. Each step of the process is explained in Table 5.1.

While a flowchart pins down the detailed design activity and can be a useful aid to teaching and ensuring all the right actions take place, the experienced designer moves through these steps often quite unconsciously. Practical design cannot simply proceed in a mechanistic manner through the steps but needs considerable iteration. Activity will move over the stages in what can seem to be a chaotic order. The experienced designer's mind also picks up on issues in quite unexpected ways and with unpredictable timing.

## 5.3 Design of Multidisciplinary Systems

### 5.3.1 Specification of Need

A client needs a system that provides operation capability (i.e., that it does the right task). It must also possess adequate operational suitability (i.e., that it also does those tasks when needed, and for as long as is needed).

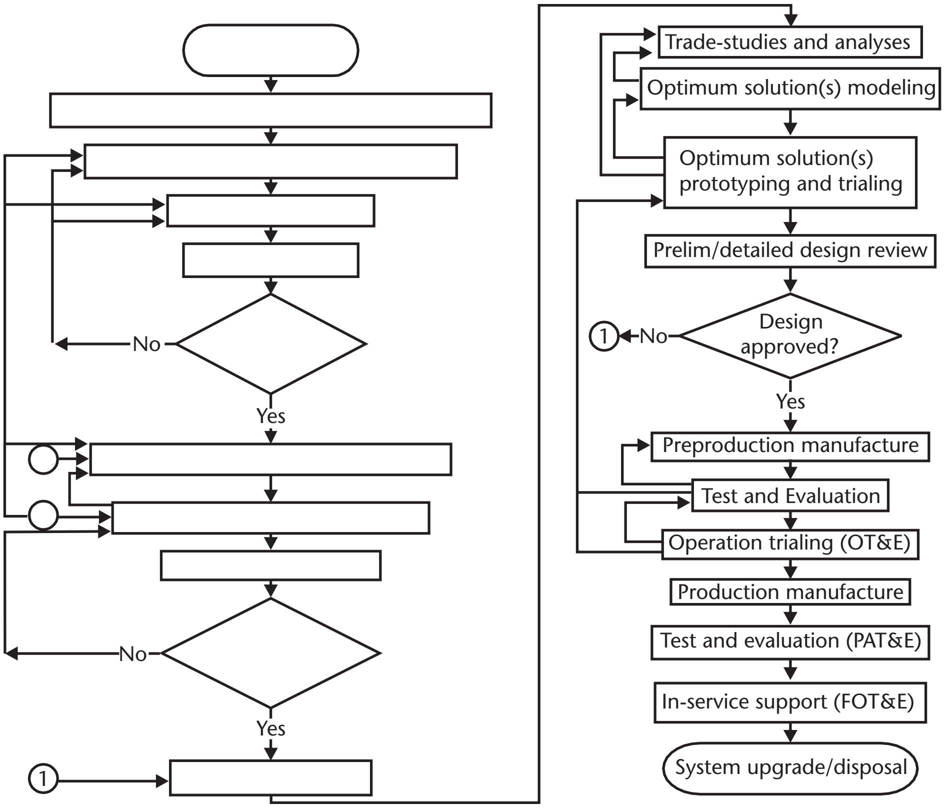


**Figure 5.4** Detailed flowchart covering the design activity of a project. (*Courtesy*: Tim Welburn.)

**Table 5.1** Design Process Element Description

| *Design Process Element* | *Description* |
|---|---|
| Identify concept of operations with customer | The process of establishing with the customer (including actual product end-users) how they intend to use the product.<br>Factors to be established:<br>Usage environments;<br>Usage patterns (duration, number of usages per day/week/year);<br>Characteristics of users (size, mass, male/female);<br>Equipment maintenance and repair philosophy;<br>Equipment size and constraints;<br>Preconceived concepts, implementations, etc.<br>Customer key performance indicators (KPI);<br>Any other design constraints, requirements. |
| Identify customer needs and requirements | ollowing on from the identification of the concept of operations, identify what the customer needs and requirements are for the system. Categorize equirements as functional, performance, or design constraining. |
| System specification | Prepare a written specification of the requirements associated with the system.<br>Format in accordance with MIL-STD-498 “Software Development and Documentation” data item description (DID) DI-IPSC-81431 “System/Subsystem Specification.” |
| Customer review | Conduct a formal review of the system specification with the customer to establish the completeness, accuracy, and commonality of needs interpretations in the specification document.<br>Review with the customer the intended methods for how requirements will be verified at final product acceptance. |
| Specification approved? | Establish whether the customer approves of the specification.<br>Approval allows further development of the system design and concepts to proceed.<br>Disapproval requires a reassessment of requirements, customer needs to be conducted, and the system specification to be amended as appropriate. |
| Function identification and modeling | Formulate a function-based model of the system that satisfies the system requirements.<br>Simulate information flow between the function elements of the system. |
| Physical allocation and synthesis | Formulate a physical model of the system that maps its functional elements onto candidate physical entities. |
| System design review | Conduct a formal review of the resultant system design with the customer to establish agreement on the concept design developed, interpretation of requirements into design, and the completeness of the design with respect of the agreed system requirements.<br>Review verification plans and intended verification methods. |
| System design approved? | Establish whether the customer approves of the system design.<br>Approval allows further decomposition of the system design and concept prototyping and development to proceed.<br>Disapproval requires a reassessment of identified functions, physical syntheses, and requirements and customer needs, to be conducted. |
| System reticulation | Conduct a reticulation (decomposition) of the system functional and physical design to identify finite physical elements of the design to be implemented in hardware or software. |

**Table 5.1** (continued)

| *Design Process Element* | *Description* |
|---|---|
| Trade studies and analyses | Conduct trade-studies and associated analyses to identify the optimum implementation for critical (risk) elements of the design. |
| Optimum solution modeling | Use simulation (where appropriate) to model the performance characteristics of critical (risk) elements of the design. |
| Optimum solution prototyping and trialing | Develop physical prototypes of critical (risk) elements of the design. Conduct performance trialing of the prototypes using test facilities (bench-testing, environmental test chambers, and end-user trialing). |
| Preliminary/detailed design review | Conduct a formal review of the preferred/optimum system design with the customer to establish agreement on the design developed, interpretation of requirements into design, and the completeness of the design with respect of the agreed system requirements.<br>Review results of candidate solution simulations, prototyping, and end-user trials.<br>Review verification procedures. |
| Design approved? | Establish whether the customer approves of the system design.<br>Approval allows preproduction/production manufacture and trialing to proceed.<br>Disapproval requires a reassessment of solution simulations and prototypes, or a review of system-level decompositions, functions, and physical allocations. |
| Preproduction manufacture | Allow-quantity manufacturing run of products, using production drawings, tooling, procedures, and verification methods. |
| Test and evaluation | Verification of product performance characteristics against the agreed system specification requirements, using the agreed verification procedures. |
| Operation trialing | Operation test and evaluation (OT&E) conducted by the customer, using preproduction units, to assess the function and performance characteristics of the product in its intended use environment.<br>Feedback provided by the customer to the contractor may trigger design and/or (planned) production changes. |
| Production manufacture | Production quantity product manufacture, verifications, and delivery to the customer. |
| Test and evaluation | Production acceptance test and evaluations (PAT&E) to assess adherence of production units to agreed performance characteristics. |
| Follow-on test and evaluation | Contractor-conducted investigations into future product design and/or performance enhancements.<br>Customer-conducted investigations into future product capability and/or use enhancements. |

(*Courtesy*: Tim Welburn.)

The system design must also meet certain cost conditions for ownership and operation, comply with a host of legally required environmental conditions, and meet appropriate health and safety regulations.

To provide this very large list of "must haves," it is necessary to tease out a large set of requirements.

Note that requirements cover much more than the task the system has to do and that this step must be done with plenty of customer and/or user involvement.

A need should be based on a real, existing deficiency as might arise from current system inadequacy, such as it being unavailable, unsupportable, or too costly to operate. Alternatively, it might arise because of a lack of a necessary capability.

The statement of need ideally should to be presented in carefully generated qualitative and quantitative terms along with sufficient detail to allow design to proceed, at least in terms of the desired functions. Some needs are best framed in customer and artistic terms because they are largely qualitative.

Defining the need can be the most difficult part of the systems engineering process. For this reason, the whole of Chapter 6 covers the development of the concept and requirements for a project.

Projects often start based on political whims and personal subjective calls, without sufficient care taken to properly establish the requirement. This is perhaps the earliest and most significant system design error that can be made, becaue the project will already be heading in the wrong direction. Quality investigation time is necessary to do a good job of requirements extraction.

### 5.3.2 Generation of Architectures Needed

Once the need is established in operational terms, it is then possible to begin to architect the system. Well-developed system architecting can give the task an organized structure that assists requirements generation [4]. Good, experienced designers can perform the task naturally, as they synthesize potential solutions that seem to meet the requirements. Underlying the process sound principles exist that can be used to make work more efficient.

System architecting is the process wherein the specification of the whole design solution is developed and verified.

The first step is to acquire a sound understanding of the requirement in terms of the desired operation.

Next, the concept of operations (ConOps; also called the operational concept) is created for the system. This defines how the system will function. A ConOps study then permits the flow of activities, or information, to be laid out in terms of black-box functions joined together (which is the first-cut system architecture) to facilitate the necessary energy or mass flows controlled by information flows. Development of a ConOps study is covered in Section 6.4.

This process leads to identification of the main building blocks needed. Once these are in place the individual subsystem block detail designs can commence.

Young, less experienced engineers mostly move to start a design by matching the need against available building blocks. Guard against this bottom-up approach; although it can lead to a solution for smaller projects, it has no way of ensuring success, or of being able to be defended as a good design. Some degree of bottom-up design is allowable, for it is efficient to use already proven units if they clearly fit the need without distorting the required system performance. Commercial off-the-shelf (COTS) items such as a personal computer are quite commonly used.

In sharp contrast, experienced engineering designers will take the top-down approach, letting ensuing decisions decide what components fit the previously operational format, abstractly expressed, needs.

### 5.3.3 Creation of Design Models

As the design takes form and shape, a model of the design is being generated. Early stage considerations use models that are not concerned with detail but are instead used at a higher level of abstraction.

Models at the early stages can take many forms, each playing a different part in assisting development of ideas and system architecture:

- Sketches showing the organic parts that make up the whole;
- Block diagrams connected with energy or signal paths;
- Physically manufactured forms of models such as those from industrial design involvement;
- Textual descriptions;
- Structures built using computer-based modeling tools;
- Formal mathematical equations.

At the early stage of design, the representation is more concerned with overall ideas and trends than with exactness. There is little place for exactness at the early stages of system development—indeed, it can actually be a hindrance to thinking.

What is being achieved is a sound way of progressively reducing the countless design choices to eventually reach the final nuts and bolts specificity needed. Figure 5.5 shows a model of the progress of the design process in action.

The problem facing a designer is to constantly make key design decisions that move some of that generality into specific data. These places of design certainty can be relied upon to use for moving further down into detail.

### 5.3.4 Analysis and Simulation in Support of Design

Simple designs can often make use of just personal experience alone coupled with reuse of past designs that are modified to suit.

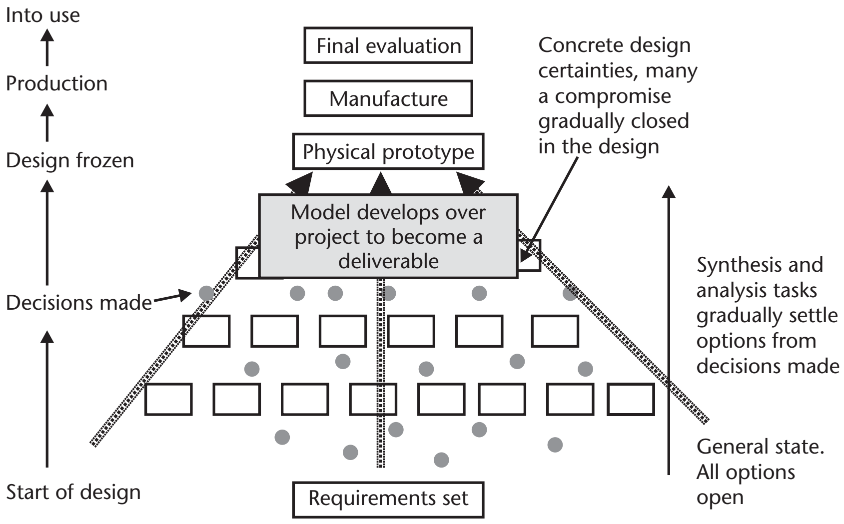


**Figure 5.5** Design process gradually reduces the degree of generality to concrete manufacturing details.

However, as the size and novelty of the design task grows, a more systematic method is needed that is underpinned by good analysis of the alternative options that have been synthesized.

Clear logical thinking is first applied to construct sound architectures. Models are then built to reflect this architecture. These are then analyzed using formal mathematical description or other techniques founded in sound science.

The use of computers in support of this process is well established. Where well-developed tools and experienced staff are available, then use of computer-based design has considerable advantages as it can be applied via a model of the design without the need to make physical assemblies.

The benefits of computer-based methods can be many:

- Faster to develop a more soundly designed product;
- Allows effective reuse of designs as the basis of rapid redevelopments;
- Finds design sensitivities, where tools support it;
- Data becomes available for related needs;
- Thermal and EMC performance can be investigated;
- Reliability studies can be carried out;
- Safety studies are improved by use of techniques such as Monte Carlo simulations of system safety models;
- Space and shape studies give realism to the design;
- Time needed to make physical prototypes is reduced as fewer are needed;
- Records exist that give reliable information.

However, a word of caution! Even the most successful CAD-based design suites cannot replicate the full extent of reality. Real assemblies are essential at crucial times to validate the models used. Further discussion of modeling and simulation in design is covered in Chapter 11.

### 5.3.5 Working with Mixed Design Regimes

Most projects involve the integration of many disciplines, typically engineering of various kinds, computer science, the sciences, and law and other humanities disciplines. The combination of software and engineering is possibly the largest interaction, for virtually all modern projects contain a significant software component. Harmony is not necessarily guaranteed for these areas.

A well-founded belief exists that software development is done differently than hardware development and that software development too often is done with less reality involved than there should be.

Some people regard software development to be a subpart of overall systems engineering development—but not all. Others see it as a separate discipline.

Software is a totally abstract entity with virtually infinite design options. Being binary in its operation, each program step is simple but each can carry a very significant outcome. There can be millions of such transitions about which to be certain; errors propagate all too easily in software code.

Code does not reveal its "meaningful" nature as does the hardware manifestation such as the circuit board or a gearbox. System changes are so easy to make in the software regime. They need careful control to ensure that propagation of a simple change does not disturb the performance incorrectly.

It seems that the inherent thinking of software designers is often different than that of hardware designers. Engineers are very deeply trained in the reductionist-thinking ethic. Their models are usually of the hard science, formal, mathematical kinds.

Computer scientists are trained in the use of logic and discrete mathematics but less so in the formal means of analysis. Engineers can be less able to cope with the abstract nature of software.

A good design team will be well integrated to handle the software/hardware codesign situation.

Overall, new IT system projects have a less-than-desired performance record and effort is continuously being expended to improve in the situation. However, as the methods improve so also does the level of performance and sophistication needed with major systems. In the first fly-by-wire aircraft control systems, the software component used as little as 8 KB of memory and an equally small program code size. Today, software in aircraft can contain millions of lines of code and require large-size computers.

As most projects have major software components, all projects could be classified as being part of IT.

Let us return to the performance of IT project start-ups. The results of a 1996 study of 14,000 U.K. IT projects [5] are instructive for its findings:

- 80% to 90% did not meet their performance goals;
- About 80% of systems are delivered late and over budget;
- About 40% of development projects fail or are abandoned;
- Fewer than 40% fully address training and skills requirements;
- Less than 25% properly integrate business and technology objectives;
- Just 10% to 20% meet all their success criteria.

Yes! Only an average of 15% of all projects were reported as fine! There are several major reasons for the failure of software projects, including:

- Lack of a complete requirements specification;
- Lack of an appropriate development methodology;
- Poor decomposition of design into manageable components.

Downside business aspects of this were significant:

- Lost business production and assets;
- Increasing software costs of enormous proportions;
- Legal liability issues increased;
- Hindrance to industrial economies growth.

Despite these rather negative pointers, the issue of codesign can be handled effectively. Indeed, many projects are highly successful; the fact is failures are widely promoted, whereas the successes go unsung most of the time.

Success in handling the multidisciplinary aspect of a development is a matter of recognizing the differences in thinking in design activity and developing that all-important coalition-working design office environment.

## 5.4 Practical Application of Design Processes

### 5.4.1 Realism and Design Creep

The task of requirements investigation could easily overrun the designer. Balance has to be drawn between how much is needed with how much can be done.

The various personalities involved in the development process can have differing ideas of what is sufficient:

- *Inventor:* will tend to keep wanting to update the ideas with improvements;
- *Accountant:* will want the least cost almost regardless of design performance;
- *Designers:* will want to create ever-better designs;
- *Software developers:* will get it right after "a few bugs are sorted out";
- *Project manager:* will need everything done yesterday.

The overall project manager has to balance these norms. This ripples down to the design team leader who must also recognize these differing attitudes.

The distorted viewpoints of the different designer regimes have been expressed effectively in a cartoon about the development of a missile (Figure 5.6).

In order to feel they are reducing the risk, it is easy for both customers and designers to overspecify issues.

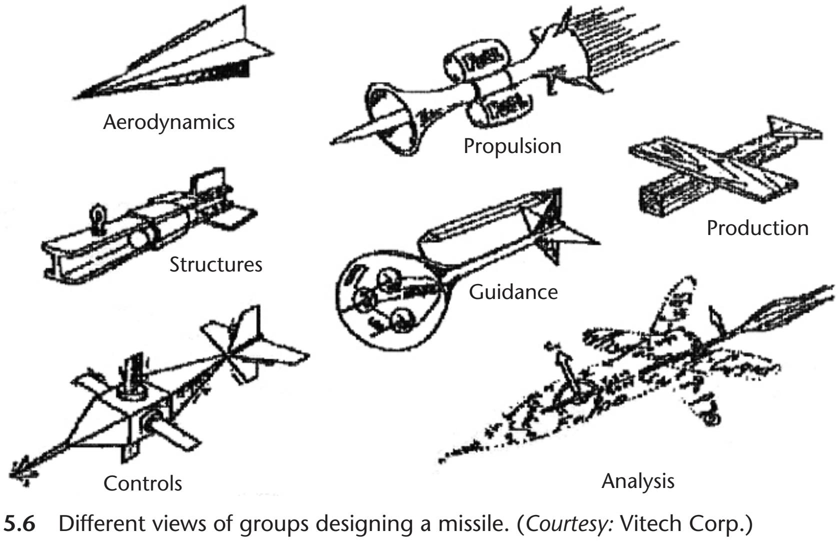


**Figure 5.6** Different views of groups designing a missile. (*Courtesy:* Vitech Corp.)

As an example of how specification creep can arise despite good intentions all round, consider the designer of a tracking theodolite that once specified the need for 5arcsec precision from a shaft encoder for a flight test range-tracking unit. His sums showed that 7arcsec was sufficient so he rounded it down to the nearest known product specification.

By the time the project director and the company's purchasing department got the order out to vendors, the specification had tightened down to 0.5 arcsec. Each had added their margin of safety.

This was a most demanding specification so the vendor, wishing to make sure the product absolutely met the need, actually built a 0.2-arcsec encoder.

The problem was that while such a "nice to have" unit was highly acceptable, the excessive performance that was delivered could not be used to the full by the mount. More significant was the fact that the cost of absolute digital encoders rises exponentially with increase in precision.

The cost of the encoder ballooned out to over 100 times that of one that would have satisfied the need. Additionally, the delivery date was greatly extended out to allow time to develop the bespoke unit now asked for.

Overspecification has to be controlled by experienced systems engineering staff that can apply judgment from seeing a wider perspective than the detail design person sees. Designers are prone to "overegg the pudding" and need to have their efforts tempered as trades are made between the designs of different groups.

### 5.4.2 Targets and Milestones and the Form of Contracts

The customer wants the specified performance delivered on time and to the agreed cost and will call for evidence of progress as the development proceeds.

There are many thrusts for a project contract; however, none of them is ideal. All of them have their place and fashionable time. Suppliers have only limited control over the type of contract that a customer places.

Types of contracts are now compared, giving a few pointers of the difficulties that can arise.

*Fixed-cost contracts.* Here, the successfully bidding contractor supplies the system for a predetermined fixed cost determined during a competitive bidding process. It is most likely to be awarded to the lowest cost bid. On the face of it, this appears ideal for the customer, but it does not necessarily guarantee the project will be delivered as needed. Lost time will see the technology being used become out of date, creating a need for system upgrades. This can cloud the original contract provision and drive the customer to seek unbudgeted improvements.

Next, the contractor may be close to failing because he or she has bid too low to win the contract. Being the only one close to providing a completed system, the contractor is often able to obtain more payments from the customer to keep the project going. In such circumstances, it also drives the contractor to cut corners where possible.

*Cost plus pricing.* Here, the contractor does the work for the cost needed to do the job, plus some agreed profit margin. The obvious problem here is in keeping the costs down, for it is in the interests of the contractor to do more work than may be necessary. On the other hand, some developments are just so risky as to not be able to be estimated well enough, and therefore must proceed this way.

*Value for money.* This type of contract basis provides effective work for the cost charged. However, working out what is "value for money" is not easy to do.

*Whole of life costing.* Here, the concept is based on the customer being more certain that the contractor is not keeping the original supply price lower through use of a design that satisfies supply at the time of delivery only, and has not passed on avoidable costs into after-acceptance time. By giving the contractor the whole of life supply task, the overall cost of many years of supply and operation all need to be integrated.

*Target cost.* This type of contract has some elements of a fixed-price contract because a maximum target cost is set. There is then a pain/gain mechanism defined that rewards the supplier with a share of any price reduction obtained or penalizes any overspend (often by only paying at cost for the overspend). This approach provides strong incentive for the supplier and the customer to seek the most effective solution in a mutually win/win situation.

Developing bids for large projects is not a task that the team leader will usually get to manage until he or she has many years of experience, but at the team level, members need to appreciate the kind of contract that the team is working within.

### 5.4.3 Design Control

Milestones, or other targets, should be set up within projects.

Test and evaluation plans set up metrics and technical performance parameters (TPMs) that are set up over the projects parameters allow performance maturity trends to be seen and corrected.

Performance-driven activity must have the necessary parameters to make the right things happen. Poorly chosen metrics, or an incomplete set, can drive a project in the wrong direction. Often the performance parameters set up are too simplistic or not that indicative of effort and success. Setting up crisp and penetrating metrics is a highly developed art and science.

For example, the simple metric of "hours worked" is a very poor indicator of "software produced." A complex set of interrelated metrics is needed to cover the many parameters that decide how much of the software being written is satisfactory.

Performance-related uses also need to allow for the fact that innovative projects will often not be able to accurately predict realistic deliverables and the like.

Design review meetings are regular events that assist integration of the design work. These use preset agenda lists to cover the various points of design that need consideration. Interface documentation is considered in effective design reviews as it identifies the areas of integration for which a design team's work needs to be monitored. It is also necessary in reviews to consider form, fit, and function for designs because interfacing considerations are insufficient to ensure good design outcomes.

More is given on design reviews in Chapter 8.

## 5.5 Reticulation of Design Activity

### 5.5.1 Reductionism Approach to Problem Solving

Large systems developments will involve vastly more issues that can be handled in one person's mind. This is known as exceeding a "brain-full" limit. An example of the size of the problem is seen in some statistics of the Australian Collins Class submarine project.

At the start of the project, the prime contract documentation comprised 22,000 pages of text and drawings. The documentation weighed in at 95 kg and occupied 2.5 meters of shelf space. The total project documentation, in hard copy format, weighed in the tonnes.

The $2 billion value of this first contract had to deal in nine currencies. There were 600 subcontracts, with production taking place in nine countries. In the 1,500 identified work packages there were 250,000 events that had to be scheduled. There are an estimated 8 million parts in the submarine. Production spanned a decade and support will be needed for more than 30 years, or even longer if past experiences apply.

While this was a notably large defense project, it was overshadowed in cost by some of the automobile new design commercial projects! Seen in these terms it is truly amazing what can actually be achieved!

Means must be used to allow a project to be broken up into subpart problems that can be given to the many designers without them duplicating effort, and in which all necessary parts are made that fit and work together in the end.

As has already been introduced in Chapter 1, engineers approach most of their problem solving from the reductionist method; that is, by dividing the requirement down from the top until small enough activities are realized that can be undertaken by each small team.

This works on the basis of creating a downward evolving tree of knowledge of the project tasks. These trees are a logical construct of the mind that motivates thought on a topic and records relationships between items on the levels of the tree.

This breakdown process is called by many names: decomposition, box cutting, partitioning, reticulation, top-down approach, task breakdown, requirements engineering, and so forth.

This seems to be an appropriate place to discuss the concept of complexity in design situations. Complexity, as used here, concerns more than just the number of items involved.

System complexity also arises from the difficulty of defining the boundary of a system; just what is involved?

It is, furthermore, concerned with the size issue, for being larger than a single brain-full means it needs systems engineering methods to cope with its extent.

Another parameter that adds to the definition of complexity is its multidisciplinary nature. Are there many technologies involved?

The nature of the internal and external connections between entities—the system topology—adds another dimension of difficulty, as does the convergence of overlapping separate systems.

Given those issues, complexity rises significantly if humans are involved in the application of the system.

### 5.5.2 Decomposition of Requirements

Systems engineering facilitates management of complexity by translating the top-level problem into a set of manageable tasks. Partitioning is thus the common approach to complexity. This breaks systems down from wholes into subsystems and then through subsystems into components. This creates manageable order.

As an example of this decomposition process, consider the air defense system for a country. At the highest level, initial decomposition yields many integrated parts, each being a system in their own right:

- Command and control, communications, radars, identification, satellites, ships, early warning aircraft, fighters, tankers, missile sites, and so forth;

From this set of systems (some would call the above level a systems of systems), consider just one item, a ship. This decomposes into its own systems:

- Hull, engines, command and control, communications, radars, sonars, torpedoes; missiles, launchers, and so forth.

Applying another level of decomposition for just the missile, we get the:

- Body, sensor, fuse, warhead, electronics, guidance, motor, umbilical, batteries, and so forth.
- Yet again, another breakdown of the missile casing alone yields radome, forebody, midsection, afterbody, air intakes, wings, fins, actuators, connector, launch lugs, and so forth.

Then onto the actuator of the missile casing:

- Case, armature, winding, spring, end stops, contacts, connecting wires, support bracket, nuts, bolts, and so forth.

At some stage it is appropriate to cease decomposition. Just where depends on the design situation. One does not normally need to go right down to the molecular level of matter but there can be a time when even that is needed in a design.

Decomposition creates interfaces that must be managed. Managing interfaces is a key activity in systems engineering, and the information interface is one that is particularly difficult to manage as it usually involves problematic human issues as well as hardware. System partitioning must specify, and also manage, the many interfaces and associated relationships. Software is often used to provide interface functions. Data flow between subsystems is a particularly important consideration. Standards for the data must be consistent across the interface.

The principle of strong and weak interface links is of value to know. The way in which a system is decomposed is not unique to a specific system; many different ways can be used.

The above air defense system has used organic entities as its units. These physical objects can be isolated relatively easily from each other (i.e., dismantled into stand-alone assemblies), and thus can be undertaken as independent design activities. They are all weakly interfaced for they all can be used without the others in some roles.

That system could have been broken down into land, sea, and air systems; or in a quite different (in fact, ridiculous) way on the basis of the kind of material used in a part, as would be in setting up a store supply facility (i.e., into, say, copper, steel, brass, and plastic parts).

The materials way is obviously very inefficient when applied to the air defense system, for it means that all systems would have to be broken down into far too small a level and that almost every system would be handled (i.e., have interfaces), to all of the different materials departments.

As another example, in the English-speaking world university campuses are usually decomposed into faculties covering like–kind disciplines, with the whole covering a wide range of disciplines that can support all industries. In contrast, some countries have campuses set up to support all aspects of a single industry, such as electrical engineering or broadcasting.

Hence we see that once the basic system design has been established, freedom exists in where and how to partition it to obtain subsystems. These different examples illustrate that a system needs to be broken down for best effect by observing some basic partitioning rules. These are:

Rule 1. Interfaces between units should be chosen where interactions are weakest. This reduces the interface design problems.

Rule 2. Strong links are best kept inside subsystems, and the system boundaries should be chosen according to this same principle. This forms logical entities and stand-alone units.

Rule 3. A system must be interfaced properly with its environment.

Rule 4. It is more convenient if subsystems can relate directly to functions but not at the expense of increased complexity.

Rule 5. It can be helpful to use more than one subsystem to provide a single function, as this allows redundancy of design. This benefit comes with a downside of increased complexity.

Rule 6. A single subsystem may provide several functions, particularly if the functions are related. Careful management of the interfaces is needed where a single element is part of several systems.

It is said, "Design for functionality, but partition for simplicity." Interface management can be quite complicated and make use of mathematical techniques by way of the so-called $N^2$ matrix technique. This is beyond the space available here to explain but suffice to state it is an orderly way to sort out how to best partition the various parts, not only in decomposition but also in their assembly and maintenance after manufacture.

## 5.6 Tree Diagrams as Generators of Ideas and Control of Activities

### 5.6.1 Examples of Use of Trees in Design

Decomposition is based on orderly dissection of a need into smaller parts, so its connectivity can be easily represented as trees with levels that move toward roots. It is actually a binary logic representational system.

Constructing these trees is a natural function for people. Creating them certainly motivates thought. An excellent, if rather old, tutorial paper has been published on their use for generating design solutions [6]. Trees can be used to:

- Develop solutions to problems;
- Show relationships between entities;
- Act as the thread of reports;
- Be used to set up rule-based problem solvers;
- Create system architectures;
- Assist in developing functional breakdowns.

Consider the simple design need to improve the performance of an audio system. Figure 5.7 shows an illustrative tree used to establish how to improve the performance of an audio sound system. The problem solution is started by first deciding the top-level issue (1.0 in the figure).

This is then broken down into the various means by which it can be improved. These are then broken down in turn to yield the full tree diagram.

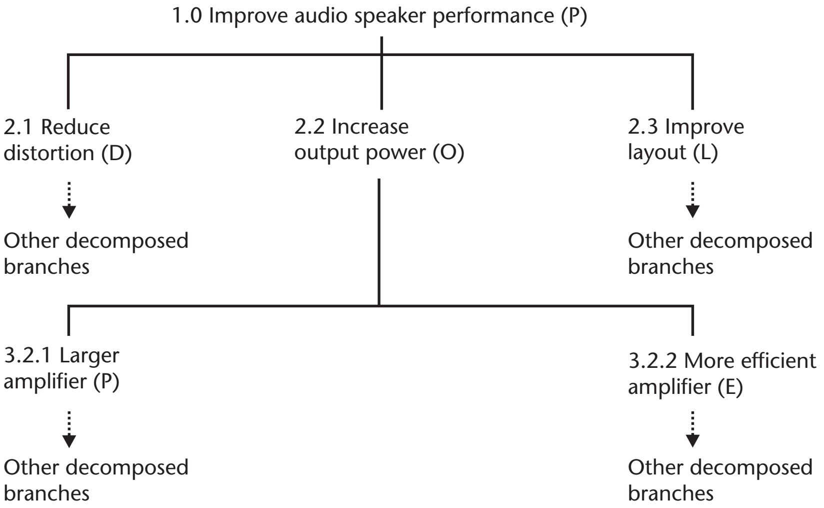


**Figure 5.7** Simple example of a tree diagram showing how to improve the performance of an audio sound system.

The basic tree can also be used to set up logical decision-making systems. If the rules by which the branches are divided are added, as in Figure 5.8, they can then be identified for use in an executable expert system for establishing things about the subject of the tree. A part of the rule set is then as follows:

| | |
|---|---|
| IF | Speaker output (W) increases |
| AND | Distortion (D) is reduced |
| AND | Positioning (L) improved |
| THEN | Audio output (O) is improved |

Obviously this example is simple; some trees can have hundreds of branches.

## 5.7 Functional Decomposition and Functional Analysis

### 5.7.1 Elements of Functional Decomposition

In requirements development, a key process is that of functional decomposition. This uses the tree breakdown representation and extends system decomposition to develop architecture, documentation, and analysis of the functions that need to be carried out. Here the initial tree is expanded within itself as well as downward.

The key thought drivers in carrying out functional decomposition are as per the acronym OFFER:

- *Objectives* (clear understanding of what is to be accomplished);
- *Functions* (what the block must do);
- *Factors* (men, money, machines, methods, materials, minutes);

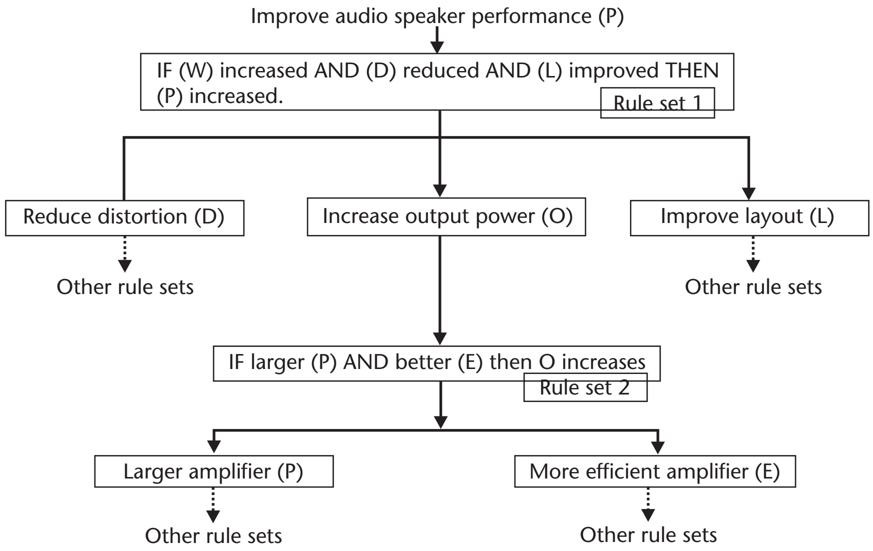


**Figure 5.8** Addition of branching rules to a design tree make it the core of an expert system.

- *Effects* (special appearances, ways to use, etc.);
- *Requirements* (usually performance related).

Rules for preparation of statements associated with the procedure exist for maintaining uniformity of numbering, linking, and symbology. Adoption of strict procedures and terms allow automation of key operations in requirements tools. For example, adoption of a standard functional level numbering system allows all items of the same kind, sensor specifications for instance, to be gathered into one report for all different systems of a major program.

Levels should follow a strict numbering convention. Names given must be succinct, meaningful, and unique. Each number has associated with it a description table giving key information as follows:

- Block number;
- Requirement description;
- Factors associated with that requirement;
- Effects associated with it.

Figure 5.9 shows part of the functional flow diagram (FFD) of a sensing system for determining the effectiveness of acquiring and displaying temperature measurement values.

The complete FFD for a system can contain thousands of such blocks and statements, each being a requirement. Shown is a selection at different levels.

Figure 5.9(a) shows the first level of functions, Figure 5.9(b) shows the second level, and Figure 5.9(c) shows the third level. Note that they each tie to the appropriate other levels. Each breaks down the link between two blocks in the level above it. Levels are added until it is no longer necessary, or possible, to break down a block any more.

For each block, there is need for a table of information, examples being as shown in Table 5.2.

Each block description must be described such that is has a single unique meaning. The description will use few words and they will always include a verb and a predicate, for example, "start motor."

Requirements are the specific requirements of the block and are usually related to performance parameters.

Selection of factors is assisted by considering each of the following six "M" issues:

**Table 5.2** Some Entries in the Requirements Sheet for the Blocks of Figure 5.9(c)

| *Block Number* | *Description* | *Requirements* | *Factors* | *Effects* |
|---|---|---|---|---|
| 3.1.1 | Provide physical connector | Physical cable and connector will connect temperature sensor to input amplifier | Must be light and flexible | Should be a COTS component |
| 3.1.2 | Provide input signal and return path | Provide EM shielding cabling and connector of 3.1.1 | Limit EMC noise to acceptable level | Use standard cable shielding |

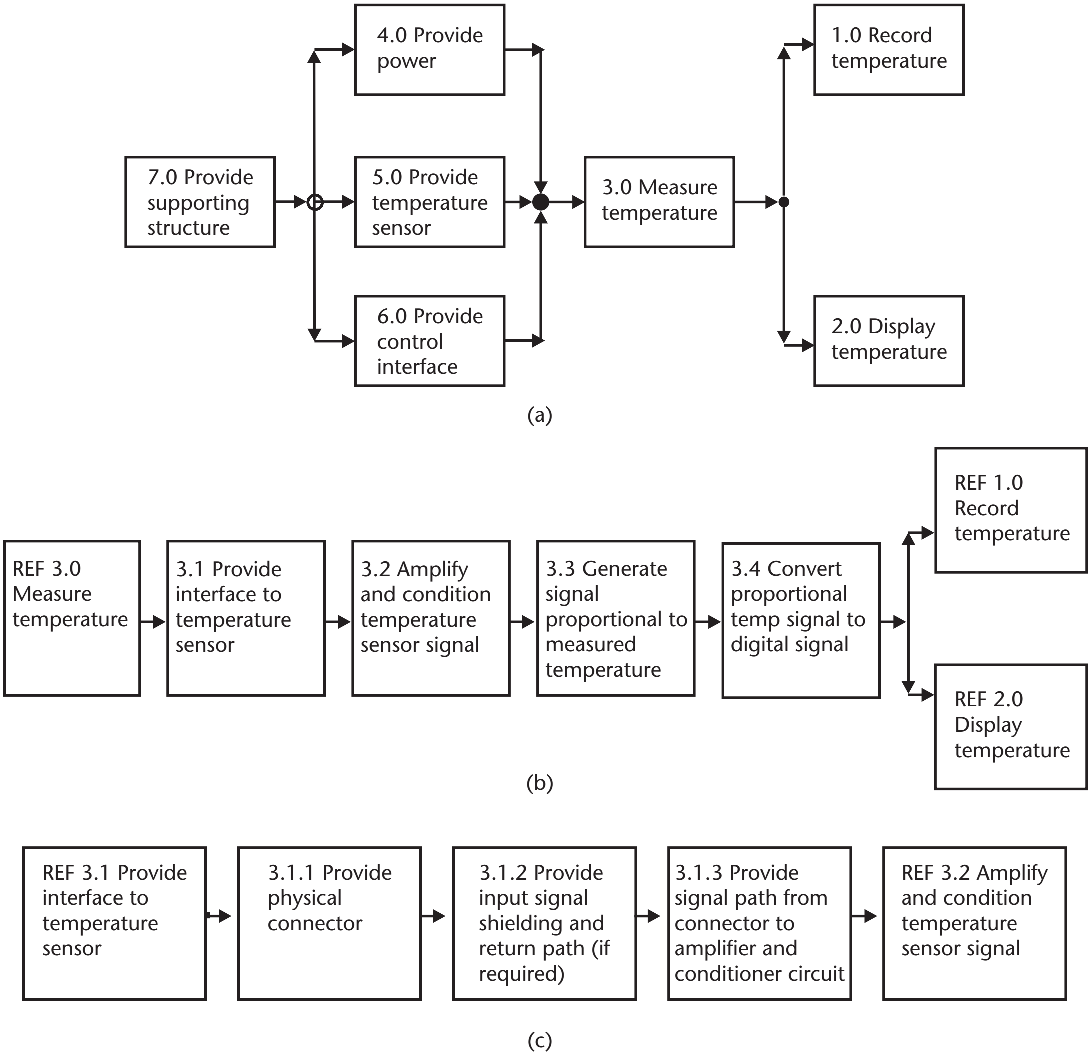


**Figure 5.9** Functional flow diagram for a sensing system: (a) first level, (b) second level, and (c) third level. (*Source:* Alan Dundas.)

- Men;
- Money;
- Machines;
- Methods;
- Materials;
- Minutes.

Effects are concerned with what is expected to be the outcome of the block build factors. These are intangible so they cannot be easily embedded into the FFD, yet if not given, could fail to be included in the final system.

Requirements extraction and management tools support automation of the routine activities such as correct numbering, but it is up to the user to develop good skills at filling in the blocks and descriptions. Standards are available that give guidance on functional decomposition activities.

The strength of functional analysis is that it facilitates requirements allocation on a functional (rather than physical) basis by providing sound abstraction at the higher layers. It is widely used and well understood, but not always done well. Where the FEL is too low this can be one activity that gets rushed, with subsequent errors appearing late in the development.

Functional analysis has a long history of successful application and its practices are well documented [7–11]. Texts covering the deeper mathematics that can be involved in the more sophisticated systems are also published [12–13].

However, it has limitations to be reckoned with. It does not deal well with replicated functions or address the performance of functions. Functions can easily become abstracted out of their environment. For example, the process can miss the fact that an operator may not be able to operate certain equipment in certain situations of use. It can add considerable overhead resource need for simple entities so must be balanced against the value of the insight gained. It is possible that the very process of completing the analysis can displace critical thought about underlying concepts and principles of operation. This is why the task of decomposition is not suited for junior staff with little experience.

Figure 5.10 shows how a stratospheric observatory project was partitioned at its first level. It is of interest to consider how the science instruments would have been tested. Where they are located in the figure shows their integration will only be tested when virtually the entire observatory element is completed. They need locating with different interfaces, at a much lower point, to ensure they can be tested at a time when they can be more easily modified if need be.

Requirements management tools are available to support functional decomposition as and generation of FFDs and their statements. They cannot add intellectual

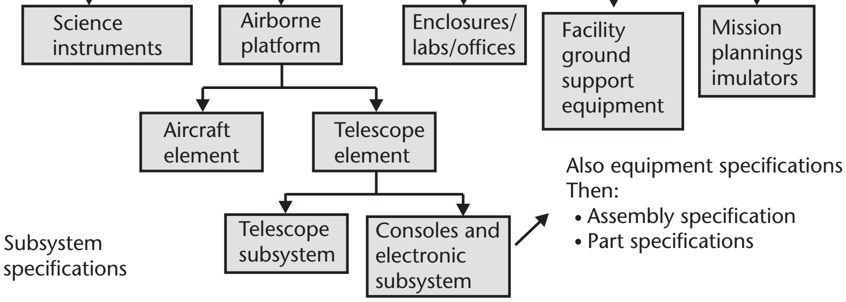


**Figure 5.10** Partitioning used in a stratospheric observatory project.

thought, despite some of the marketing words used about them. They can only provide as good a result as the care taken in filling in the links and statements.

Tools need careful selection; they do not all offer the same functionality. Automation support can only be expected if a part of the FFD task can be described formally. Watch for sufficient compatibility of these tools with the general computing applications of the project as a whole. More is given about tools in Chapter 4.

A good start to tool selection is to consult the INCOSE Tools Database [14]. The tool vendors located there will provide assistance and advice of considerable value.

## 5.8 Summary

This chapter has moved the discussion on to the fundamentals and practices of overall design.

It has explained where design fits into the life-cycle process and the types of relevant design that are practiced.

The nature of design has been overviewed as a process also covering its multidisciplinary dimensions in large projects.

Application of design fundamentals has been covered, showing how large projects are decomposed into smaller problems by the use of functional decomposition undertaken according to well-known practices. An example of a project structure has been given.

## References

[1] Asimow, M., *Introduction to Design*, Englewood Cliffs, NJ: Prentice-Hall, 1968.

[2] Sydenham P. H., "Disciplined Design of Sensor Systems—Pt 1: Types of Design," *Measurement*, Vol. 14, 1994, pp. 73–80.

[3] Sydenham P. H., "Disciplined Design of Sensor Systems—Pt 2: Knowledge Based Systems in Sensor and Sensor Systems Design," *Measurement*, Vol. 14, 1994, pp. 81–87.

[4] Rechtin, E., and M. Maier, *The Art of Systems Architecting*, Boca Raton, FL: CRC Press, 1997.

[5] OASIG, 1996 report; cited in Connolly, T., C. Begg, and A. Strachan, *Database Systems: A Practical Approach to Design, Implementation, and Management*, Reading, MA: Addison-Wesley, 1999, and on OASIG Web site.

[6] Marshall, R. C., "Ideas to Order," *Electronics & Power*, Jan. 1978, pp. 54–57.

[7] Burgess, J. A., "Organizing Design Problems," *Machine Design*, Nov. 27, 1969, pp. 120-127.

[8] Wymore, A. W., *Systems Engineering Methodology for Interdisciplinary Teams*, Chichester, U.K.: John Wiley, 1976.

[9] NASA, *NASA Systems Engineering Handbook,* SP-6105, June 1995.

[10] Blanchard, S. B., and W. J. Fabrycky, *Systems Engineering and Analysis*, (3rd edition), Upper Saddle River, NJ: Prentice-Hall International Inc., 1998.

[11] Sage, A. G., and W. B. Rouse, (eds.), *Handbook of Systems Engineering and Management*, New York: Wiley, 1999.

[12] Conway, J. B., *A Course in Functional Analysis*, Springer Verlag, 1997.

[13] Lax, P. D., *Functional Analysis*, New York: John Wiley, 2002.

[14] INCOSE, 2003, Tools data base on www.INCOSE.org.

## CHAPTER 6

# Design Concept and Requirements Development

The starting point of system development teases out the many requirements of the customer needed to carry out detailed engineering design. This chapter explains:

- The environment of development in which the customer, contractor, and other groups interact as requirements are extracted;
- Viewpoints of each of those groups, which differ widely;
- The nature of a good requirement and how each has to be teased out by a process of rigorous investigation, learning, guidance, and patience;
- Management of the requirements extraction process;
- The fact that the requirements are actually constraints gradually limiting design options;
- Ways for developing requirements;
- Nature, scope, and application of the operational concept (ConOps) methodology used as a focus for the requirements extraction activity;
- The content of a ConOps report;
- The way in which requirements flow down into technical specifications needed to carry out engineering design;
- Legal issues to be allowed for in the requirements extraction task.

## 6.1 Customer, User, Designer, and Vendor Relationships

### 6.1.1 Groups Involved in a System Design

This chapter deals with the starting point of a system's development; that is, the creation of a sound set of statements, called requirements, which define the needs of the customer.

Requirements are the first step in setting the direction of design possibilities. Care is needed in their development; if they are not right at this early stage, design work will be done that has to be corrected at a later stage.

However, before we develop the issues pertaining to requirements generation—also called requirements extraction or requirements engineering—it is necessary to become familiar with the differing points of view held by the various groups of people involved in a system development. Collectively, these impact on the requirements needed and their implementation. Stakeholder groups are:

- *Customer,* who pays for the development;
- *Users* of the system, who are not necessarily the customers;
- *Contractor,* within which reside the designers who perform part of the contractor role;
- *Vendors,* who provide subassemblies and components (includes the original equipment manufacturers (OEMs) for large systems);
- *The public,* who can greatly influence design, yet may never use or pay for the system.

Figure 6.1 shows where these groups fit into a generalized system development. Keep in mind this model of the situation as this account proceeds.

The process of development of a new system is complex, with everyone involved learning as the activity advances, and each person having a different standpoint in the venture. Many means have been used to minimize adversarial attitudes in a project—teaming and partnering, IPTs, contracts signed in terms of mutual trust, and more.

The characteristics of each of these groups are now considered to show how they are expected to behave. As we will see, project relationships can easily be adversarial in nature and thus pose difficulties to be overcome.

A somewhat negative description is given of each group to bring out likely factors to monitor. In practice, not all of the difficulties will arise in a project, especially where all concerned are working hard to reduce conflict situations.

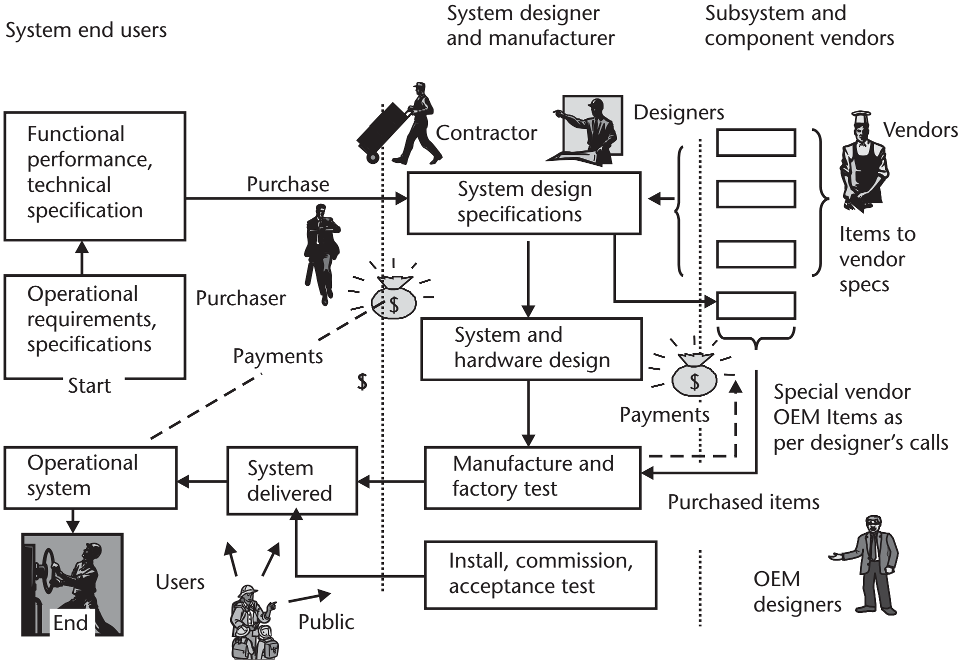


**Figure 6.1** Relationships between groups involved in a system development.

### 6.1.2 Characteristics and Viewpoint of the Customer

The system is being built for a customer with a need. This is the person, or more likely an organization, which predominantly dictates the design need. Here is where the project financial income is largely controlled.

Personnel of the customer organization will form key decisions about the need with, perhaps, specialist consultants involved to give advice. These needs-setters will have developed a high-level appreciation of what is desired in terms of a business strategy, or military need. They are less likely to understand, or have time to address, how their high-level concepts are transformed into a final system by the contractor groups.

Executives in a customer organization cannot be expected to know all that is needed, so they rely on others to assist them. Experts from the organization are used to create some form of a committee that provides the interface to the requirements extraction activity performed by the contractor. This group will work through the contractor's representative, who in large developments is the project or program manager from the project or program management office.

The customer is driven to:

- Achieve the organization's goals of delivered system performance;
- Need the system to be available by the agreed time;
- See the project come into operation within the budgeted cost;
- Follow shareholder and market forces;
- Seek maximum performance for money, often unrealistically if the pursuit is a short-term gain.

To these ends, the customer will often pick out the merits of different contractor solutions and ask for all of these good features in their system for the price of the lowest bid. This combination is usually not feasible because each of the good features is only obtained at the expense of less performance from others.

As they control the finances, customers usually want to make the critical final choice decisions. In this process, it is not uncommon for subjective feelings of high-level personnel to override objective argument put forward by the designers. For example, a senior executive of a large automobile maker gave a close friend a test drive of the prototype car. She did not like the sound of the exhaust. The outcome of that encounter was a rapid redesign of the muffler system, despite much market study and engineering design having taken place to see what was needed by the market.

At times, customers' internal issues can cloud judgments. For example, the need to go to market at a certain time can lead to inadequate systems being fielded, sometimes with disastrous results.

Customers can easily set unrealistic internal goals by believing that more performance is possible for a given cost than can be actually provided, building an inflated expectation into their business plans.

There can also be bias toward choosing "good name" contractors in preference to the bids of lesser known suppliers. Usually, the opportunity to tender will be limited to a selected set of so-called preferred tenderers. The customer does not always put together this set of contractors with the proper care it really needs.

In one instance, the preferred tendering company list for a major defense contact was created from one person's recollections of some company names that came to mind at the time. Little research into other potential contractors was done. No open call for expressions of interest to tender was published.

It is often observed that the customer's decision-makers place a surprising level of reliance on often overly simple performance and costs metrics, not appreciating their possible shortcomings or poor relevance to the whole system choice. Comparative trades studies of candidate proposals can easily be biased by selective use of metrics and data.

Many systems bids provided are not able to come up to scratch but this is often not detected until it is too late. Customers all too easily go for the lowest tender price without giving sufficient consideration to the reasons why that price is low compared with the others.

The customer can feel very much in control up to the commencement of a contract, but the situation can change from then on. Once the contract is signed, customers often have to accept an inferior completion for many sound, but unfortunate, reasons. The customer-to-supplier relationship can change to give the supplier increased influence over final acceptance criteria. Seniority of command in a corporation or a defense hierarchy does not necessarily mean high-level capability in requirements capture and system acceptance exists.

Some reasons for apparently acceding to a supplier stance are that the customer:

- Will need to have functionality available at a given start-up date;
- Has to accept the reality that the task set may have been overly ambitious;
- Cannot change suppliers at a later stage because no other supplier can complete the system any faster;
- There are insufficient funds left to pay for a second attempt by the time difficulties being experienced are exposed to the customer;
- Will need to save face, especially in highly charged political situations.

Many systems are accepted as complete when they are still really prototypes under development.

The customer needs to be satisfied that development progress is truly up to the targets as each payment milestone arrives. To this end, the customer needs to be experienced in performance metrics and how they are used, not only to assess finally delivered systems, but as maturing entities all through the development.

The customer-to-contractor interface can be carried out with reduced ongoing conflict, and less late error, by giving quality attention to the early-up requirements extraction process. However, all too often this stage is rushed to get design staff onto the job, thus demonstrating apparently sound progress.

### 6.1.3 Characteristics and Viewpoint of the User

The user is often not the initiating customer of the system. The user's main drivers are:

- Effective execution of its purposeful role;

- Suitability for that purpose in terms of ongoing operation;
- Low risk of nonoperation because failure to operate can be expensive in terms of money, or in defense systems in terms of personal injury and lost lives;
- Safe operation.

Commercial systems use extensive market surveys to develop the user needs role for a system development. Defense groups use computer models and real trials to establish needs.

For all of these investigations, it is commonly seen that the end-user has been too far removed from the design development process. Often the user only has the opportunity to rate their acceptance of a system after it is fielded. One example is the market failure of a new automobile model that was technically excellent, but it did not sell because the public did not like the subtleties of the human factors aspects of the vehicle.

The users are the ones who will need to make the system work, idiosyncrasies and all. They also will often have to service the system. In these circumstances, they give little credit to the niceties, elegance, and detail of design solutions; they just want to use it with good outcomes. The well-preached design philosophy "keep it simple stupid" (KISS) applies for them.

Too often the upshot is that users have to accept a deficient system, a situation that is not effective for all concerned. As an example, army personnel, landed in a hostile situation, found their provided radio communication system was not effective for local communications. They made use of their privately owned commercial cell phones to get around the shortcoming.

Therefore, user input is highly essential in the early stages of a development. Designers, in situations where the needs are not made clear, often second-guess the user's needs, which can be dangerous. IPT-style project operations contribute greatly to improving the contractor-customer-user relationships. Many success stories support this more recently adopted kind of development.

### 6.1.4 Characteristics and Viewpoint of the Contractor and Designer

In most projects, a main contractor—usually known as the prime contractor—is appointed to pull all of the system development together. This prime organization generally (but by no means always) has the financial size to support the work to be done before payments are made, and is also able to cover the costs of any lateness, budget overruns, and litigations that arise.

The kind of contract given can vary widely (see Section 5.4.2). Contracts can cover one or more of the SE life-cycle stages: concept development, feasibility studies, design and manufacture, installation, operation, upgrades, or combinations of these.

Contractors may be different for each of the stages. Once started, projects can also be abandoned at any stage; many aircraft designs do not get past the concept stage or go into production.

Sometimes the customer is also the system developer. For example, many communications suppliers build systems in speculative anticipation of sales via their own supply and service subsidiaries or other suppliers. In these cases, the development and manufacturing operations are usually kept separate from the supplier subsidiary.

Prime contractors rarely have all of the work performed within their own staff and facilities, passing out some of the work to subcontractors.

It is not uncommon to have several prime contractors appointed for various aspects of larger projects. Interestingly, the prime contractor is not always larger than the subcontractor, this situation arising, for example, when a large organization wishes to develop the concept for a major development.

As the prime contractors bear the major technical and financial risks, they will tend toward giving less for the money spent than customers expect to get, both being driven by their own internal forces into overlapping aspirations. How well a contractor performs is impacted upon by both the customer's ability to give reasonable requirements and also by the subcontractors that supply components and subsystems to the prime contractor.

Contractors are often required to show how they would execute the work in order to be awarded a contract. However, they would rather not have to disclose how well things are going as that might not lead to beneficial outcomes for them. They are inclined to hold back reporting on negative issues such as lateness in delivery, budget overruns, and lack of scheduled performance. A USDoD study of 100 "failed" programs found project managers were inclined to believe that given more time the problems could be fixed, so they waited for a while (too long, in fact) before data on such issues was released.

Contractors are sometimes able to take advantage of customers, the latter often not being experienced enough in deciding requirements and leaving it to the contractor to make key decisions.

Suppliers of systems and components to contractors are able to plan defect and lifetime failure rates to assist their profit-making, and have little incentive to supply a better-than-called-for system.

Long-term involvement for the prime contractor is thus often problematic. This difficulty has to be factored into the design activity.

Not all of the above situations will arise in a given development, but they do need to be guarded against.

The ever-present conflict of interest existing between the parties involved can be contained and controlled by well-written contracts executed in the atmosphere of a great deal of trust and goodwill. It also means all concerned need to be vigilant and experienced—trends in defense acquisition have worked to generate the so-called smart customer.

Engineering designers are part of the various contractor entities. Their loyalties are to their employer. They work to specifications that emerge from the requirements extraction process. Designers are not usually involved in requirements development, as that work will have taken place before they start up their tasks. They must have confidence that the earlier processes have delivered sound requirements to them.

The situation is not always perfect. For example, in a large project, two teams were later found to be designing the same assembly without knowing it—requirements checking had failed to find the duplicated requirement.

Recall that an engineering design is a voyage of discovery that is best based on hard science and sound engineering. Despite good work and sound practices there will be need to make adjustments to the design, called rework or iteration, as interface requirements clarify through cooperative activity between all of the groups.

Engineering detail designers are not that appreciated in an overt manner, unless, perhaps, if they are later hailed as the inventor of something historically important or interesting. Some large engineering systems have had a particular person associated with them: Brunel for bridges and tunnels, Whittle for the jet engine, Cockcroft for the hovercraft. Today, engineers usually work in largely anonymous teams.

The situation climate in which the engineer works is summed up by the statement that when a space shot is successful it is a great scientific achievement, but when it does not work it is an engineering failure.

Unlike some professionals, such as lawyers, where time is billed to a client for virtually every service given—phone calls for booking meetings included—engineering designers are expected to give lots of advice for low reward.

Design engineers, then, have to accept much traceably auditable responsibility. They tend to work at some distance from central management. They rarely have to face the public over their work in the same direct manner as does a politician or a medical practitioner.

It is widely observable that engineering designers work for the self-satisfaction of seeing a design done well and properly. They tend to be very critical of their own and their team's performance, concentrating on the negative issues that need attention more than on the joys of design success. The designer is, after all, a person in the development cycle who has to make decisions that result in actual things being made to operate according to the customer's needs.

As design work is carried out, better solutions become apparent. As a result, designers have a tendency to constantly want to improve their designs. Often their work has to be frozen to allow production to start; they can see still better ways to solve issues and want to improve things.

### 6.1.5 Characteristics and Viewpoint of the Vendor

Contractors create much of a delivered system from already available assemblies, or from bespoke (also called custom) designs provided by specialist suppliers. An automobile, for instance, has several distinct systems (electrical, fuel, braking, entertainment, and suspension subsystems) that are rarely made by the vehicle maker. Such suppliers are known as original equipment makers (OEMs).

OEMs are important players. They do their own R&D to keep abreast of their competitors and will carry out special developments if contracted to do so. They need to sell their designs into large projects to get returns for their R&D effort and to amortize the cost of their factories. Long-term sales are important to them as they operate in long time frames.

As manufacturing processes improved, the need to supply parts ever closer to the time of their use—the just in time (JIT) principle—has made parts suppliers ever reliant on contractor orders. Conversely, their need to deliver in time gives them some leverage over the contractor. Many design decisions are not in their control yet they must provide the definitive equipment. They will lose major contracts if they do not perform in the short-to-medium term. Designers in this situation need to think and behave differently than a contractor.

OEMs, however, do not directly take the brunt of user complaints. The public sees a product recall as being a prime supplier's deficiency, not that of the OEM provider. For example, a vehicle recall for a defective automobile braking system will be publicized in the name of the automobile maker, not the brake-system maker. This could be interpreted to mean an OEM can hide behind its somewhat unnamed position, but obviously the prime supplier will usually have alternative suppliers available if dissatisfied.

Being a sole and wanted supplier of unique products is a nice market position to have. This situation was extensive in electronic systems a few decades ago. Each computer system had its own maker-specific operating system, input and output port connections, communications standards, and case construction. The disadvantages of this were obvious to the purchasers, who were very constrained in what they could purchase for upgrades. Gradually, the open system (OS) connection concept developed. Today, plug and play interfacing is now the norm, and all concerned have benefited because the whole area of supply was able to expand the available options, thus increasing the total market.

When selecting OEMs it is advisable to use, where possible, parts and services that have availability from at least a second source. A large amount of vendor-supplied components and assemblies are standard and can be used as replacements.

The OEM seeks to minimize cost to produce, maximize income from sales, and to stay in business in the long term. Be on guard with vendor inputs; to meet their business targets, they will often not provide design support for their products. For example, reliability data is not always available for the low-cost power-point voltage converters used with electronic equipment. If these are chosen for COTS use, it will not be possible to carry out sound reliability analysis studies for the overall system.

As shown in Figure 6.1, two main kinds of vendor-supplied items exist. First, there are routine items such as are offered from a catalog. These are usually kept in stock for fast delivery, but major size orders need to be scheduled into the vendor's production runs and thus could take months to provide. Manufacturers may swing all of their production output over to their large customers, leaving smaller projects with lengthy delivery delays.

The second kind of vendor item is the "special," which is a modification of a standard catalog item or a totally new design. Special items can be very costly to produce in small lots, take considerable time to supply, and possibly will not be well proven. For instance, asking for a batch of common electronic resistors to be provided in different strip mounts, or painted differently, will require changes to a production line set up that are expensive and time consuming. A rule usually invoked in system design is to use already made and proven items. Use of the just-released new model may well provide a market edge, but if delivered late or not working to specification, it may cause loss of the market completely.

The buying interface of OEM suppliers with users and purchasers is at a distance. Designers need to have a well-developed and responsive interface with the OEM development and manufacturing units, as that will assist in getting access to design data of the vendor's parts.

### 6.1.6 Public Viewpoint

There was a time when engineers could generally design anything they wanted to without being seriously challenged by societal groups. Unsafe systems such as the automobiles of the 1950s and ’60s were given massive engine power without commensurate chassis design, braking, and collision strength. They escaped public comment until ways were found for the public to influence the designs. Safety in systems design is covered in Section 9.5. Legal issues are dealt with in Chapter 10.

The public at large have been able to impact designs regarding their reliability, safety, appearance, environmental impact, recycling waste, pollution, and the like. Interestingly, this happens despite the fact that this group is often not directly paying for the development or being the user.

Defense equipment and its use are also under public scrutiny today more than ever before. As peace-making forces go into action, a media TV camera shows the world how the activity is being carried out. This has become known as the CNN factor (after the particular style of TV news reporting that took place during the Gulf War in the 1990s). When an aircraft carrier battle group is planning an action, the battle group commander is consulting the military lawyers on board about the legal aspects of the strike. A good example is the situation regarding the residues of a battlefield encounter, for these are now the subject of considerable public debate and criticism.

Public intentions often drive issues more from the heart than from hard engineering and scientific reality. Civilian laws can severely limit design horizons. For instance, to carry out a simple military test in the United States can require over 150 environmental regulations to be studied and met before it can undertaken.

Well-balanced viewpoints on environmental issues are not always present. It has been asserted that the environmental impact process, which has to be approved before most major projects can start up, is flawed. This process seeks to record the current state of the environment related to the project before the development takes place. To do this, numerous measurements of easily recognized and available parameters are carried out as part of the approval mechanism. These parameters are often poorly related to the metrics appropriate to the critical issues involved. A plan for monitoring critical issues is often not in place to ensure that those issues are being held within limits over time. Instead of use of metrics to detect trends toward undesirable states, trigger levels are set for which monitoring can only tell when they have gone out of hand; which is usually too late for easy remedial action.

Politicians and other public leaders often get caught up in a development task, adding a political element. A project parameter can be dictated by political expediency that overrides use of best practice. For example, there are agreements that require organizations of stated countries be involved despite their lack of best practice to offer to the project. Social welfare schemes are implanted into projects to ensure groups of disadvantaged people are employed in preference to the best available. These kinds of conditions further add constraints for the designer to work within.

An example of how this can affect the complete system design is the political and economic decision made for the U.K. rail network system. Government adopted a safety choice for the national railway system of implementing a rapidly introduced, low improvement signaling system instead of a much longer term, but superior, one. This political choice was made to suit the public purse and public perception considerations.

Politicians often want to support many project start-ups with low FELs rather than select a small number that are properly funded with adequate early funding.

Public groups clearly influence progress; they always have acted this way. The Red Flag Act of the early 1800s made it necessary in England to have a flagman walking in front of the new steam-breathing omnibus carriages. These carriages could drop cartage prices between major cities to a tenth but the commercial forces of the canals and railways were at work slowing down progress.

As a parting example, the almost unbelievable account of the USDoD electric boat project of the 1970s shows what can happen in the engineering of systems. That project development and management was so influenced by the admiral (who was the customer, not the contractor!) that he was personally controlling the contractor and its personnel appointments on a daily basis from his office. He also managed to close down a significant hull concept development that was able to give a far better solution for a submarine design. It was competitive to his preference! The investigative journalists' account of this is a good record of defense acquisition gone wrong, and a must for designers to read [1].

This section has been provided to alert the less-experienced designer about the forces that could be at play as a project develops. In the early stages when the requirements are being set, these interactions are working hard to influence the key choices that later impact design flexibility. With an appreciation of the characteristics of those involved now in place, we are now ready to explore how requirements are generated for a project.

## 6.2 Requirements Generation

### 6.2.1 Teasing out the Requirement

Establishing the set of requirements for a project requires patience, understanding, and experience. It can take considerable time to assemble a sound set of issues that characterize the customer's need. These must be set up carefully and completely and rarely can be done well enough. The topic of requirements is such a large field of research that it supports national annual conferences, meetings. and sessions. It has had major resources allocated to it over a decade of university research in all Western countries. A technical committee addresses this issue, for the SE situation, in the INCOSE organization.

This section can only give an introduction; more detail is found in several texts and standards on the topic and in numerous published papers and standards documents [2–7].

Requirements cover much more than the operational task the system has to meet. Need should be based on real deficiencies: a current system is inadequate, is unavailable or unsupportable, or is too costly to operate.

The statement of need should be presented in specific qualitative and quantitative terms, there being sufficient detail to allow the systems engineering process to proceed in functional terms.

The requirements extraction activity generates the inputs for system specifications that, in turn, establish design requirements. First then, let us look into how to approach the development of requirements.

Requirements extraction is just that—extraction of hopefully "hard" objective detail from what is initially often quite abstract thinking. It is usually necessary to provide assistance to the customer to transform the initial expressions of need into the format and knowledge content needed to flow down tasks to the detail engineering activity stage.

At the time that serious requirements extraction commences, the need will not be well teased out in the definitive terms needed by designers. Skilled requirement engineers must work up the detail from the various needs statements and with the client.

Customers are not experts at this task, and usually will not have approached establishing their need on well-structured lines that suit the extraction process. To get a project approved they will have been working from a different direction to the designer's need, coming in, instead, from a business plan or budget bid that makes its case in terms not suited to requirement extraction.

For example, the starting point for the requirements extraction activity of a multimillion-dollar development was a two-page statement provided as an appendix to the organization's bid for funding. Consideration of this statement showed it had no clear logical structure but was, instead, a somewhat rambling set of things that could be done. Few quantities with metric properties were present to give size and shape to the expected development outputs. In addition, the nature of the final product was only vaguely described.

Requirements elicitation starts with formulations of the key factors, often called the critical issues (CIs)—via a process of discovery [3]. It is a detective process carried out by the requirements extraction team on behalf of all involved in the development of a system. A representation of the steps of this discovery process is given in Figure 6.2.

Although the customer will usually provide a written needs statement, the contractor actually prepares the first requirements list. This developing document needs to be regularly checked with the customer to ensure it is what is needed. In this activity it is important to ascertain that the customer is doing a sound job of verifying suggestions; they may well be distracted by other more urgent internal matters.

Several facets of the extraction process can be defined and expanded.

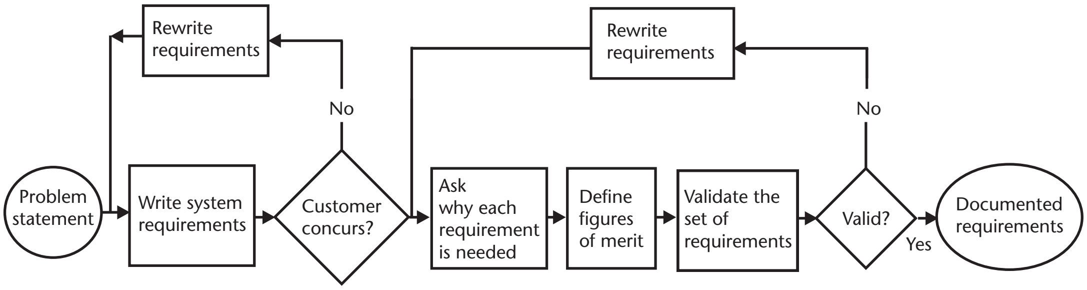


**Figure 6.2** Requirements discovery process. (*Source:* [3].)

### Issue Formulation

Always keep in mind that this is a most critical step in the life-cycle process; this is where the signposts now uncovered set out directions of effort that can be very expensive if not correct. Major projects often create special contracts to develop the concepts so that sufficient attention is given to getting these initial activity signposts right.

As the customer is unlikely to be able to adequately define the issues, and the contractor cannot yet fully understand the concept that sits in the mind of the customer, it is necessary for the contractor to ask many questions. Use of requirements workshops is a sound idea. These are conducted in the form of a several-day brainstorming session guided by a moderator coming from outside the project. Specialist consultants are available to assist setup and also run these events.

A client needs a system that:

- Provides operational capability (i.e., does the right task);
- Possesses adequate operational suitability (i.e., does the above tasks when needed, for as long as needed);
- Meets certain cost conditions for ownership and ongoing operation;
- Fits within a host of legally required environmental conditions;
- Meets appropriate health and safety regulations.

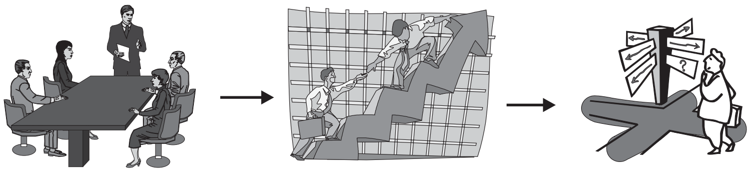
To provide this very large list of must-haves, it is necessary to tease out a long set of requirements. A sound way to get started is to generate an operational concept or ConOps document for the project (for detail of these refer to Section 6.4).

After becoming familiar with every statement about the project that is then available, the next step is to explore the nature of the problem to be serviced. Key issues to address are:

- Why is this system needed?
- What role does it fulfill?
- Is it a new system with few precedents, or is it an updated copy needed to give your customer a place in a market?
- How does it provide for that need?
- Is it a major activity in that will need to push forward the technical edge, such as in defense?
- Is it a new innovative use of existing largely proven technology, such as a new generation telecommunication system?

Differences realized here will highlight many requirements issues. This is the time to also make a short study of the type of system needed in terms of its hierarchical and organizational natures (see Sections 1.3.1 and 3.5). The kind of development it will be will then show up, revealing the generic group of engineering solutions that might be applicable.

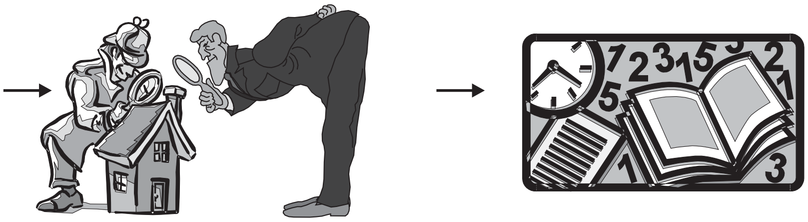
As depicted in Figure 6.3, this activity involves looking for directions as well as specific engineering needs. Engineering design must start into its detail only when the needs and constraints are adequately appreciated. It should not leap off with a



Customer sets a need

Guidance is needed to assist customer

Is about setting directions for designers



Is an ongoing, highly iterative investigation

Results in an objective report listing requirements statements

**Figure 6.3** Requirements engineering is a matter of setting up signposts that lead to solutions.

specific solution at this early stage, but be top-down driven from a sound requirements extraction.

Next, a situation assessment should be developed. General approaches to apply here are:

- What should be?
- What factors matter over time?
- What to do and how to do it?

An important aim of requirements development is to be able to recommend a preferred course of action, usually by pursuing two or three of the most promising solution directions. The most likely approaches need their performance, effectiveness, maintenance, and logistic support to be made clear.

This critical identification step is all too often jumped into using intuition alone to start an investigation of requirements. That may well start to motivate the mind but its outcomes must be followed up with analytical assessment of the findings. When taking the analytical view, keep in mind the need to arrive at four key components:

1. Definition of a goal for the system;
2. Knowledge of the current position with respect to the goal;
3. Knowledge of the environmental factors and influence parameters;
4. Determination of a plan to achieve the goal, given the above knowledge then being available.

It is helpful to create and act out scenarios. Run a walk-through for each idea. Do storyboarding. Conduct models and simulations using suitable tools, topics covered in more detail in Chapters 4 and 11. At this early stage, avoid use of models that need precise information, for their operation can bog down progress and smother innovative thought. Run simple simulations. Do many different things to allow the need to be viewed from different angles. Conduct exploration workshops.

It will not be feasible to address every issue that is discovered. Concentrate on the critical issues; large systems will identify hundreds of CIs. Learn from similar past projects; many CI definitions and metric units can be reused.

CIs group into four kinds to do with:

- Operational task (What is it to do?)—see Chapter 9;
- Suitability (Will it perform when needed?)—see Chapter 9;
- Political, social, legal, environmental (What are the key constraints?);
- Programmatic (How well will the contractor perform in the development?).

### Maintenance and Support Requirements

Being able to provide adequate operational service when needed is as important for a system design as is making sure it does the right job. Ability of a system to successfully fulfill its mission objective is highly dependent on the effectiveness of the support infrastructure that is provided by the design. This is variously called the reliability and maintenance (R&M) "ilities" or special functions aspect; see Section 9.2.

A maintenance concept must be developed in parallel with other required systems concepts. This stems from the definition of system operational requirements and evolves into a maintenance plan. Life-cycle costing could be a major consideration at the requirements extraction stage.

### Requirements Analysis

As the operational needs are teased out and transformed into requirements, they need to undergo analysis that is as objective as is reasonably useful at this stage. The main areas of interest to consider will usually be:

#### Operational distribution or deployment of the system under development:

- Geographical considerations.

#### Mission profiles or scenarios for the system:

- Identification of prime and secondary missions;
- What must the system accomplish and what functions must be performed? Define operational profiles in terms of utilization versus time and energy use versus time.

Performance and related parameters:

- Description of basic operating characteristics or functions of the system for such parameters that fit from range, accuracy, rate, capacity, throughput, power, output, size, mass, and so forth.

Utilization requirements (leads to determination of some of the stresses imposed on the system by the operator):

- Anticipated usage: hours per day and duty cycle.

Effectiveness requirements (together these define how effective or efficiently the system may perform):

- Cost;
- Reliability, availability, maintainability;
- Personnel qualities, skill levels.

Operational life characteristics:

- Length of operation;
- Duty cycles of operation;
- Maximums and minimum/maximum cycles of stress.

Environment (for system's operation, transport, and storage):

- Such parameters as are appropriate from temperature, shock, vibration, noise, humidity, airborne, shipboard, and so forth.

### Requirement Formats

Requirements are best prepared as descriptions of the operation of the system under development, and should not state the design solution—that emerges later. Too often writers of requirements fall into the detail design mode of thinking, as that is where they are more familiar with ideas. Avoid writing any requirement that dictates a technical solution.

Small projects can maintain a hard copy record but that form cannot make use of the useful support functions of tools such as searching, duplicate checking, prioritizing, status reports, autolocation, and modeling of the full system.

When the number of individual requirements exceeds a few hundred it becomes essential to use a requirements management computer-based tool. It is usual in large projects to end up with as many as 15,000 or more individual requirement statements. These all fit into a tree structure created by intelligently generated functional decomposition activities starting out with a few hundred CIs.

Requirements management computer-based tools are available to manage the various sizes of development. Tools will support the task well, possibly reducing the requirements engineering task from years by the older longhand method down to months when tools are used. Caution is needed. As tools allow rapid generation of statements, it is easy for poorly stated requirements to result.

If the requirements elicitation process were perfect, all parts designed and made would integrate to form the customer's required system. This is rarely feasible for, recall, this is a journey of constant discovery for all involved. Lots of iteration is essential at this stage. Typical reasons for iteration might be:

- A more efficient system decomposition becomes apparent;
- Customer needs to inject an allowance for a market change;
- Analysis of the concept proves a critical subsystem concept is not feasible.

In such cases there is, here, a distinct danger that the necessary adjustments will not be made leading to very costly rework later. Rework at that time is the cheapest to do, but this may not be accepted then for reasons of haste. SE management will need to make the case for more study and give sound reasons for the resultant delay.

Detail design should only start after careful study of the requirements has developed a sound set of requirement statements that have been carefully and fully validated.

### Features of a Requirement

Pointers on the features of a good requirement have been published [3]. They are only guides; there will be exceptions in their application. These are now summarized from that source:

1. Describes the what, not the how (does not preempt the technical solution or stem from a likely solution).
2. Is atomic (is not part of another statement and contains one idea only).
3. Is unique in its labeling and content (tools are able to test for duplication provided the format and terminology of description used is well controlled).
4. Is documented and accessible to those who need to know.
5. Identifies with an owner who alone controls its use.
6. Is approved, not generated without authority.
7. Is traceable up the requirements tree to its source.
8. Is really necessary (overspecifying in the not-needed aspect and better made than is needed are both costly).
9. Is complete (clear and concise).
10. Is unambiguous (use simple language; avoid synonyms and homonyms and meaningless words. A well-run project will make use of a thesaurus of terms and styles of expression).
11. Is not always written (common sense stuff is not written down but watch for what is regarded as normally known knowledge).
12. Quantitative and testable (where possible, but not overdone by going too far down the requirements tree levels).

13. Identifies applicable states (qualifying these issues in succinct ways is essential but an art to master).
14. States assumptions (gives confidence and shows the matter is properly addressed; include written statements of all assumptions, including those that seem poor at the time, as that advises those following the project of the rationale in force when the statement was generated).
15. Use of “shall”, “should,” and “will” (“must,” “might,” and “routine,” respectively. These definitions usually form a part of the requirements document).
16. Avoid certain words that imply objectivity but do not actually help (“optimize,” “maximize,” and “minimize” are not to be used as they are not provable; nor “simultaneous,” as is not commonly understood in the same way).
17. Might vary in level of detail (set to suit user of statement).
18. Contains date of approval and approver.
19. States rationale of statement (set down a flow of logic on how the requirement was developed. Seldom done as it takes time and can be seen to indict the developer if it proves to be incorrect in some way. Would be most useful to understand the thinking behind the statement).
20. Respect the “media effect” (be guarded; take care not to create an opportunity for the media to quote it, out of context, with a negative effect on the project).

### 6.2.2 Managing Requirements Development

High-level considerations arise where the customer specifies the requirement. Lower levels of the requirements trees are the responsibility of the contractor’s organization. It is the role of the customer, with assistance from the contractor, to select the best option for a high-level concept. As already mentioned, some kind of requirements interface group is needed. In the IPT methodology that team does this.

Where the government is the customer, as it is for the national telecommunications, defense, and utilities areas, the task of setting up much of the design options detail has often been carried out by a government agency with support from consultants, and maybe contractors. This situation arose when the government owned and operated the advanced design, test, and sophisticated manufacturing facilities that industry was considered to not to be able to provide. In these cases, the government agency carried out the system design, issuing the detail within the tender to build the system. The government then carried most of the risk. As a result of this practice, they often overspecified materials and components using conservative standards that were not tracking commercial best practices.

This practice has largely moved to now place more of the development risk with the contractors, who must bid competitively to win the contract. This assumes that the contractor is capable of delivering the task. Audits of contractor capability are commonly done but it is often the case that the customer is not experienced enough to be able to make sound judgments.

Whichever type of customer-contractor relationship is used, it will not be perfect.

A problematic issue is how to assess the degree of detailed work needed when generating requirements. Gauging how far down the hierarchy to go with requirements development needs management decisions and supervision. The need here is to carry out sufficient work to be sure that a viable solution exists, or can close off an option with a substantiated case being in place that justifies it is a poor choice.

A balance must also be maintained between the need to keep several parallel solution options open against the cost of following up too many.

### 6.2.3 Suggested Complete Requirements Generation Process

The discovery process given previously in Figure 6.2 can be extended to show its part in the whole requirements development process. Figure 6.4 from [3] gives a suitable flow chart of the steps involved. It is useful as a check for designers to verify that the task is being done well enough.

While appearing to be a process that has a smooth flow-through, considerable iteration is essential around all possible loops within the whole. It may be desirable, on resource grounds, to move through the steps rapidly by not checking all interactions of decisions made. That practice, however, will assuredly lead to gross errors being made that need later, costly, correction or that lead to project failure.

As each requirement is generated, it is necessary to establish how its outcome will be tested and evaluated. A nonverifiable requirement would leave unknown performance behavior in the final design, possibly only being tested in service. In short, a requirement must be testable to be included.

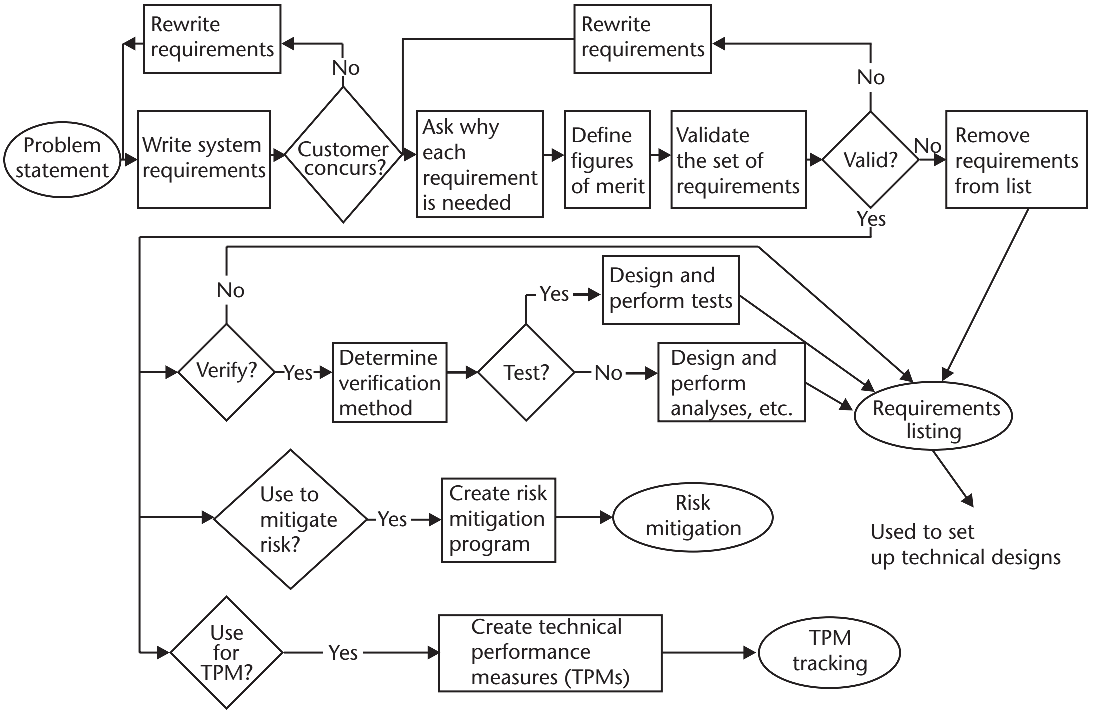


**Figure 6.4** Whole requirement development process.(*Source:* [3].)

Note the clearly stated use of verification in the process shown. Included is creation of the appropriate performance measures that will later allow tracking of the progress of the design. As has been covered in Chapter 2, depending on the performance control thinking in use on the project, there may also be an integrated parallel development taking place that generated a test and evaluation master plan (TEMP)—see Section 2.7.

### 6.2.4 Constraints Imposed by Requirements

Another way to appreciate the finer points of requirements generation is to look at how they impose constraints on design solutions. As seen in Section 5.3.3, design is a process whereby a development task starts with full openness of choices, the aim being to select best options that collectively lead to the detail of a specific realization. It is, therefore, one of progressive, considered, and moderated development of constraints until virtually only one design schema remains.

Constraints start to appear when the customer sets the need; they close off solution options not required by the customer. Care is needed to not close down options too early, as that may not lead to any final solution at all when the detail is worked up. Closely constraining the situation at this stage gives the designer less freedom within which to find the best solution.

The customer can certainly indicate preferred constraints but should understand clearly the impact of these constraints. The more the customer specifies, the more is dictated the solution.

Key types of approach are:

- Generic problem statements that allow maximum supplier freedom;
- Cardinal points specifications that allow some supplier freedom;
- Detailed technical specifications that define a specific solution.

These approaches all have their place depending on how sure the user is of the needs. That depends on the degree of quality work done by the customer. Customer-generated statements need careful validation by the contractor for unfortunately customers often rush into assuming given solutions.

The gradual closing effect of these options is seen from analysis of the various situations. Figure 6.5(a) shows the generalized illustration of the relationship between the range of solutions and the number of independent constraints for the three cases given above. Figure 6.5(b) shows how the designer's options are reduced as various strategies are employed, and how the final need to set technical specifications further limits the design options.

Contractors, as shown in Figure 6.5(c), can chose options that suit them, further limiting solutions that can be used. Some factors influencing the contractor's situation are that they:

- Will be influenced by their past experiences;
- May have a limited range of creative ideas;
- May wish to use existing subsystems or components;
- May be bounded by existing manufacturing capability;

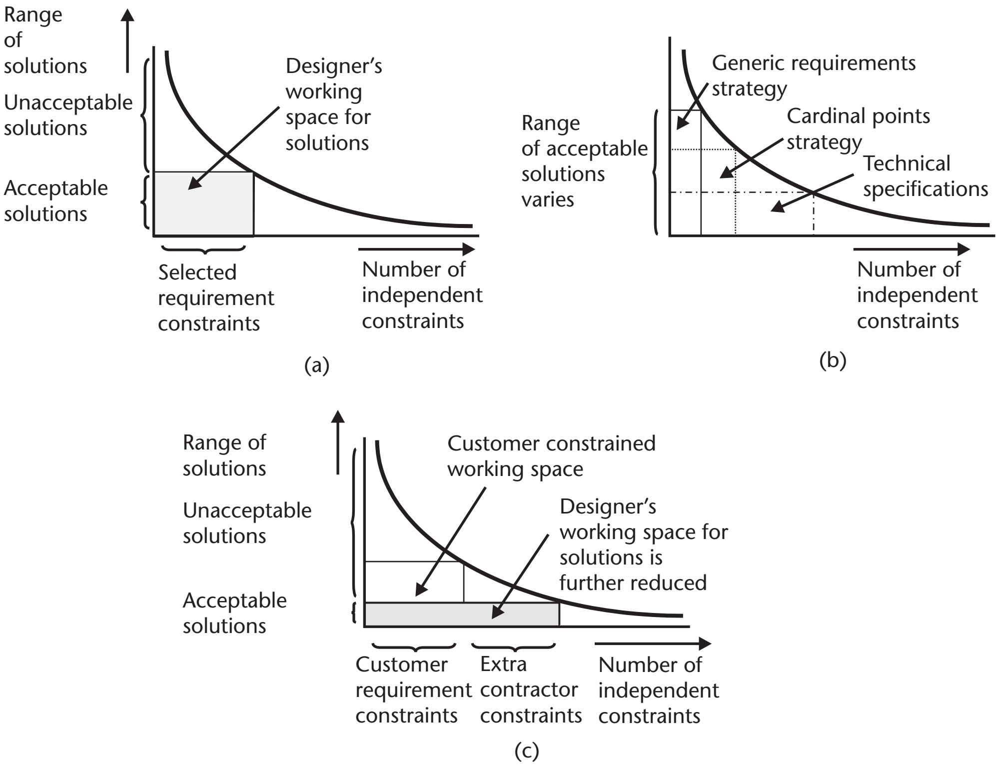


**Figure 6.5** Design options change as constraints are added. (a) Setting constraints separates out the available solutions. (b) Differences between types of specification strategy in design options. (c) Addition of contractor constraints further limits solution options. (*Courtesy:* Ken Hambleton.)

- Will need to maximize profit or return on investment.

Constraints are also added by their vendors, who can only supply a certain set of affordable items in a given time frame.

The public also are able to set constraints that will be different from those of the customer, contractor, and suppliers. In some cases they are able to totally stop a project by adding so many constraints that it is not economic or feasible to proceed.

Things to be on the lookout for are:

- Be sure that the basic of rules given here are not broken, as that can lead to late errors that are expensive and embarrassing to fix;
- Ensure good training is provided for all personnel involved in requirements generation;
- Be patient with the customers, as their initial appreciation of the importance of this issue is often insufficient;
- Do not leave the requirements generation task to junior staff to do without adequate supervision; the task needs considerable experience to make wise calls and to author sound requirements statements;
- Make sure that the requirements are allowed as the result of the discovery process, to flex in the early stages of the extraction task.

Having covered the requirements generation process, it is time to discuss how this process impacts the detail design engineer.

Designers will usually be the recipients of the outcome of the requirement elicitation process. They may never need to consult the higher-level statements. At the detailing stage some requirements will then prove to be unworkable, strange, unexpected, untestable, incomplete, over the top, unfathomable, or appear simply incorrect. In such cases, designers should not use personal initiative and second-guess the intention, but take appropriate action to verify the need by inspection of the trace system and by consultation with appropriate people. A project "change notice and approval" process will be in place that provides for such challenges. Equally, if a requirement seems deficient to the design team it should be challenged before detailed design commences.

## 6.3 Specifications

### 6.3.1 Nature and Purpose of the Specification Document

Correctly used, the term specification, when applied in a systems engineering context, is the statement of a technical requirement. This statement describes the thing that is to be made in terms of how it is to done.

Specifications are generated as an output of the requirements generation process wherein that discovery process produces an operational specification then transformed into technical terms.

Many types of specification are used in a project. Table 6.1 gives a summary of the essential types. The examples are all drawn from the U.S. Military Standard (MIL–STD). MIL documents are still a sound source of ideas; they are give more detail on the how as well as the what of their topics, and they are now in the public domain and available free of charge.

This standard has largely been replaced in most projects today by AIE-632 and others, but the standards to use in a project will be dictated in the contract or by the systems engineer. Many standards may be in force in a project; expect inconsistencies and the need to work with several standards simultaneously!

Other kinds of specifications are:

- Documentation;
- Installation;
- Packaging and transport;
- Standard items;
- Modified items;
- Special subcontracts;
- Incoming inspection;
- Use of vendor specifications in projects;
- Service and maintenance;
- Safety;
- Security.

**Table 6.1** Essential Types of Specifications

| *Specification Type* | *Description* | *Example Format* |
|---|---|---|
| Operational requirements specification | A specification describing the requirements of the proposed system in terms of user needs, its relationship to existing systems or procedures, and the way in which it will be used and maintained. | MIL-STD-498<br>DI-IPSC-81430<br>"Operational Concept Description" |
| System/subsystem specification | A specification describing the requirements to be satisfied by the system, and the methods to be used to verify that the requirements have been satisfied.<br>The SSS is used as the basis for design and verification of the system. | MIL-STD-498<br>DI-IPSC-81431<br>"System/Subsystem Specification" |
| Interface requirements specification | A specification describing the requirements associated with a system that defines its interface(s) with other systems.<br>Interface requirements may be defined as part of the SSS, or in a stand-alone IRS. | MIL-STD-498<br>DI-IPSC-81434<br>"Interface Requirements Specification" |
| Subcontract manufacture/quality specification | A specification identifying requirements and standards of workmanship for items of a system supplied by a subcontract agency.<br>Such requirements may be identified in a subcontract statement of work (SOW) as part of a contract, or the SOW/contract may refer to the suggested stand-alone specification. | MIL-STD-498<br>DI-IPSC-81431<br>"System/Subsystem Specification," tailored to identify requirements associated with safety, system quality factors, and design and construction, as well as other SOW-style clauses associated with the manufacture and quality of items. |
| Acceptance test specification (Subcontractor, factory, Field) | A specification identifying the criteria for acceptance of system requirements described in the SSS.<br>The specification may be tailored to address acceptance criteria for requirements verified by a subcontractor, at the facilities of the contractor prior to delivery to the end customer, or in the field (i.e., when the system is delivered to the end customer) | N/A |
| Installation specification | A specification identifying requirements associated with the installation of the system in its target (end-use) environment. | MIL-STD-498<br>DI-IPSC-81431<br>"System/Subsystem Specification," tailored to identify requirements associated with installation of the system in its end-use environment only. |

(*Courtesy:* Tim Welburn.)

Which of these are to be used in a project is usually designated in the systems engineering manual for the project.

## 6.4 ConOps

### 6.4.1 Creating a ConOps Document

With a background in requirements now developed, it is appropriate to look more deeply into how a sound model of the concept can be developed.

It has earlier been suggested that an important activity is the preparation of a ConOps [8]. Figure 6.6 is a simple model to keep in mind. A ConOps is useful in developments as it assists reduce rework and offers good early error trapping.

Regardless of the application, all ConOps statements will be expressed in terms of their physical attributes and circumstances. Some examples of its use could be in:

- Medical imaging systems;
- Space shots;
- Security systems at airports;
- Voting systems for gathering public consensus;
- Ship propulsion systems;
- Supermarket operations.

The valuable features of a ConOps are its:

- Usefulness for motivating thought and acting as a focusing point for issues;
- Clear understanding developed of the relevant parameters at each stage of concept model;
- Maturing model of growth of development from start to use first formed;
- Information provided for developing many key processes, such as schedule of development activities and task responsibilities list;
- Creation of a set of measures for monitoring performance of the development and eventual use;
- Good appreciation of the whole, by all concerned;
- Growth of ownership of areas it assists;
- Reporting assistance of the above issues.

A ConOps describes the relationship between the dominantly involved groups and gets communications going between the various groups. It principally addresses:

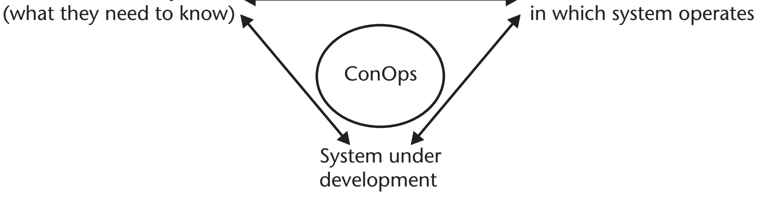


**Figure 6.6** Communications in the development of a ConOps report. (*Courtesy:* Jack Ring.)

- Users for which it is aimed;
- System under development to perform the intended task;
- Real, open system in which the system being developed operates.

It is essential to adopt a user-centric attitude in design thinking. This seems to be an obvious thing to state but it is widely observed that this is often overlooked.

For example, a civilian passenger aircraft audio system refit had the AV controls in the top of the armrest. The control buttons were such that an arm resting on them would change settings of the adjacent person's system. A recessed set of buttons would have avoided that flawed design aspect and would have been simple and fast to correct at the requirements description stage.

At the commencement of the development, it may be helpful to set up the ongoing report system as a set of hyperlinked files for that allows faster and more convenient access to its various parts. It also enables the user to be linked to off-computer material. This format will, however, need to be reformatted into a simple report if hard copy is needed. It may also be appropriate to set up the report on a LAN or Internet server to allow anytime, asynchronous access.

Factors of the ConOps to clearly identify are the:

- Need of the system;
- Operational requirements;
- Maintenance and support.

The development, managed by the systems engineer with assistance of whoever needs to be involved, starts by gaining a thorough understanding of the purposeful tasks that the system must perform, and the circumstances in which it will have to operate.

It is developed as a sequential process of identifying issues as though you are the actual person setting it up, stage by stage. Imagine you are the leader "fighting the battle" with the system you are developing. Working with those who will be involved as stakeholders in its use, tease out key issues concerned with the operational requirements:

- Operational use;
- Operating environment distribution;
- Length of its operation;
- How effective it needs to be, for what parameters.

Do not specify technical solutions in the ConOps activity unless they are already given as a constraint. Evaluate several feasible concepts of solution. Create iconic models as well as textual statements. Pictures can convey ideas that need thousands of words to describe. Set up a thesaurus of defined names and word uses; ensure it is being used. Set up checklists formed from previous experiences. Keep the language simple and unambiguous.

Throughout the development of the ConOps be as quantitative as is reasonable at this early stage. Factors that lend themselves to numeric quantity are:

- Usage environments;
- Usage patterns (duration, number of usages per day/week/year);
- Characteristics of users (size, mass, male/female);
- Equipment maintenance and repair philosophy;
- Equipment size and mass constraints;
- Preconceived concepts, implementations, etc.;
- Customer key performance indicators (KPI);
- Any other design constraints or requirements.

Table 6.2 gives some examples of metrics.

The suggested contents of a ConOps report are now summarized in terms of the sections it should contain.

*Opening pages:* These will be as needed by the organization's practice, including authorizing agency, security classification, distribution, and contact points;

*Section 1:* Purpose of document;

*Section 2:* Scope of document;

*Section 3:* Description of anticipated intended user and their roles, authorities, interfaces, and responsibilities;

*Section 4:* Description of the anticipated real environment (content, structure, behavior, pertinent external and internal attributes, persistence, variability such as glint, scintillation, position, etc.);

*Section 5:* Description of desired relationship between material of Sections 3, 4 above as a basic observation and an interpretation scenario (regardless of realizability) using aspects such as:

- Existence of something (both the internal and external attributes);
- Location of something (including the related factors);
- Persistence of something (including the related factors);
- Variability and contrast exhibited by that something (such as range of values, the repetition rate of pertinent changes, the least count of observations).

*Section 6:* Conceptual description of anticipated system under development;

*Section 7:* Description of desired relationship between the environment and the system under development;

**Table 6.2** Example Metrics for Use in ConOps Developments

| *Attribute* | *Unit Type* | *Low* | *Medium* | *High* |
|---|---|---|---|---|
| Measures | Number | 1 | 2 | Many |
| Precision | % Full Scale | 0.1 | 0.01 | 0.001 |
| Error | Precision | >1.5 "x" | 1.5 "x" | <1.1 "x" |
| Frequency | Cycles/second | 1 | 102 Hz | 104 Hz |
| Trigger | Type | 1 | Periodic | Event |
| Time | Seconds | 1 | 0.1 | 0.01 |
| Latency | Seconds | 10 | 1 | 0.1 |
| Interfaces | Number | 3 | 10 | Many |
| ConOps | Artifact | Optional | Recommended | Mandatory |

(*Courtesy:* Jack Ring)

*Section 8:* Description of desired relationship between the intended user and the system under development;
*Section 9:* Description of model of the system in operation (showing flow of activity as a task is undertaken and where to access any executable models formed in a computer);
*Section 10:* Description of metrics to be used (Table 6.2 gives some examples);
*Section 11:* Summary;
*Appendices* (where needed).

An example of a simple ConOps model is given in Figure 6.7. It shows how it is proposed that systems engineers be better trained [9]. Note how it is potentially more holistic in its approach than education systems of today are because it integrates the needs of the student, educator, and user into one delivery system of trained engineers. The holistic modeling makes it clear why metrics are needed for the performance of all three groups involved. The model given in Figure 6.7 is the first level of explanation.

To this is added the various metrics (as measures of effectiveness, or MOEs) to each of the stages of the serial process—see Section 2.5.2.

## 6.5 Legal Issues in Requirements Development

### 6.5.1 Summary of Legal Issues to be Addressed in Shaping Requirements

Legal issues involved in design are covered in more detail in Chapter 10. At this point, it is only necessary to summarize them to ensure they do not get overlooked in requirements development.

Aspects to certainly address at the requirements extraction stage are:

- Contract conditions (these will partially define scope and method);
- Dispute resolution means (third-party appointed arbitrators, courts, etc.);
- Legal liability (litigation made on the supplier and customer parties involved due to unsafe design leading to personal injury or death);

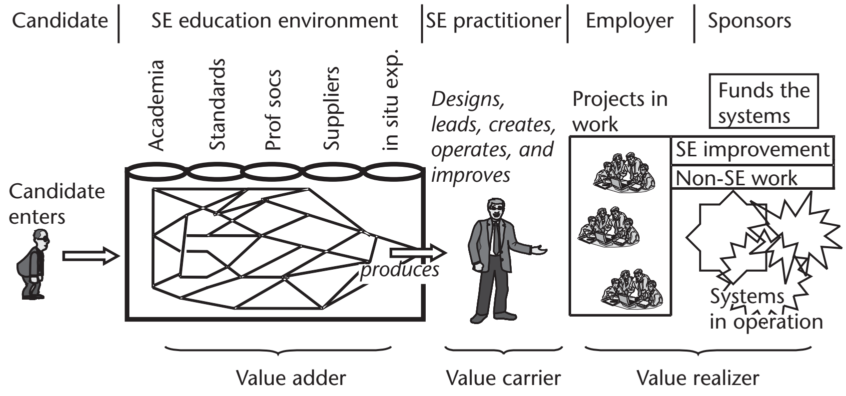


**Figure 6.7** Example of a ConOps system for delivery of trained systems engineers. (*Courtesy:* Jack Ring.)

- Laws and regulations such as health, safety, and ethics requirements (these can arise from local government, national, and international sources plus organization policies and trade associations);
- Standards needed by law (as are appropriate);
- Product recall (failure of the supplied items);
- Usage by various authorized and unauthorized parties (copyright, mailing list generation and use, patents, registered trademarks, and the like);
- Use of the Internet to support the project (laws vary widely on what can be published).

Obviously the situation may well be complicated enough to use the services of a suitably experienced legal person. Large organizations will have their own law staff to look after these issues. In such cases, the design team does not need to be overly concerned with arranging the right services. Teams in the small firm, however, will need to hire in expertise. As is explained in Chapter 10, a product recall or a drawn-out litigation can easily bankrupt an excellent team's firm. The cost of these services is money well spent for they assist in avoiding late errors, thus reducing risk.

As evidence of lax attention to the legal side of product design, it is the experience of a large international product test house that their client's systems fail acceptance far too often on health and safety and other legal grounds, not the technical operational aspect. If legal issues are not addressed at the requirements stage the first time, it will be may well be in final testing, or worse, in its application after delivery.

## 6.6 Summary

This chapter has developed the background and principles for getting started with a system development, namely the task of extracting the requirements.

It began by discussing the environment in which several groups interact to satisfy their various needs.

Material presented then dealt with the nature and scope of requirements and how to develop them.

The characteristics and issues involved in extracting a good requirement were given, showing that it needs rigorous investigation, learning, guidance, and patience. Web site reviews are available [10, 11].

Requirements are actually constraints that gradually limit design options; the implications of this have been examined.

Extraction of requirements needs a framework for their development. The nature, scope, and application of the operational concept (ConOp) methodology have been explained as being a suitable mechanism for focusing work of this task.

The way in which requirements flow down into technical specifications has been explained, as has the need to give early consideration of the legal issues that are usually involved the requirements extraction task.

The process of requirements starts the need to make many important decisions, skills needed all through the system life cycle. The next chapter deals with that important designer capability.

## References

[1] Tyler, P., *Running Critical: The Silent War, Rickover, and General Dynamics,* Harper Collins, 1986.

[2] Institute of Electrical and Electronic Engineers, *Guide for Developing Systems Requirement Specifications*, (IEEE P12330), New York; IEEE Standards Department, 1993, and later, Institute of Electrical and Electronic Engineers, *Guidance for the Development of the Set of Requirements*, IEEE Std 1233, 1998 Ed. (R2002) (Includes IEEE Std 1233-1996 and 1233a-1998), IEEE Standards Department, New York, 1998.

[3] Sage, A. G., and W. B. Rouse, (eds.), *Handbook of Systems Engineering and Management*, New York: Wiley, 1999.

[4] www.incose.org/rwg, INCOSE, 2002. International Council on Systems Engineering, SE Management Technical Committee, Requirements Working Group.

[5] Bray, I., *An Introduction to Requirements Engineering*, Upper Saddle River, NJ: Addison-Wesley Publishing, 2002.

[6] Hull, E., K. Jackson, and J. Dick, *Requirements Engineering*, Heidelberg: Springer Verlag, 2002.

[7] Grady, J. O., *System Engineering Planning and Enterprise Identity*, Boca Raton, FL: CRC Press, 1995.

[8] Ring, J., private communication, 2002.

[9] Ring, J., *Development of Educational Methodology*, Work in progress for Education and Research Technical Committee of INCOSE, www.incose.com, 2000.

[10] http://easyweb.easynet.co.uk/~iany/reviews/reviews.htm, reviews of books on requirements engineering, Nov. 2002.

[11] www.niwotridge.com/Books/REBooks.htm, reviews of books on requirements engineering, Nov. 2002.

## CHAPTER 7

# Establishing and Selecting Design Choices

During all stages of design activity, decisions must be made between competing ideas. An important part of making design decisions is the gathering of sound information. This then needs to be applied using methods for assisting in decision-making. This chapter deals with the following aspects of decision making:

- How the necessary information is gleaned;
- Sources of information;
- Generation and ordering of the parameters associated with issues, including the brain storming, slip writing, and TOP methods;
- Consensus building and the Adelphi technique;
- Setting up project checklists;
- General principles of all decision-making;
- Choice-assistance methods, namely utility analysis and decision trees;
- Strengths and weaknesses of the various methods;
- Setting up to make a decision.

## 7.1 Gathering Information in Support of a Design

### 7.1.1 Establishing an Information Support Base

Design often involves making a choice between alternative solutions ranging from high-level needs, such as in the concept stage, right through to simpler situations, such as selecting the paint color for a carry case. Examples will arise when working on such aspects as:

- Architectures;
- Technologies;
- Configurations;
- Components;
- Circuitry types;
- Power supplies;
- Packaging;
- Staffing.

Design is much about reducing the risk of not achieving what the customer needs. The choices that have to be tackled throughout a development involve making numerous decisions when the issues are often unclear or in conflict.

Where simple logic leads to clear ways forward then decision-making is straightforward.

In many situations, however, the variables will be problematic. Techniques are needed for handling the parameters in as logical and objective a manner as is reasonable.

When seeking to solve problems, the process needed is:

- First sort out the real need succinctly, with as few parameters as possible;
- Express it in writing;
- Obtain appropriate quality information;
- Set up a decision-making assistance method;
- Interpret results and make selection.

The task of locating relevant and sound information is now addressed in this section.

In the seventeenth century, Descartes suggested four rules for "properly conducting one's reason." They are sound rules to observe when selecting information:

- Avoid precipitancy and prejudice;
- Accept only clear and distinct ideas;
- Conduct orderly progression from the simple to the complex;
- Complete analysis with nothing omitted.

With so much available today this can easily lead to information overload. There is a need to decide which approach to use for each given decision-making situation. Alternatives to use include:

- Relying on one's memory and records, or of others where it is easily accessible;
- Mine down into the existing knowledge;
- Build new knowledge as a fresh investigation.

Deciding which to use requires understanding of these alternatives.

We consider here the experiences of self and others, libraries and the Internet. Each has its merits; none is necessarily sufficient alone.

### 7.1.2 Past Experiences

Expert designers have considerable experience. They are able to recall quite unexpected things at the right time and know how to reapply ideas that their wisdom encapsulates. How this professional intuition works is not well understood.

People think in two different ways when mentally processing new situations.

Some find it easier to consider a specific need by approaching it from a general representation of the principles involved [1]. An example is the use of an equation that models a range of situations.

Others find they approach problems better by starting with specific examples of like situations out of which they can sense the generality and adapt that to their situation.

Both ways of thinking need to be allowed for.

Extracting knowledge from experts is called knowledge elicitation. Its methods include:

- Experts writing down the pertinent knowledge in free-style expression;
- Experts filling in proformas;
- Interviews conducted with experts by knowledge elicitation staff;
- Making oral recordings on the topic with some prompting, but generally with their own ideas of what is recorded and how.

These work with varying success. Unfortunately, considerable wisdom is often lost about a topic because it can be too costly to undertake the elicitation work.

The use of previously executed designs can assist direct and indirect solutions by application of what is called analogous design.

For example, it was demonstrated that two magnetic armatures, one spinning at high speed and the other being at an input near to being stationary, would generate a phase-varying output signal proportional to the angular rotation of the near-stationary armature. This was used to measure fine increments of static rotation with great success. The same principle was then applied using the so-called *dual* of electric fields, that being a capacitive implementation. This latter method was cheaper to make, smaller, and could provide more accurate measurements.

Analogous connection between inductive and capacitance methods would have been reasonably obvious to electrical engineering experts for the two regimes can be modeled with similar equations.

Not so obvious is that the same principle is also applicable to spinning optical encoder gratings, there the link being its ability to also provide a phase-shifting signal. That implementation had superior design features to the capacitance method. Perhaps there is still another analogous way to implement the same basic idea?

There are many ways of stimulating ideas from people. The well-used process of group brainstorming will often keep triggering the minds of participants to come up with surprising innovations as their interaction proceeds.

It has been said that any maker of a new gizmo product will sell at least as many items as it has competitors for they will each want to see how it works and is made. A good source of ideas could well be a like product in its final form or patent description. Reverse engineering is a well-developed practice. There are ethical issues in this approach but as long as one works within legally allowed practices they will be acceptable, especially if used in a different situation.

Whereas the mind can come up with amazing ideas at times, it is, however, not always reliable in recalling detail. What is remembered needs checking because the memory can do strange things. An idea will be sometimes recalled in a different sense than its original context. It might actually be better than it was used before—but it might not!

Often the recorded truth about an item is distorted, or not understood correctly. For example, reports in learned journals on instrumentation can be rosy descriptions. Those who try to build the item from the report are often unable to get it perform as described.

Poor records do not support later reestablishment of ideas. Reports should be written for an unfamiliar party to use who has not had the experience; that being also you at a later date! The original description might also have been for operation in a different working environment.

If your idea is not along conventional and accepted lines it may suffer lack of acceptance, even hostility. Too often one hears statements such as, "Your ideas seem sound and logical, but if other major organizations have not managed to solve the problems that way with their million dollar programs, why should this one succeed?"

When being innovative outside of the proverbial box it is necessary to be courageous and stand one's ground with sound evidence ready to support the decision.

### 7.1.3 Library Processes and Support

Libraries were once the only main repository for recorded knowledge. Today the Internet is changing that situation. Library stocks, or course, still have an important place.

Around the 1960s, electronic paper abstract services were established for use over satellite links. At that time these were a great advance in locating the existence of journal articles but these services did not provide for book and trade materials. Electronic abstracting of journal articles also began then. Material published before electronic abstracting began is virtually impossible to find. Unfortunately, there is a prevailing attitude that old material is inferior to that of recent times. Much of today's stock of basic knowledge was set up from times before 1960! Locating and getting access to the older material can be costly and take months.

Another fact, not well known, is that U.S. abstracting services mainly decide what gets into the electronic databases and their policies can give greater weight to inclusion of U.S. published materials than from elsewhere.

To a large extent the Internet delivery service, with its global coverage, has widened selection potential. As will be discussed later it is gradually making all written knowledge available.

Electronic searching of library stocks has several limitations:

- May not be able to provide e-file materials until comparatively recent times;
- A vast quantity of older material exists that is not yet, and never will be, entered into databases;
- Users need some training for effective searching;
- Material may not be published where it is expected to be found;
- Material may not be published at all;
- Sophisticated library e-catalogs are more user-friendly today;
- Catalogs are usually on-line for major libraries.

Librarians are highly skilled at the task of finding material and can make a fine contribution to a search. It is often worth the time to visit the library personally instead of using only on-screen communication.

### 7.1.4 Internet Sources

The Internet has supplanted some library services and should be seen as another knowledge access service, not the sole one to use.

Its information storage features are:

- Relatively easy to mine into, but often will come up with considerable irrelevant material;
- Good graphics retrieval;
- Up-to-date information (compared with library stock that has a fixed time stamp ranging from weeks for journals, to years for books);
- Electronic format makes it easy to capture and use.

Electronic searching using the various search engine services has provided great benefits in accessing material. Three issues that need attention in searching for material are:

1. Considerable variability exists in the quality and veracity of knowledge available this way. Some of it is rubbish and easily seen through. The more worrying problem is knowledge that seems plausible but is not correctly interpreted, or is just a little inaccurate in ways that cannot be detected easily.
2. Incompleteness of searching. It is impossible to get total recovery of what might be there to find. Some material will never be published on the Internet.
3. Inability to interpret what is found will occur if the user does not possess the right level and background to appreciate the material.

### 7.1.5 Veracity of Knowledge

When information is found, how can we be sure it is sound? When the bulk of it was published by reputable publishers some level of guarantee existed that it was truthful, complete, in context, and thus reliable to use. Today, however, anyone can publish material on the Internet so the veracity safeguards are much reduced. Knowledge is often available without indication as to where it came from.

Users of all information on the Internet need to be discerning and know how to make judgments of its quality. Here are the principal methods by which knowledge can be verified as truthful. None is foolproof. Each method given below needs an understanding of how its process operates and of the quality of the people involved:

- *Single, first person, source.* This is the least certain method and arises where the person providing the knowledge is asserting things by provision of a personal argument. How well the argument is constructed as a logical process, coupled with the soundness of the "facts" involved, can give pointers to the veracity of the statement. This type of information must necessarily be treated with suspicion.
- *Reviewed by one or more other experts.* External reviewing is often used to verify new knowledge. Primary journal papers are reviewed by two or three people. This makes it a little more certain that the knowledge is sound but the

selection of reviewers, terms of operation, personalities, and the final analysis of their reports often leaves matters open to question. It is possible for the many to be wrong!

- *Reviewed by a group of people to gain consensus.* At times reviewers are set up to create a consensus-forming group. More people involved and a better process can lead to an opinion about some knowledge that is more widespread. However, selective use of reviewers can be used to bias the so-called consensus result.
- *Mathematical model.* Where possible, a sound mathematically described model can be generated that models the behavior of the situation. This can be tested and evaluated using formal methods, meaning all who use it will get the same results if they use the same inputs. The difficulty is that much of knowledge does not succumb to this reductionist method. Where it does, it affords powerful means for being verified. Again it is possible to set up bias by appropriate choice of the mathematics and coefficients used.
- *Real world tryout.* "The proof of the pudding is in the eating" sums this option up. Having some knowledge applied to its actual use is as good a test as can be obtained. However, it still may not represent the circumstances that might apply in the next interval of time after the test. It also may not testable even though it has been built.

Overall, using knowledge is always problematic and often an uncertain activity. New applications using past reliable knowledge need care to establish if it then fits.

### 7.1.6 Publishing House Trends in On-Line Delivery

The way that knowledge is being made available is changing fast now that we are in the Internet age.

Initially, starting in the 1960s, abstracts of journal papers were provided in e-file format, allowing computer-based searching over satellite links. The service was later extended to include book titles with a few keywords. This did not allow access to the full material for all entries, only parts to see which was likely to be relevant.

During the last decade, publishers have ramped up on-line provision of the full text of journals on the basis of single journal subscriptions being made to have access to publisher's Web sites. This is not that useful for subscription by individuals who will need to access many journals. This method is mainly provided at an institutional level.

CROSSREF is a central cooperative journal on-line service currently being built up. Some 150 publishers of thousands of journals are providing single point access for finding and paying for the knowledge provided. Expect to see a move to a "pay as you go" structure for future use of knowledge services. This will also allow implementation of the all-important general access to all services instead of having to subscribe to all journals and books on an individual basis.

Recent trends are to provide, on-line, the content of texts and major reference works.

Organizations and businesses offer information in support of their products via their own Web sites. As well as providing the expected catalog and ordering facilities, they sometimes provide information on the basics of their field.

At present, publisher-provided material is usually only retrievable as direct copies of full articles. Once the format of the knowledge is in e-file form a host of advantages appear compared with delivery in the hard copy format. These include:

- Increasingly better searching, with smaller granularity and more precision in the desired topic's content;
- Illustrations, images, sounds, and videos can be provided in full color;
- It is easy to manipulate the knowledge using select, copy, and paste methods.

The above features facilitate provision of commonly needed specialist tools to assist in using the knowledge for such needs as:

- Compile a lecture or a report using the reference base knowledge;
- Create specifications using given standard formats, providing powerful tutorial assistance when setting in the various specifications;
- Rapid linking to external knowledge sources via Web links;
- Automatic compilation of lists of terms and citations from a publisher's specialist knowledge base, formed from the book material.

With the e-form of offering information, it becomes increasingly easier to locate precise information that can be efficiently used in design work.

## 7.2 Parameter and Ideas Generation

### 7.2.1 Slip Writing

As well as needing information about topics, decision-making also needs the key parameters of a situation to be separated out. An essential skill in decision-making is to be able to externalize and prioritize the issues. This section covers how to do that. Techniques explored are:

- Slip writing, a rapid parameter extraction method;
- Knowledge trees, which offer a way to order knowledge and motivate thinking.

The following section deals with:

- Brainstorming, which encourages innovative group thinking;
- Delphi technique, which maintains independence for extracting expert reviews.

Slip writing is used to gather key features on a topic from a group or by an individual. The methodology is simple. First, a problem is expressed as a simple sentence, for example, "What are the parameters that we regard as the most important in assessing the effectiveness of a soldier's footwear?" A clerk assembles a suitable group, giving each person a pad of paper and a pen. The problem statement is put up for all to see. The group is told, "Having seen the task, you now have 2 minutes to write down the issues that come to mind, one issue per sheet." When the time has expired, the slips are collected by the clerk who sorts them into similar sets of issues. This has identified likely issues and assigned to them a crude priority. The importance of a parameter is indicated by the number of appearances in the collection. No comment is recorded on the entry of individual slips.

Features of this method are that there is no influence on the thinking of each person by other members of the group and that short-term recall is not impeded by the need to structure the slip statements.

This process extracts a rapid idea of the issues but is not a considered response, which can be both a strength and a weakness. Maintaining confidentiality is essential in some circumstances, such as in a study by the design team on how to improve their operations.

This method comes in many guises and forms of expansions. One variant takes the topics generated on the slips, one per card, and asks the team to place them into classes and priorities by sorting the cards on a tabletop. Participants each keep changing positions of the cards until it seems little change is taking place. This additional stage allows each person to appreciate the standpoint of others and make corrections to the thinking about the problem under investigation.

A further extension is to combine slip writing with the use of knowledge trees, covered in Section 5.6. This structural approach is useful in that it:

- Orders the issues to show linkages;
- Motivates selective thinking on specific issues that can too easily become clouded when the whole task is attempted as a whole;
- Records the thinking that is in place for later users of the information;
- Allows each element to be addressed in turn to provide detailed descriptions and justifications;
- Immediately shows another user the information that has been so gleaned.

It is surprising how much can be externalized from the mind through by the use of tree diagrams.

For example, initial preparation for building an electronic system automatic design tool needed to identify the key factors involved in such designs. It took around an hour to set up some 30 trees with 4 to 5 layers each. Trees are powerful aids to extracting knowledge that is buried deep down in the mind.

### 7.2.2 Brainstorming

Extending the above ideas leads to discussion of ways by which participants generate likely solutions to design problems. Brainstorming is an appropriate method to use in such situations, for in this method the ideas of each person can spur on innovation toward an ever-improving solution by the group.

An example of this was a study on detecting casting sand remaining in an aluminum casting after molding.

It began when an experienced brainstorming organizer created a statement of the need that was expressed in customer terms. This report was three pages in length. Related materials and artifacts were collected, namely here some sectioned castings showing sample sand inclusions and ready-to-use sand casting forms.

An appropriate team of experts was identified that brought to the group experience in industrial chemistry, electrical and electronic engineering, and mechanical engineering. A company process expert was included; he also represented the company.

Each person was sent the needs statement, provided with access to the samples, and given 2 weeks to ponder on the task before the 2-hour brainstorming meeting was held.

At the appointed time the team assembled. Sheets of white butcher paper was put up on the walls. The group then reacted informally with ideas on how sand detection might be done.

As ideas were realized they were recorded on the paper for all to see. Many ideas were exposed as the team reacted together to rule an idea out or add more support for one. The pros and cons of the ideas were also recorded as notes on the paper.

Gradually, several feasible candidate ideas emerged, some involving combinations of ideas. When it seemed little more was to be gained the meeting ended.

It might be thought that using paper is somewhat antiquated when white boards and laptop computers could be used instead. Paper has the distinct advantage of allowing the participants to easily see the ideas at all times. They can also be bundled up to take away with the haste that is usually associated with busy schedules and tight meeting room bookings.

After the meeting, the leader prepared a report of the ideas using a numbered tree, seen in Figure 7.1, accompanied by short descriptive statements of the pros and cons of each case. The report ended with a summary of the recommended candidate solutions given in priority order.

While this method facilitates stimulating open thought, it can become overly dominated by a strong member.

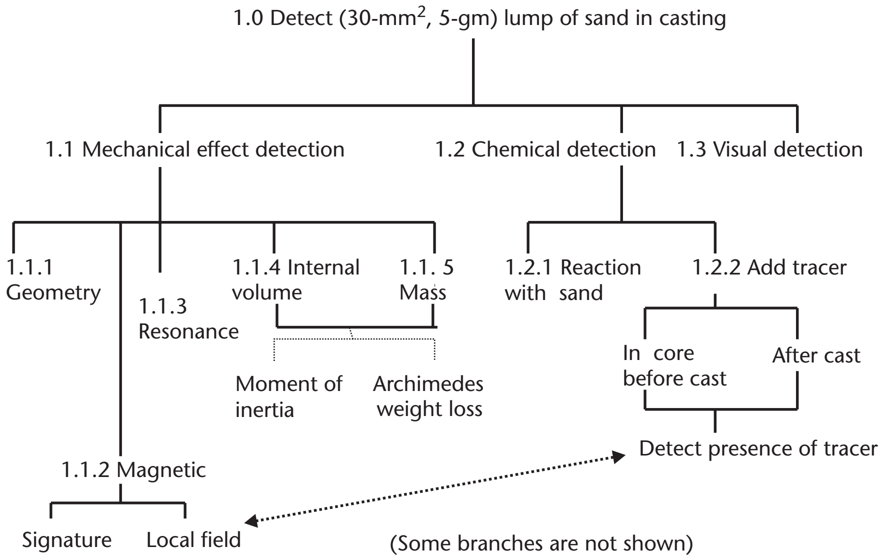


**Figure 7.1** Tree basis for brainstorming session investigating detection of retained sand in castings.

Variants on this process exist. Consultants are available who specialize in setting up such events. Think-tank and blackboarding sessions achieve similar objectives to brainstorming.

## 7.3 Prediction Methods

### 7.3.1 Delphi Studies

Experience expressed by a single individual can be biased and limited in scope. There is often need to build a wider consensus of available knowledge by integrating the views of many people. Several ways to get this consensus are through a:

- Collation of published statements by various authors, where they are available;
- Survey of the opinion of suitably selected people who represent a full spectrum of ideas;
- Use of multiple facet representation at group meetings, as in the IPT method;
- Use of the Delphi technique.

The Delphi technique is now outlined to illustrate the features of consensus-building methods. This technique is used when experts need to consider the problem without being influenced by the views being expressed by other members of the wisdom group.

It starts with the problem being written up in concise terms. Examples are, "How will cell phone technology develop over the next decade?" and "What is the best approach to the introduction of automation into a manual factory process?"

Experts are selected and invited to participate without knowing who else is invited. It is essential that no interaction on the topic takes place between them.

They are asked by the organizing person to consider their opinion over a sufficiently long time period to allow them to use their own resources to develop their answer. They each submit a major report.

The organizer integrates the reports, preparing a summary document giving the general issues and common findings.

This consolidated report might then be returned to the experts for a second, or more, round of consideration. Confidentiality is still maintained.

With the Delphi method, experts have time to gestate their ideas and little influence is exerted on each person's thinking by others in the group. However, remember that experts in a similar field, at any point in time, often tend to follow the same fashionable ideas so systematic bias can exist in these studies.

## 7.4 Checklists

### 7.4.1 Development of Checklists and Their Use

Often the issues associated with making decisions are regarded as being well known and lying within that perceptive entity called common-sense.

It will, however, usually be found that common-sense knowledge is different from person to person and that their collective set is larger than for any one of them.

For this situation, the use of checklists is appropriate. These record the factors as they are realized. A checklist helps to ensure all of the relevant factors are addressed, if only to rule some of them out. Without checklists it is all too easy to overlook parameters that should be addressed. Rethinking issues for each new situation can be counterproductive.

The contents of checklists usually develop naturally where a generic task is continually repeated. Each time it is used more factors can be added when new items appear to be needed. Table 7.1 is an example of a checklist generated for testing a measuring instrument.

The mature organization will have many of these in place, design review agendas being commonplace examples (see Section 8.6). They also can be used for later projects for they are formed of factors common to all projects.

## 7.5 Decision-Making in Design

### 7.5.1 Nature of Decision-Making

Having found information and set it up in charts and lists, the next step is to use it to make decisions. This section now looks into the basics of decision-making.

Design often involves deciding which alternative item, design principle, or combination of parts and the like is best to use. Engineering is about maximizing the use of scarce resources so there will often be a need to choose which option to adopt from a set of alternative, somewhat qualitative, variables. Making subjective choice situations more objective is a feature of organized decision-making.

Often there arises a need to compare different scenarios in order to decide which combination of variables and data offer the best overall value. Examples might be:

- Which tool set should be used?
- Which machine should be acquired?
- What is the best defense strategy for the near future?
- What is the most cost-effective method for designing an item?

Whereas the aim can also be to optimize a situation, it will rarely be possible to optimize all parameters at once, for they are usually in competition. Increasing the power of an electronic amplifier invariably means a heavier assembly. This may be fine in the domestic audio system setting where weight does not overly matter. In sharp contrast, increasing the weight of a high-power RF amplifier in an electronic warfare system for an airplane will be a severe penalty.

Decision-making is a very large topic. Much has been written about it [2–11]. Its texts are found in three main library areas:

1. Business management;
2. Computer science;
3. Math theory.

**Table 7.1** Checklist for Assessing a Measuring Instrument

*Issues to Be Considered When Reviewing an Instrument Design*

☐ Does the instrument excessively load the observed situation?
☐ Is it compatible for interconnection?
☐ What extra interfacing needed?
☐ What is the detection sensitivity?
☐ Is it adequate?
☐ Is amplification needed in its actual use?
☐ Is it able to respond fast enough to changes in observed variables?
☐ How well will it work in the presence of the various influence variables existing in its working environment?
☐ What is the real cost of developing and using the instrument when all additional charges are added?
☐ How is it calibrated?
☐ Where it is done and how long does it take to do it?
☐ What calibration interval is appropriate? How will it be calibrated?
☐ What is the essence of the transduction principle used?
☐ Is it well made?
☐ Has its declared performance been verified elsewhere, and how?
☐ Is the documentation adequate for its lifelong needs?
☐ What power supplies are needed?
☐ What are the maintenance requirements?
☐ What is the spare parts situation?
☐ Is any special support equipment needed?
☐ How well known and reputable are the makers?
☐ Is the technology old, current, or new?
☐ What is the delivery time?

(*Courtesy:* Tim Welburn.)

The management material gives descriptive ideas but does not support application if one needs to be quantitative. In engineering design, the time available to make most decisions is relatively short. Most works, however, assume that the reader is familiar with the deep mathematics used and has lots of time to devote to learning and applying the methods. Unlike a war department deciding on the best strike to make or a large corporation seeking to improve its profit, the engineering designer has to move on rapidly. Even though engineering is concerned with decision-making, detail engineering courses rarely include the topic. It is often found in systems engineering offerings.

Here is given a short overview of the main principles involved, showing how they are applied in some examples. The methods given here are easily used during the course of a design, being applicable in minutes to hours for their preparation and execution. They can be carried out with little training or prior experience.

When the parameters involved are obscure, uncertain, or subjective then a decision needs to be made in a state of uncertainty. The case then involves:

- Risk reduction and risk taking;
- Seeking to balance these two by use of externalized methods;

- Using decision-making methods whereby it is not left entirely to human intuition to make the choice from the heart, but rather uses methodical thinking, justification, and recording;
- Situations involving conflicting multivariables are more normal than with just one variable.

Some generic features exist for all decision-making situations. These are:

- Decisions need to be made under conditions of constraint (e.g., limited money, fuel load, time, life, support cost).
- A decision is a choice from alternatives in competition with each other. Subsequently, every decision must have some form of criterion for judging the alternative choices;
- A common, and sufficient, set of parameters for the situation must be found for all candidates in a review;
- The end result of methods usually leads to a matrix of numbers that can be calculated to yield graded preferences for acceptance—the trade-off matrix.

It will be seen how these arise in the methods given below.

Decisions will be made in one of several situations of uncertainty. They depend on the kind of uncertainty that prevails and the persons involved in making them.

### Decisions Made Under Conditions of Assumed Certainty

Given full information, as when the system behavior adheres to well-defined scientific laws, decision-making is easy because all of the facts are crisp and indisputable. In such cases, the final choice can be made using rigorously applied logical deduction. Logic trees and Boolean algebra truth tables are basic tools here. This sort of decision-making is found implemented as:

- Heuristic rule sets, which are basically logic binary trees using subjective, rule of thumb, statements.
- Expert systems decision support tools, which are formally implemented logic trees of rules being searched in a binary manner. These can have degrees of uncertainty built in to the rules to make them more realistic.
- Fuzzy rules in expert systems, which extend fuzzy systems concepts to cater to unclear situations by the assignment of a law (the membership function) to each variable to allow formal calculation.

Fuzzy logic (FL) systems are well-developed theoretical and hardware systems for carrying out logic-based decision-making.

Under assumed certainty, the risk of making an incorrect choice is virtually zero as hard facts are being used. It, however, does not acknowledge an ignorance factor that often exists when it is assumed that everything obeys known laws—for it often does not.

The assumed certainty situation is usually not realistic enough for conducting major trades studies about real systems. Other assumptions need to be used to obtain more realism in decision-making.

### Decisions Made Under Conditions of Risk

When decisions need to be made in situations that are not at all well understood, the key issue is what degree of pessimism or optimism is to be adopted for the uncertain parameters. There are no specific recommendations for this because it depends on personal acceptance of risk.

The desirable way to best proceed would be to carry out much more investigation so that the level of uncertainty is reduced to be negligible. That, however, takes time and money to do, or may not be possible. It is also often necessary to make the best judgment possible in a relatively short time.

Where they can be applied, a more realistic situation is to assign probability factors to the uncertain parameters to make allowance for the ignorance about their behavior. This is commonly used for such inputs as experimental evidence, expert opinion, and subjective judgments.

### Decisions Made Under Conditions of Uncertainty

There will be uncertain situations when one cannot reasonably assign probabilities to the parameters being compared. The approach then is to assign uncertainty as lying at some point on the scale ranging between the extremes of pessimism and optimism. Lack of a sound basis of substantial evidence makes this method hard to accept by some people. Although the methods are indeed problematic in use, they can be better than nothing in some circumstances.

Laplace's principle of insufficient reason applies here in that each scenario is seen to be as likely as the other. Probability of occurrence of an event is then $1/n$, where $n$ is the number of events involved. On this basis, a major mathematical system can be generated for modeling the situation existing in large investigations.

Techniques that can be applied for this decision-making situation can use different criteria to suit the conservatism needed. The most used are:

- Maximin/maximax criteria, which uses extreme states of pessimism and optimism for assignments;
- Hurwicz criteria, which uses a state somewhere between total pessimism and optimism.

Turning now to another issue that usually occurs: How do we include the financial factor in choice making?

It is usually best to not include monetary cost as one of the parameters within the decision-making technique itself but to apply it after grading the candidates. Figure 7.2 is an example plot that allows comparison of different solutions. Here cost is plotted against effectiveness, that being a popular comparison but only one of several cost types that are used.

Four different solutions are plotted in Figure 7.2. Solution 1 is a low-effectiveness, low-cost solution. It might well have a high effectiveness/cost ratio but it fails to reach an acceptable minimum threshold of effectiveness. Solution 2 meets the criteria and is less than the maximum budgeted cost so that is a sound choice. Solution 3 is a solution that gives more effectiveness than is required but it exceeds the allowable cost.

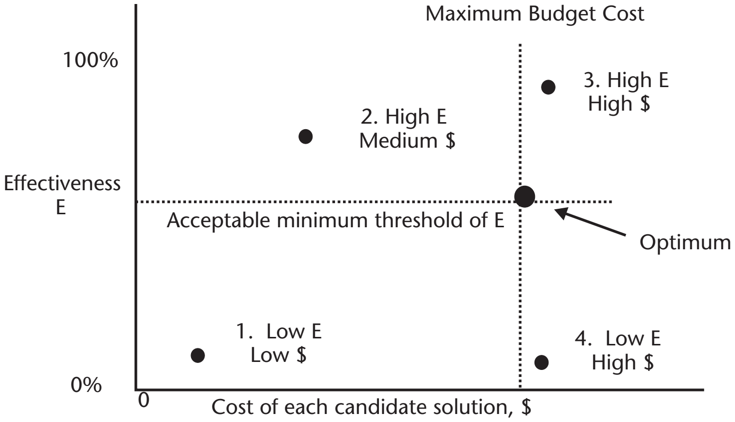


**Figure 7.2** Comparing the financial cost factor in candidate solutions.

Looking at Solution 4, it seems someone has made a major error in design because it offers little effectiveness for a high cost. Surprisingly, many systems are offered with this kind of relationship, and they get acceptance for lack of understanding of the alternatives by those making the selection.

Where the cost and effectiveness lines intersect is the point where both parameters are satisfied with least penalty, therefore giving the customer the required performance and expected system price.

The plot given in Figure 7.2 allows only one variable to be displayed for effectiveness. Many situations need several factors to be judged as a set. For example, a submarine design is judged by its depth, speed, silence level, combat running speed, and fighting capability. All of these cannot be optimized together, so when several designs are submitted they will exhibit different performance levels for each parameter.

In general, these arise when more than one criterion coexists, such as when nonfinancial and financial elements are present.

An approach for judging the best in such cases is to set up as many separate plots as there are variables, each with their own thresholds. Overlaying them all on the same plane enables visual comparison, called an eyeball analysis.

Figure 7.3 shows a generalized multiple parameter situation for three candidate solutions. Obviously many more candidates can be added, the limit being the number that the user can visually manage. Computer-based tools are available for this task.

## 7.6 Selected Decision Support Methods

### 7.6.1 Triangle of Pairs

Investigation in preparation for making a decision will reveal many issues and parameters that could be considered, usually far too many to fully explore. Methods are needed for ranking their importance; that is, for assigning a weight to each.

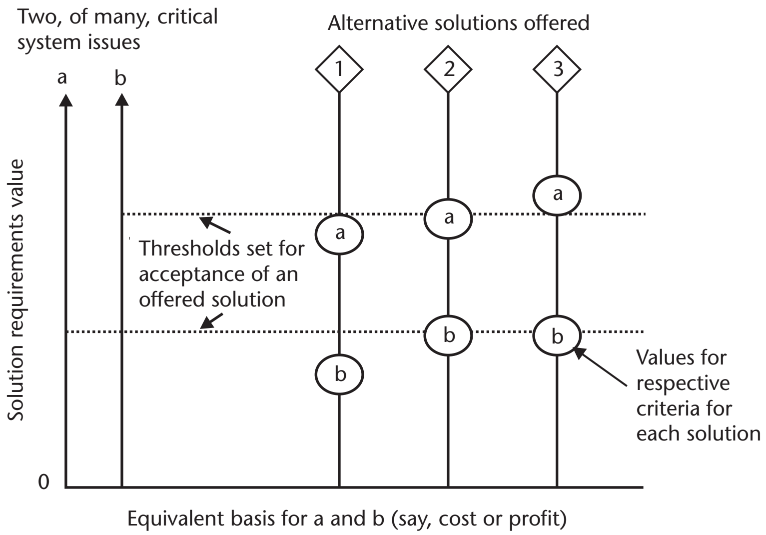


**Figure 7.3** Generalized multiparameter display of candidate solutions.

One method of preference ordering is the triangle of pairs (TOP) method.

The first step here is to decide key parameters using such methods as slip writing. Each parameter is then compared against all the others, asking, “Which one of the two do you prefer?” or “Which of the two is the most important?”

When each parameter is compared with all of the set, the result is the TOP shown in Figure 7.4.

The number of times a parameter has been preferred indicates its preference importance.

The above description uses the simple binary yes or no selection. The same principle can be extended to allow for more finely graded choices by scaling the preference on a 1 to 10 scale, or by the use of a weight factor in the range 0 to 1.0.

| Size | Crustiness | Appearance | Softness | Parameters |
|---|---|---|---|---|
| # *Si*<br>*W* | *C*<br># *W* | *A*<br># *W* | # *So*<br>*W* | Weight |
| | # *C*<br>*Si* | *A*<br># *Si* | # *So*<br>*Si* | Size |
| | | # *A*<br>*C* | *So*<br># *C* | Crustiness |
| | | | # *So*<br>*A* | Appearance |

\# = Preferred choice of the two

Scores (number of times preferred)

| *Si* | *C* | *A* | *So* | *W* |
|---|---|---|---|---|
| 2 | 2 | 1 | 3 | 2 |

**Figure 7.4** TOP ranking of measurands for selecting bread in an automatic inspection system.

### 7.6.2 Utility Analysis

With the various principles and techniques that underpin the decision-making methods explained, it is possible to discuss two methods that incorporate that material for selecting best choice in a multiparameter situation.

Utility analysis is used to find which candidate solution is the best when the candidate designs have the same describing parameters with different characteristics.

The first step is to decide the parameters and order of importance (weighting) for the needed solution. For example, when selecting which loaves on a bread baking line are acceptable, the measurement system would need to include comparison parameters such as weight, size, and so forth.

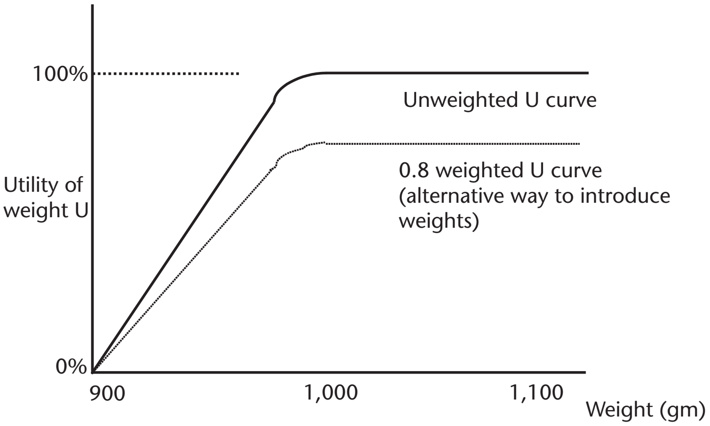
A utility (usefulness) profile for each of the parameters is drawn to show how the utility changes with variation in size of the parameter. Figure 7.5(a) is an example utility curve showing how utility varies with weight change for a nominal 1-kg loaf of bread. When a loaf reaches and exceeds 1 kg, it is acceptable as far as weight is concerned. If a loaf is less than that value, its usefulness falls away according to the slope of the curve because it has value proportionate to its weight. A curve is prepared for each parameter being used in a study. Just how a utility curve varies is decided by an expert who understands the application and context.

Creation of these utility curves is usually straightforward. They need only to be an estimate of how it changes, so precision in curve generation is not necessary in simple situations. Interestingly, it is found that different people will produce much the same curves for a given parameter.

At some stage the weighting of each parameter, perhaps established by use of the TOP method, needs to be added into the calculation. This can be incorporated into the utility curve by drawing the plots with the reduced scale as is done in Figure 7.5(a). Alternatively, it can be added into the calculation matrix.

Note that up to this stage, the various candidates' information has not been involved; up to this point the utility curves have been the focus.

Attention is next given to carrying out the comparison between candidates. After constructing a decision matrix table that lists all parameters, each candidate—here



(a)

**Figure 7.5(a)** Typical utility curve showing the usefulness of a loaf of bread as its weight increases.

the loaves that pass the measurement station—is visited and its individual values read as the utility value taken from the master curve for that parameter. Figure 7.5(b) is a partial decision matrix for three of the parameters. In this case, the weightings have been applied to the plots.

Each row of the table is then summed to give a total score for each loaf. In this simple and limited example, the acceptance requirement is that a loaf for sale has to have a value exceeding a preset value of 1.8.

The utility analysis method can be carried out with as few as four or five parameters; major applications can use hundreds. Once total scores are available they can be used to rank candidates. The reasons why one candidate is better than another are found from inspecting the individual parameter values. In this way, it is possible to tune a design to increase the score.

### 7.6.3 Decision Trees

A design solution will often involve the selection from candidates formed, each having a different set of combinations of parameter choice and value of parameter, there then being numerous candidates.

When the need is to decide the best combination of parameters and values to use, the decision tree analysis method is appropriate. Compare this with the utility analysis method that decides the best to use from several given systems having the same parameters.

The methodology of decision tree analysis is now summarized, and an example is then given to show how it is used.

As with all methods, the key design parameters of the problem are first identified. As will become evident in the example, these should not be overselected—around four to five are usually sufficient in the smaller design situation.

Next, decide how the parameters will be set up to indicate the different values. Only three to four steps over a range are needed; such as low, medium, and high; or material types 1, 2, or 3. These are reference symbols, not data values.

| Parameter<br>Object under assessment | Weight (gm) | Size m$^3$ $10^{-3}$ | Appearance (grade) | Score (sum of rows) |
|---|---|---|---|---|
| Loaf 1 | (970)<br>0.4 | (4)<br>0.2 | (poor/good)<br>0.4 | 1.0 |
| Loaf 2 | (1,000)<br>0.8 | (3.5)<br>0.2 | (good/excellent)<br>0.8 | 1.8 |
| Loaf 3 | (1,100)<br>1.0 | (4)<br>0.2 | (excellent)<br>0.8 | 2.0 |
| • | • | • | • | • |
| • | • | • | • | • |
| Loaf n | etc. | etc. | etc. | etc. |

(b)

**Figure 7.5(b)** Partial decision matrix for the loaf measurement system.

Creation of all of the optional combinations come next, thereby creating the full decision network. Even with a small number of parameters, and only three steps in a range, the number of alternative links becomes very large!

To make the task feasible, and to reflect that is usually restricted engineering choice, the decision tree is then reduced to its pragmatic form. What remains of the original tree is now opened out as a flat diagram showing all feasible choices remaining. Preferences for each parameter branch are then assigned in a 0 to 1 range.

Calculation is now carried out down each tree branch. The highest score is the most preferred design path. Working back up that path to the origin leads to which parameters are needed, and thus the best choice design.

This is now carried out for a simple design need—selecting the parameters and values for making a reed relay. (This example is modified from [12].)

The key design components are identified from a schematic illustration of the generic design of a reed relay, Figure 7.6(a), and listed in Figure 7.6(b).

In this case only six parameters are chosen: reed material, reed bending stiffness, filler gas, contact material, contact thickness, contact area, and contacts gap. For each the maximum number of grades or types is three.

All possible options are now drawn to show how and where they link; Figure 7.6(c). The total number of optional choices to make before the full tree can be calculated is 1,458 branches—each needing preferences to be assigned.

Since some combinations are known to be not suitable because they are not available material or combinations, or are of little importance, it is possible to remove many of the links in Figure 7.6(c). Allowing for these pragmatic factors, the grid reduces significantly to give Figure 7.6(d).

It is now time to open out the grid to form a flat tree, Figure 7.6(e).

With the tree opened out in this way, the expert then works down each branch adding the preference for each branching point (the total must add to 1.0 at a branching point). For example, *RM*2 branches as 0.4 to *SM* and 0.6 to *SH*. These assigned, the multiplicative value of each path from the top to the roots is calculated.

The highest value at a root is the most preferred design combination. Here the path is that of value 0.1411, being $RM_2 \rightarrow S_H \rightarrow G_M \rightarrow A_M \rightarrow T_S$.

The best design is then the list of those parameters plus any others that were ruled in earlier, in this case:

- Reed material—Permalloy;
- Medium stiffness reed;
- Medium gap;
- Medium area of contact;
- 1-μm contact thickness;
- Nitrogen gas filler (decided earlier);
- Silver-gold alloy contacts (decided earlier).

As the gas was already reduced to one choice only ($GM_2$)—see Figure 7.6(d)—it does not feature in the reduced grid as it has already been selected. A similar

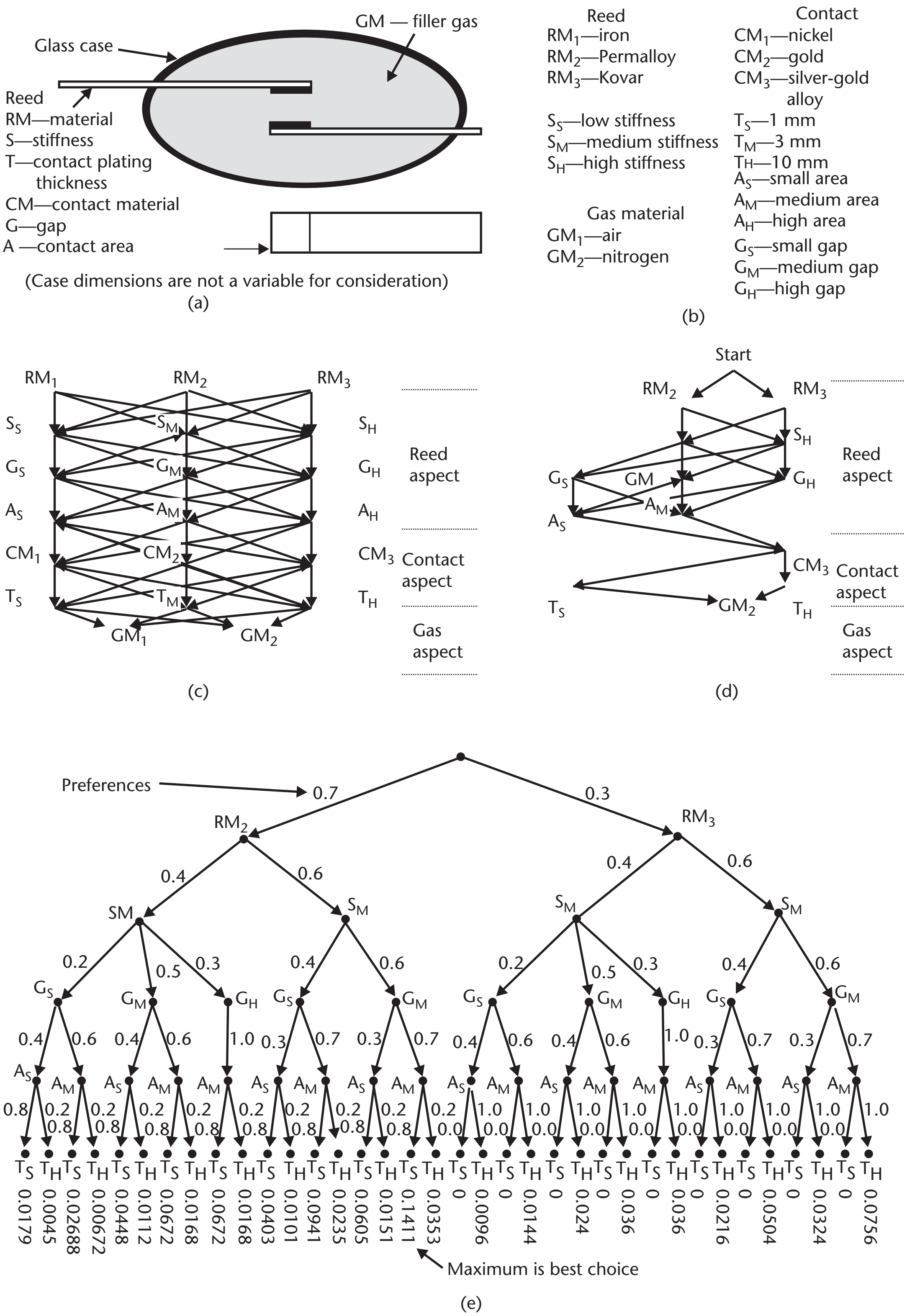


**Figure 7.6** (a) Key components to be chosen to make a reed relay. (b) Parameters identified as choice variables. (c) Decision tree with all choices present. (d) Reduced decision tree after allowing for pragmatics. (e) Opened-out tree showing all practical options. (*Source:* [12].)

situation exists for the choice of contact material for that was also selected at the grid reduction step.

### 7.6.4 Problems of Calculation

It will be apparent that these decision support methods always leave room for some doubt in that they are seeking to transform a subjective situation into an objective one without enough certainty of fact.

At every opportunity, the qualitative issues are converted into quantitative ones to allow formal procedures of math to be applied. None of the methods is judgment-free; that is easily overlooked when using the results of decision support methods. They are at best an aid to decision-making, not decision makers.

There is no absolutely sure way to calculate the decision matrix. Options for integrating the values of a row include:

- Summation, the simplest to use but does not give an alert to a 0 entry that might mean it may not be workable at all;
- Multiplication, also simple but a 0 takes the result to zero, which might indicate the system is not feasible;
- Root mean square (RMS)—gives more allowance for outlier values
- Statistical average, according to some profile, but which?

How to manage these alternatives is the subject of mathematical texts on decision-making. It can become very complex as a more certain answer is sought. The way in which the data is calculated can indeed lead to different conclusions [13].

Thus, all of these decision support methods contain doubt about their relevance. So why use them? There are some good reasons:

- Concentrates the mind on the choices to be made;
- Teases out the less understood areas of a needed decision;
- Uses some degree of systematization to the best extent possible;
- Records the thinking behind the choices made;
- Can be applied with reasonable effect if all agree to the degree of conservatism needed;
- Is better to use than a personal hunch!

It must never be forgotten that they only reduce the level of risk in decision-making and do not remove it.

Often the very act of starting to use these methods so clarifies the mind that the solution becomes obvious before the method is fully completed. They will be seen in various guises wherein different methods are combined into an integrated package. When using tools in which ideas are embedded, it is imperative that the process used be available for perusal. If the detailed operation of a tool is not known it is possible that they are not performing appropriately for a particular application. There is a case here for building your own tool [14].

## 7.7 Preparation to Make Decisions

Given the above material, it is possible to lay down a generic process for making decisions.

It is first necessary to assess the background issues:

- Amount and quality of information already available;
- How much research is needed to support the methods to be used;
- Kind of decision situation in terms of the degree and kind of uncertainty;
- Amount of time that can be devoted to the task;
- Degree of acceptance of the methods used by those approving the work;
- Where the outcomes will be used;
- What skill and experience level is available to support the task.

With these issues sized up it will be time to gather more information for as long as time permits. This sets up a foundation for deciding the type of problem and the key issues to be covered.

The relative importance of the issues then needs to be decided. Application of the parameters, their data and weightings for each now being available enables selection of a suitable sequence of decision support methods. This leads to ranking of candidate solutions.

Outcomes might need to be displayed as plots to reveal their relative cost effectiveness.

A report is then compiled to capture the process and data used and to argue how the conclusions were reached.

## 7.8 Summary

Risk in decision-making can be reduced as the parameters of the problem are better established and their numerical quantity made more certain. This chapter has given an outline of the ways in which risk can be reduced when decisions need to be made. It has covered the following aspects of decision-making:

- How the necessary information is gleaned;
- Generation and ordering of the parameters needed for making decisions;
- Consensus building to widen the breadth of facts used;
- Project checklists as aid memoirs;
- General principles of decision-making;
- Triangle of pairs, utility analysis, and decision tree methods;
- Strengths and weaknesses of the various methods.

## References

[1] Smith, N., and M. Ainsworth, *Ideas Unlimited*, Melbourne: Nelson, 1985.

[2] Blanchard, S. B., and W. J. Fabrycky, *Systems Engineering and Analysis*, Upper Saddle River, NJ: Prentice-Hall International Inc., 1998.

[3] Clemen, R. T., *Making Hard Decisions: An Introduction to Decision Analysis*, Florence, KY: Duxbury Press, 1997.

[4] Gregory, G., *Decision Analysis*, New York: Plenum, 1988.

[5] Johnson, S., *"Yes" or "No." The Guide to Better Decisions*, New York: Harper Business, 1993.

[6] Kaufmann, A., *The Science of Decision Making; An Introduction to Praxeology,* Berlin: Wiedenfeld, 1968.

[7] Linstone H. A., *Decision Making for Technology Executives: Using Multiple Perspectives to Improve Performance*, Norwood, MA: Artech House, 1999.

[8] Koomey, J., and Jon Koomey, *Numbers Into Knowledge: Mastering the Art of Problem Solving,* Oaklands, CA: Analytics Press, 2002.

[9] Sage, A. G., and W. B. Rouse, (eds.), *Handbook of Systems Engineering and Management*, New York: Wiley, 1999.

[10] Samson, D., *Managerial Decision Analysis,* Columbus, OH: Irwin/McGraw Hill, Homewood, 1988.

[11] Skinner, D. C., *Introduction to Decision Analysis,* Gainesville, FL: Probabilistic Publishing, 1999.

[12] Baker, D., et al. (eds.), *Physical Design of Electronic Systems*—Volume 1, *Design Technology*—Volume 2, *Materials Technology*—Volume 3, *Integrated Device and Connection Technology*—Volume 4, *Design Process* —Volume 5, Englewood Cliffs, NJ: Prentice-Hall, 1972.

[13] Bahill, T., S. O. Dahlberg, and R. A. Lowe, "Difficulties in Using Multi-criterion Decision Making Techniques for Tradeoff Studies Selecting Amongst Alternative Concepts," *Proc. Conf. INCOSE 98 (CD)* Section 2: paper 1.2.3, 1998.

[14] Ragsdale, C. T., *Spreadsheet Modeling and Decision Analysis*, Mason, OH: South-Western College Publishing, 2000.

CHAPTER 8

# Optimizing a Design

Sound work has led to a basic working design but that is not enough; the design then needs optimizing. This chapter explores:

- Why designs need to be optimized;
- Costs of additional effort in carrying out optimization;
- Sources of design sensitivity, and how to find and characterize them;
- Influence effects on practical realizations;
- How to go about the optimization of a design;
- Understanding how the alternative practices of experimental and modeling methods are employed to assist in optimizing a design;
- Use of reviews to maintain design integrity and thus optimum design outcomes.

## 8.1 Importance of Design Optimization

### 8.1.1 Error Propagation from Poor Design

To develop "best" designs, they need to be tuned by making use of materials to obtain best performance. Poorly set up designs all too easily lead to late errors—see Section 5.2.3—so it is important to constantly apply optimization techniques throughout the development.

For example, an electronic power amplifier may well work in limited testing but later fails due to the dissipated power being too close to a critical thermal point wherein it fails when several factors align simultaneously. Operating the power amplifier away from such critical points makes the design far more robust and capable of withstanding unexpected excesses.

By approaching the need for best design throughout the development, the rework costs are kept low. Developing the parts of systems in isolation of a holistic view can lead to serious errors and limited performance. A few hours spent reviewing a design for best operation, or increased tolerance to environmental factors, can lead to cost-effective improvements. This chapter covers these related design optimization issues.

### 8.1.2 Justification for Optimizing a Design

The creation of new technical artifacts and systems is a joyful situation. The less experienced detail designer will usually be quite delighted that a design solution has been created. However, the more experienced person will be looking ahead and thinking where it can go wrong as the initial design passes into later development stages. Issues that would be on their minds are how will the tolerance of parts add up to give a failed system from time to time, or what will happen as the assembly settles into operation.

First-cut designs often fall short of best design and are prone to poor operational tolerance. They need to be revisited and tuned by optimizing the design variables and parameter interactions.

Differing reasons exist for creating a more robust design. These include:

- Keeping competition at bay by allowing it less room to maneuver in attempting to produce a better design solution;
- Reducing the risk associated with the critical issues to which each subsystem contributes;
- Increasing the effectiveness of the operational parameters;
- Making the item more maintainable and thus giving more user satisfaction;
- Ensuring it is not operating too close to a limit, thus being more likely to fail under modest provocation;
- Increasing the reproducibility of replicated systems where tolerance spread can lead to failures;
- Increasing the safety of the system as a whole;
- Enhancing the personal satisfaction of the designer (unfortunately this is not a well-valued reason!).

Despite the existence of these many reasons, systems are often poorly optimized. The reasons for this are:

- Design can be too complex to fully appreciate in a short development time;
- Due to pressures to move onto the next steps, there might be insufficient time made available to adequately iterate the design cycle;
- Designers can be too easily satisfied that they have found a solution;
- Designers and their supervisors can be overly conservative toward making changes once a solution has been found lest it regresses instead of improves;
- There can be a shortage of adequate modeling tools, and associated experience with their use, to support efficient optimization;

Optimization will need more resources to be expended, so is it worth the extra effort?

The answer is certainly a resounding yes. Such additional studies provide confidence that a design is sound and as good as it can reasonably be carried out. Optimization studies convert a starting point design from a naïve state into one that is professionally sound.

They can also show up things that were not expected. For example, self-heating of critical components in electrical sensing systems is not that well appreciated. Yet it is simple to cope with once it has been pointed out as a factor that needs optimization. Study of the system parameters can show how to choose system parameters to keep measurement error due to the self-heating effects below tolerable levels.

Another example concerns the design of structural mechanical members, because there it is often not the load strength that matters but the deflection under load. Optimization of the load strength will usually result in an overly compliant member. The design needs the compliance to be within limits. This case shows that design is not simply a case of minimum use of resources but their use to meet the requirements; here both strength and compliance need to be satisfied without much extra cost in materials. In some cases, a design solution might be waiting to be found that is stronger, less compliant, and also less expensive to implement.

### 8.1.3 Costs of Optimizing a Design

Taking time to explore how a design can be improved will incur expenditure of early life-cycle resources. The cost issues need to be understood in order to counter the argument that costs must be kept down regardless of the longer-term impact of leaving in sources of likely error.

Cost of ownership of the finally delivered system is made up of many more factors than the initial purchase price alone.

A list of cost components that the owner has to find includes:

- Initial acquisition;
- Acquisition of spares;
- Acquisition of replacements;
- Holding costs of spares and replacements;
- Scheduled maintenance;
- Repairs;
- Loss during down times;
- Scrap during manufacture;
- Damage caused to other systems by faulty operation;
- Legal liability suits for unsafe and noncompliance;
- Acquisition of special support equipment needed;
- Personnel training for use, maintenance, and repair;
- Overheads for all operations.

To these must be added the costs of carrying out design improvements, which are:

- Increased design time;
- Increased cost of some components to obtain superior performance;
- Additional testing costs associated with the recursive design changes;
- Relevant overheads of longer development;

- Losses of scrap systems used in improving the system.

These costs are not nearly as significant in the early stages for they relate to only a small number of items, and to design changes that cost little to implement while the design is still on the drawing board.

Total costs for optimization will, if controlled satisfactorily, be considerably less than the additional recurrent and one-off costs that will need to be borne by adhering to a naïve design for the sake of short-term thinking and apparent cost savings.

Different cost scenarios might apply for a project. Which scenario is in vogue sets the design scene. These are shown in Figure 8.1:

1. Maximum effectiveness, regardless of cost;
2. Maximum effectiveness, with cost constraints;
3. Minimum cost, irrespective of effectiveness;
4. Minimum cost, with minimum effectiveness constraint;
5. Maximum effectiveness/cost ratio, regardless of any constraints;
6. Maximum effectiveness/cost ratio, with constraints on minimum effectiveness;
7. Maximum effectiveness/cost ratio, with constraints on both cost and effectiveness.

However, it is not always obvious which situation is in force. Several may seem to be the policy at the same time. They can change over the life of a development.

These alternatives show that many kinds of costs are impacted by design optimization and that they will differ in their effect, dependent on the cost scenario in force.

What is needed is a way of representing the overall situation. This is illustrated by showing the effect on costs to the owner, in terms of costs to maintain, design, and operate. Figure 8.2 shows their relationship in simplified terms, sufficient to illustrate what is at stake here. In real systems of high cost, it is necessary to conduct deep accounting analyses to establish the situation for each project.

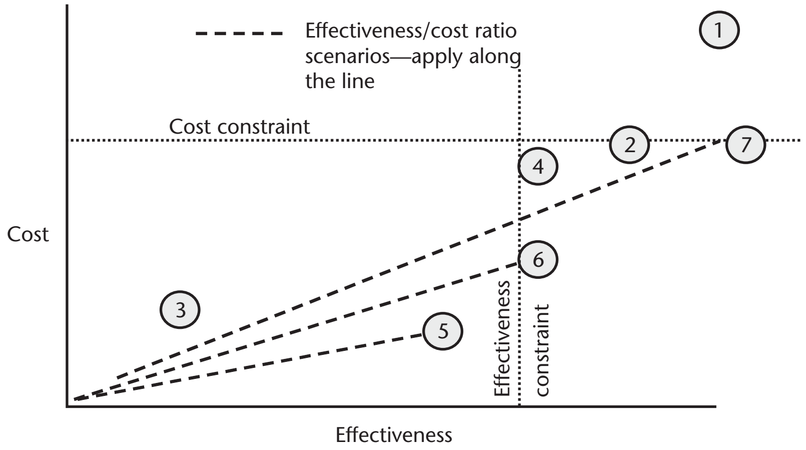


**Figure 8.1** Comparison of the alternative cost scenarios that might be in force for a project.

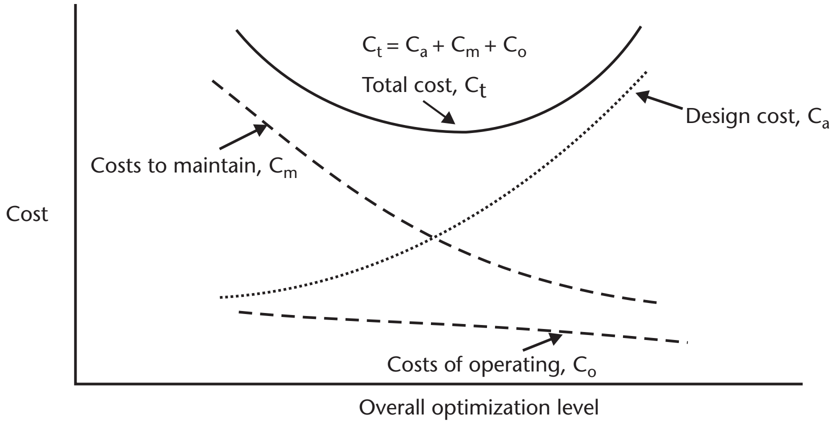


**Figure 8.2** Costs associated with optimization and how they impact ownership cost.

If greater effort is put into obtaining a more robust and better design then it is usually the case, but not always, that the maintenance cost will drop. However, to do this the cost of design increases. The costs of operation will not change markedly.

The three costs—maintenance $C_m$, design $C_a$, and operation $C_o$—can be totaled to obtain the total ownership cost, curve $C_t$. The particular set of values given in Figure 8.2 shows that there is, in this case, a minimum total cost suggesting there is a time to cease optimization work.

This finding is intuitively satisfying but it must be recognized that each case will need its own investigation. It is quite possible for resources to be expended that do not yield any gains or that there are modest gains to be had by varying the allocated effort in certain ways.

### 8.1.4 Some System Factors in Optimization

It is beyond the scope of this book to give a complete list of the parameters of a design that can be the subject of specific optimization studies. To illustrate the kind of things to consider, the following is a list of optimization aspects of an electronic system design development:

- Availability of subunits;
- Second sourcing of parts;
- Commissioning and acceptance;
- Complexity;
- Computer aids;
- Decision-making;
- Delivery;
- Designer's environment;
- Documentation;
- Environmental factors.

This brief list is for some of the systems aspects; there are dozens to consider. Note that none in the above list is about internal design of the electronic implementation itself. We come to that later.

## 8.2 Monitoring and Controlling Early Error

### 8.2.1 Keeping Watch on Systemic Issues

At the detailed design level, attention to design improvement will naturally concentrate on the inward aspects of the work being carried out by the local design staff.

Processes must be in place to help ensure that what it being done well by the design team is also being done right.

What is taking place elsewhere will be more remote, less easy to keep in touch with, and harder to influence. Communication on optimization matters between the various teams can easily suffer information attenuation with important integration design issues losing their impact. Components of a design can become fractionated and run off of the requirement rails.

There is constant need for regular checks that local work is aligning properly against key master planning documents. Responsibility for this integration lies with the design team leadership, for they are the people who form the human interfacing between design groups and the overall systems engineering leadership. They will have access to the key technical planning documents including the equivalents of the systems engineering plan, test and evaluation master plan, and the ConOps and requirement statements.

However, all of these documents were formed in an earlier time of learning the development. They were visionary statements made about an uncertain envisaged future. No matter how good the planners were at their job the vagaries of real life will often upset the best-laid plans. To counter the unpredictable issues the various master plans should be the subject of regular review and upgrading. That is the job of the systems engineer. Such changes then filter down into regular design team reviews to show where designs need to be modified.

Conversely, designers will sometimes find that the information given to them, on which their designs are to be based, does not fit in some way. For example, a specification may call for a given level of computing power, but time has so overrun what was the best available at the time that it now seems unsound to supply it in the originally called for form.

Making changes locally can incur unpredictable and major impacts elsewhere in the system development. Change notice processes must be used where optimization changes impact on other parts of the design.

## 8.3 Sources of Design Sensitivity

### 8.3.1 Developing Design Sensitivity Tables and Charts

Experts will be very familiar with the sensitive spots of design in their own area of expertise. They instinctively will know what to investigate when tuning a design.

This said, the fact is that it is easy to overlook important factors. In addition, it is commonplace to assume the newer team members have as much experience as the older ones. To this end, it is unwise to leave what has to be done entirely to one's commonsense and memory.

A systematic, recorded method is needed to ensure optimization actions are taken. Sources of design sensitivity, in terms of variables and effects, should be recorded and checked off as they are investigated. Various recording methods that can be employed include:

- Matrix plots showing variables and risk levels (see examples in Table 8.1);
- Tabular listings (see examples in Table 8.2);
- Databases of the formal kind, preferably as a relational or object-oriented system;
- Sensitivity graphs.

For simple studies, the tables need not be that sophisticated. If the number of linking relationships becomes too large to remember easily then a database or use of hyperlinked files are worth considering. The key thing about these data sources is

**Table 8.1** Examples of Detailed Design Aspects Sensitivities for Components in an Electronic Amplifier

| *Detail Aspect* | *Envisaged Design Sensitivity* | | | |
|---|---|---|---|---|
| | *Ambient temperature (-10°C to –70°C)* | *Ambient pressure* (-10k to 70 kPa) | *Relative humidity (10%–90%)* | *Mechanical vibration (0–20 mm/sec in three axes)* |
| Resistors | High | Low | Medium | Low |
| Op-amps | High | Low | Low | Low |
| Voltage source | Medium | Low | Medium | Low |

(*Source:* Peter Holloway.)

**Table 8.2** Some System Aspects and Sensitivities

| *System Aspect* | *Description/Consideration* | *Sensitivity Assessment* |
|---|---|---|
| Commissioning and acceptance | Location of production commissioning and acceptance<br>Personnel involved<br>Timing of commissioning and acceptance. Time required to conduct.<br>Procedures to conduct commissioning and acceptance<br>End-user involvement—skills, numbers | Level of influence effects (temperature, pressure, vibration, relative humidity, EMI) in operating environment, versus specified levels |
| Complexity | Risk assessment, including mitigation strategies<br>Technologies reuse<br>Use of state-of-the-art technologies | Incorporation of features in design (selection of components, calibration) to compensate for influence effects |
| Computer aids | Mechanical simulation tools—shock, vibration, temperature<br>Electronic simulation tools—circuit simulation/emulation | Accuracy of mechanical and electrical simulations versus actual system performance |

(*Courtesy:* Tim Welburn.)

that they should flow into subsequent projects for appropriate reuse. All too often they are not formalized into company SE practices and thus become forgotten orphans once a development is completed. The next team has to relearn the factors again, often making the same mistakes!

The sophistication of such tables will depend on the time available to compile them. If they are to be used as part of a defined company process, they will need more regulation and explanation than if created for personal use.

Setting up a relational database, such as can be easily done in MS® Access, will entail some initial work. Once in place, however, the knowledge can be easily topped up, give useful checklists by way of a query function, compile reports using a report function, and afford ready access to the hard data needed via sophisticated sorting.

Having set up a system for developing reliable lists of related variables, the next step is to find out how they relate to each other.

For example, it is easy to realize that the stability of an electronic power supply voltage probably depends on temperature, but just how does it vary as the ambient temperature of operation varies? The optimized system should best work where the parameters vary at low rates of change, not where a small incremental input of an unwanted variable creates a large change in the wanted output.

In practice, the situation will have more than one variable changing at any given time, each with a different rate of change. Optimization in such cases requires a designer to exercise professional judgment of how to pick the best parameter values. That is often done best by visually observing the appropriate sensitivity curves using an eyeball analysis—looking at them all, seeing what the various movements are as one is varied. Setting this up to find a multivariable optimization by formal mathematical means is often not feasible due to overwhelming complexity, or lack of sufficient time to generate a realistic optimization model. The methods given in Chapter 7 can be used here to estimate overall behavior.

Sensitivity profiles can be generated by mathematical models, or from practical testing; the methods are discussed later in this chapter. Figure 8.3 shows a generic example of a two-dimensional sensitivity profile.

If the system is operating at the steep part of the profile shown, then a small change in the absolute value of the unwanted input parameter will give rise to a large swing in output effect. It is best to operate the design where the slope is flatter and with the lowest sensitivity. It may be the case that low parameter performance has to be tolerated to gain flat error sensitivity over a wide range of unwanted input.

The nature of the sensitivity profile can be very revealing. The profile in Figure 8.3 shows how the sensitivity of the hypothetical design feature varies quite unexpectedly and that the design just might be set up to operate in a very poor place.

Profiles can be made up of various types:

- Single steady slope—use anywhere as the working point. Rate of slope indicates the degree of control needed over the sensitive variable.
- Minimum dip, or maximum peak—best to work the system at these positions as the sensitivity is there least for a wider range.
- Complex slopes—offer definitely optimum positions (as in Figure 8.3).

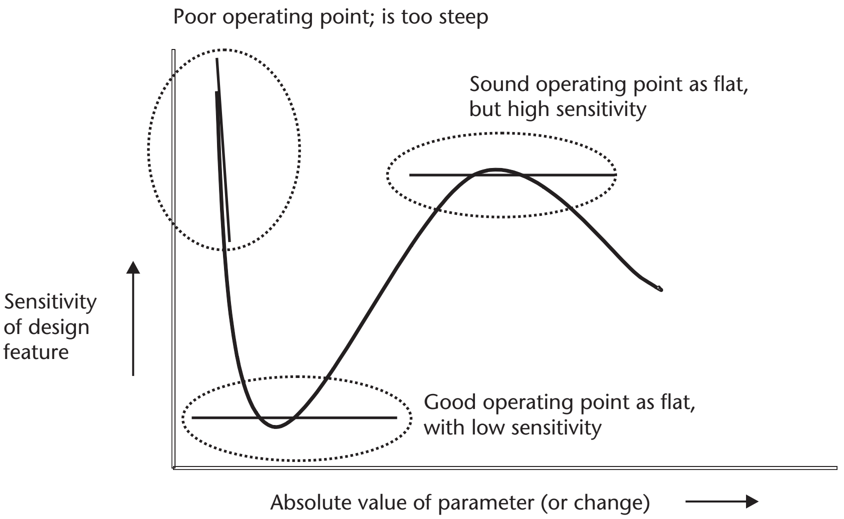


**Figure 8.3** Generalized example of a 2-D sensitivity profile.

- Sudden sharp slopes and short spikes—operating points to keep well away from.

In practice, real situations will have several parameters with different sensitivity profiles. The 2-D profile can be extended to cater to three dimensions, to create sensitivity surfaces. Figure 8.4 shows an example. These are more difficult to interpret but do show up the good and bad regions.

It becomes very difficult to show greater than three dimensions in one plot. Larger numbers can be handled by setting up many 2-D profiles in one viewing area, and by use of different colors.

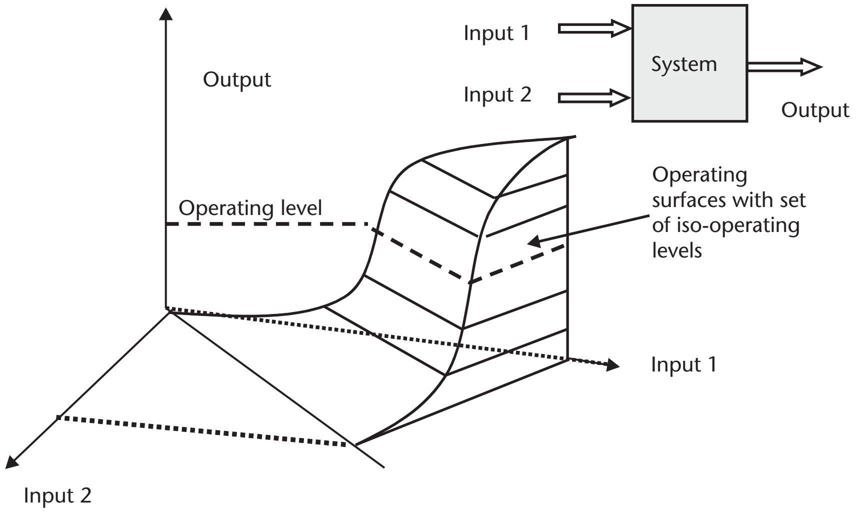


**Figure 8.4** Operating surfaces for a system; 3-D representation of sensitivities.

Another way to increase the number of variables being optimized is to normalize them in pairs, thus reducing the total number by one dimension for each normalization undertaken.

An example of a system being optimized is found in one form of precision gravity meter used in oil exploration. This design comprises a simple, highly delicate, spiral spring supporting a small mass. The gravitational attraction between the Earth and the mass causes the spring to vary in length. Minute variations in the spring's length provide a measure of "g" at that location.

It is impossible to design a perfect spring in which the spring rate is totally insensitive to ambient temperature. However, it is known from experience that the spring rate for the material used varies with ambient temperature with a temperature sensitivity profile that has a peak (i.e., giving a flat zone) that is slightly different for each individual spring. To gain optimum sensing stability, the spring and displacement detector unit of the gravity meter are placed inside a temperature-controlled housing. The internal temperature is tuned to make it operate at the temperature of the least sensitive region of operation. Once the optimum temperature condition has been established the gravity meter is then continuously temperature controlled. Turning off that control will cause the spring sensitivity profile to change, necessitating a recalibration.

Why go to such lengths? In this case, there is no better alternative for obtaining the optimum degree of measurement precision. Sensing capability is worth large sums of money because it can be a major element in the discovery of oil.

### 8.3.2 Sensitivity Control Process

Real systems will have numerous sensitivities to consider, especially at the detail design level. It is not possible to consider all existing sensitivities for a system in great depth so the first step is to use available knowledge sources See Section 7.1, to identify likely effects.

Clues are to be found by working through the standard lists of external influence effects that are covered in Section 8.4. Do not forget that a design may also have internal design sensitivities dependent on the operating level of the system itself.

The dominant effects are then ranked according to their relative importance. Where they are still quite subjective, use of the methods outlined in Section 7.6 will help to establish their order of priority. Where they can be quantified, the worst case design situation should be roughly calculated to yield the orders of magnitude of the effects. This soon sorts out those needing attention and redesign.

Usually the effects of temperature will be larger than those of other parameters—but that is not always so.

When the design circumstances are different to previous experiences, do not risk leaving what to look for to unsubstantiated opinion. Surprises are frequent and it is better to find out early! Make an exhaustive list of all effects that can be envisaged and systematically rule them in or out by some simple calculations.

When the critical issues of design sensitivity have been clarified, the next step is to give them all an assigned magnitude along with their individual uncertainty estimate.

Having decided which sensitivities need alteration, it is then time to systematically reduce them, starting with the most sensitive first. It is a good idea to set numerical targets for required sensitivity levels, for it is easy to spend too much design time on some that are not that important.

One sound method for controlling the overall optimization process is to set up a link diagram moving from the existing sensitivity situation of the chosen parameters through to the desired ones. These chains will, at times, link to other chains due to their interdependence. Along each path, create "islands of certainty" where an interim target is set. Gradually whittle away at all links, creating desired uncertainty levels for the islands. With this method, the overall sensitivity position situation will be clear at anytime, as will the weakest links still needing attention. More is given on this method in Section 12.3.1.

## 8.4 Influence Effects on Designs

### 8.4.1 Nature of the Influencing Effects on Design

Any design will need to operate satisfactorily within a given set of ambient conditions. All systems are influenced by these external parameters to varying extents. Even seemingly simple systems will be impacted in complex ways.

To appreciate the extent to which these effects complicate design, consider the displacement sensor formed by using a simple electrical capacitor formed with two parallel conducting plates of area $a$, and having a separation of $d$. The material between the plates has electrical permittivity $\varepsilon$.

Elementary physical explanations model the relationship of these parameters at its first principles level as:

$$C = \varepsilon\, a / d \tag{8.1}$$

From this simple relationship it is possible to calculate capacitance for any combination of the three design parameters $\varepsilon$, $a$, and $d$. This simple model may well suit understanding of its general behavior but it is far from realistic enough to support practical design. It needs extension to allow for secondary effects that engineers cannot omit to consider.

In use, the capacitor will be subject to several dominant ambient environment parameters. The area of the plates will depend on their temperature; size will change with temperature. As there must be a structure to hold them in place, the gap is also temperature-dependent so that will also change the value of $C$.

Now consider the material in the gap for which its permittivity value is critical. This is also usually temperature-dependent and could also be subject to ambient relative humidity (RH) effects.

For very sensitive use, the ambient pressure (P) can also affect the physical dimensions of the mechanical parts.

If the original equation has all of these factors added to its model, it then becomes

$$C = \varepsilon\, fnc(T, P, RH) \cdot a\, fnc(T, P) \,/\, d\, fnc(T, P) \tag{8.2}$$

To make matters more complex, the T, P, and RH parameters are often interdependent. Furthermore, each parameter can also be time-dependent and vary according to its recent past and long-term, past operational history.

In use, the expanded model of (8.2) needs material data for the various coefficients of the expanded model. These are not always available to the level of precision required.

Thus, the original model has rapidly become complex and difficult to apply. It is not surprising that so much design is done using only the first level modeling of devices, but that is not sufficient.

It is always necessary to decide what secondary influence effects need to be considered. Often, seemingly unimportant parameters can have a large impact on system performance. For example, natural environment systems are particularly prone to trigger effects that occur when a highly sensitive parameter undergoes a small variation causing major output swings in system behavior.

### 8.4.2 Commonly Met External Influence Effects

A system has to operate satisfactorily in the environment for which it was designed. Taking it outside the specified envelop means it may not perform as well as needed or even fail.

A development needs to have its working environment carefully specified as part of the requirements capture process. The construction of a boundary limits diagram (see Section 5.2.1), assists identification of critical parameters.

Often, in small projects, this important aspect is ignored or misspecified by persons who are not familiar with the realities of design limitations.

For example, a pressure sensor was to be developed to replace one that was failing too often in use. At first, the customer did not consider the working environment other than to describe the likely situations. When asked to confirm a set of working conditions that it had to work within, the customer's response was to ask for those stated for the previously used units—but with all parameters increased by 20%. This led to a design that was impossible to make. When asked how the customer would test the sensor systems, it became clear that no adequate test plant was available, meaning it would not be known how it well it would perform until placed into use, thus repeating their original difficulty.

This example is typical of too many design situations. It is up to the designer to broach the issue with the customer, otherwise critical issues like these can go unaddressed until the crucial time of operation.

The following are the main external effects to consider.

*Ambient temperature.* This is the most dominant effect. Effects usually vary according to the absolute (Kelvin) temperature scale. For convenience, a temperature coefficient may well be quoted for a component at a stated temperature, yet it can be different at other temperatures of operation. Sometimes a better statement is available as a mathematical law or a graph. Quantitative detail of influence effects is paramount for best design.

The design situation may not be only for a long-term, steady-state situation but be working under transient conditions where component parts are at different temperature values for a period of time as heat transients settle.

Temperature differential across the parts of equipment are often a cause of major error.

*Ambient pressure.* This is less often a problem than temperature. Its effect can be small enough to ignore unless the situation has large excursions of pressure such as those that arise in underwater, flight, and space applications. Just how small it is needs to be verified by some rough order of magnitude calculations. Note that even in sealed chambers the internal pressure is dependent on temperature, as characterized by the gas law of physics relating volume, pressure, and temperature. Related is the fact that transporting instrumentation and other delicate equipment in nonpressurized aircraft holds can lead to loss of calibration or destruction due to the severe pressure variations.

*Ambient relative humidity.* The moisture content of ambient air can give rise to sensitivities where air gaps are used in electrical devices such as capacitors. It also affects surface charge effects and can give rise to corrosion and surface leakage effects for electronic components. A conformal coating of a specialized vacuum deposited monolayer polymer is used to reduce these effects.

*Electromagnetic interference (EMI).* Electromagnetic waves emitted from sources, such as electric motors and transmitters in cell phones, are complex and can seriously interfere with electrical systems. Many computer modules generate EMI. Sealing systems to prevent radio frequency (RF) leakage from inside units to a minimum needs carefully executed, complex enclosure design.

*Mechanical vibration.* Acceleration of component parts from operating excursions and vibrations will create higher forces on parts than for a static system. The simple measure used is g-force, that being the increase in its effective mass, which is proportionate to the g value. Humans can stand forces of 3 to 5g. In situations such as those that arise in explosions, the accelerations can rise to thousands of g, thus exerting extreme forces. The lifetime of many materials is dependent on the number and amplitude of the times the forces reverse. Large magnitude cycles will cause failure earlier than small excursions, but even minute vibration amplitudes can, for many materials, eventually cause failure due to collapse in strength or excessive creep in size.

*Ionizing radiation.* Effects created by such things as X-ray generators and nuclear materials can give rise to unsafe systems. These effects can also impact operation. As with EMI, this is a complex issue with effects varying with wavelength. This parameter is also one for which there is no clear design situation, for the long-term effects of it are still regarded as problematic. Semiconductors exhibit cumulative effects to radiation; they also exhibit this for high temperature use. Gallium Arsenide (GaAs) systems used for the higher temperature applications, such as deep borehole logging, have recorders installed to take a record of their time to allow allowable operational life to be estimated.

*Time.* Time will affect all design parameters to some greater degree. As the magnitude of time effects get smaller, it becomes increasingly more difficult to formalize the behavior. Heuristics that describe the various relationships are often used to capture these characteristics.

Those mentioned above are the most commonly encountered influence effects. Many others exist for specialist areas of design; they will be known to those working in the area. For example, merely changing the hydrogen annealed magnetic shields used in accurate CRT systems can destroy the protection simply by removing them without taking care not to stress the metal.

Checklists of those relevant to a design team's work should be developed as they are realized. Each effect should be named and characterized in terms of its impact, likely interactions, quantitative assessment method, and means for reduction. It is better to rule them out from a generously long list than it is to overlook them at the low-cost early design stage!

### 8.4.3 Minimizing Influence Effects in a Design

Once a first draft design has been generated, it then has to be optimized to reduce unwanted sensitivities. Improvement in tolerance to the many influence effects is usually done by considering each in turn, assuming there is no interaction between them. That certainly makes good progress but interactions need to be considered in due course.

Effects are minimized by altering the design using one of three main alternatives:

- *Avoidance.* Use an alternative principle, or implementation. This may not be possible because an alternative cannot be synthesized. If it can, and it is better, then the alternative should be used anyway.
- *Elimination/reduction.* Design for tighter design parameters and parts specifications. This is a safe way to proceed but it will usually incur increased costs for the higher tolerance parts.
- *Compensation.* Reduce unwanted effects as far as is economically possible and then use some means to reduce the unwanted effect by deployment of some form of compensating mechanism. Examples are temperature control of temperature-sensitive parts, or common-mode noise rejection systems in electronic instrumentation amplifiers. This method must be implemented carefully, for usually the amplitudes of the original effects are still large and thus can cause other deleterious effects such as saturation of signal excursions. Compensation is often the only way forward when materials and fundamental laws pose limits on design freedom.

A word of warning! A final design that is overly full of sophisticated principles, tight tolerance parts, and using complex compensation may seem to be a real design achievement but experience has shown that not keeping designs simple can lead to operational and support difficulties.

## 8.5 Optimization Methods

### 8.5.1 Role of Engineering in Optimizing Use of Resources

Design is a process of applying and testing alternative solutions to the many specific situations that arise in a development. Once a design has been developed, it should be considered for its goodness. It is best to have available several candidate solutions, not just one. Optimization effort will soon show up deficiencies that can rule out the first choice.

Two ways exist for exploring the goodness of a design: by using abstract computer-based models in mathematical form, or by building a physical prototype on which are performed organized experiments. Both have their place.

Mathematical modeling is the preferred means for making a fast study of parameter sensitivities; however, development of a sufficiently detailed model may be prohibitive. See Section 11.4 for more on models.

Some industries, notably the electronic one, have sophisticated models and tools available that support design to the point of not needing physical prototypes to assist development. However, mixed regime design is another matter. Some areas are poorly supported because formal description has not been as achievable as it has for the electrical regime.

Experimental methods of optimizing systems are usually needed to ensure no surprises appear at the manufacturing stage but the trend, especially in the electronic regime, is clearly toward modeling that leads to real systems needing little correction.

### 8.5.2 Design Sensitivity Analysis Using Mathematical Methods

Here, a mathematical model is generated of the system. Model development is best started from the commencement of the project, increasing in sophistication and detail over the product or service life cycle.

Mathematical models only represent aspects of the real system, not the whole; this tends to be overlooked. The first step when using a model is to verify that it adequately covers the behavior being optimized. Models not built to strict policies and processes need care in application. Section 11.4 covers the setting up of models.

Assuming an adequate model has been realized, the next step is to determine the sensitivities to be explored.

After setting the model to the nominal state, each parameter is exercised in turn, recording the appropriate outputs. Results are shown using graphical displays.

Models work well in closed systems design situations but are more risky in open system investigations.

To illustrate the underlying process of optimization by a mathematical method consider the simple electrical thermistor sensor system, as has been studied elsewhere [1].

A thermistor is a nonlinear, temperature-sensitive, semiconductor device in which its electrical resistance reduces as temperature rises according to a well-defined exponential law.

The sensing thermistor is interrogated by using it to form, in its simplest use, one arm of a Wheatstone bridge as shown in Figure 8.5.

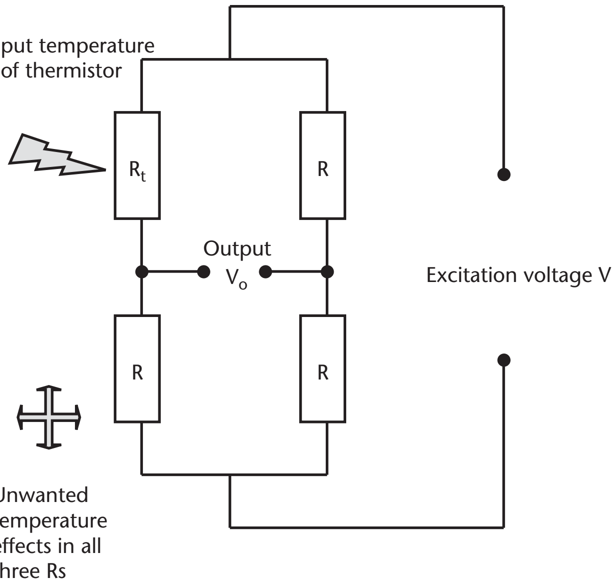


**Figure 8.5** Simple thermistor thermometer circuit.

As temperature varies the resistance of the thermistor $R_t$, the voltage output of the bridge $V_o$ varies in a systematic, predictable, manner.

Choice of system components can make a large difference in performance of the sensor system. Two optimization issues that are usually needed for a sensor system are its sensitivity as a temperature sensor, and sensitivity of the circuitry elements to temperature change (which can generate apparent temperature errors).

The optimization task is to decide which component values will give maximum temperature sensing and to select operating conditions that make internal and external error sufficiently small.

The first step is to set up the equation expressing the relationship between the temperature input $T$ and the output voltage $V_o$, this being expressed in terms of the value of the resistor $R$ used to form the fixed resistor arms of the simple bridge. The output/input relationship here is:

$$V_o = V \cdot R_t / \left(R_t + R\right) \tag{8.3}$$

where $R_t = R_{20}$ . exp (B/T – B/293), B being the characteristic temperature constant for the specific model thermistor, with T being in degrees Celsius.

This expression can be differentiated to show the rate of change of the output with temperature input to obtain:

$$dV_0 \;/\; dT = V \cdot R \;/\; \left(R + R_t\right)^2 \cdot dR_t \;/\; dT \tag{8.4}$$

Where this equation has a maximum or minimum is the optimum value of $R$ to use. A plot of (8.4) for a given typical sensor setup shows that it is a slowly varying, relatively flat, rising curve indicating, that the largest value of $R$ is best to use. In addition, it is found that varying *R* makes little difference to the sensing sensitivity. This has established the first optimization requirement, the best value of *R* to use.

Having chosen the best *R* value, the next step is to select the optimum voltage $V_o$ at which to excite the bridge. Equation (8.3) shows that the output voltage is proportional to the excitation voltage. Upon first sight, this suggests that the excitation should be made as large as possible. However, there are other factors to consider because *V* also decides the internal working conditions of the bridge components.

Inspection of the circuit of Figure 8.5 shows that the excitation voltage generates currents in all resistors forming the bridge and for all values of sensing range. Even when the output voltage is balanced to the zero condition in the bridge, these currents are still flowing.

Current flowing in a resistor creates self-heating in the resistor. The bridge resistors are chosen to be stable with temperature change so they are little affected by this quiescent heating. The thermistor, however, is especially sensitive to temperature change and thus rises in temperature giving the appearance of a sensed temperature rise. This is called the self-heating effect.

Thus, *V* must be chosen to be sufficiently low as to keep the self-heating effect to a tolerable level. A math model is generated to show how self-heating changes with *V* and *R*. Power dissipated in the thermistor is given by:

$$P = V^2 / (R + R_t)^2 \cdot R_t \cdot \theta \tag{8.5}$$

where $\theta$ is the thermal resistance of the thermistor type being used. This expresses the temperature rise, caused by the heating taking place in the device due to the current flowing in it, as degrees Celsius per watt of heat dissipated.

From this, it is seen that the ideal excitation *V* to use from this point of view is as small as possible. Being a square law effect, the self-heating error reduces rapidly as *V* is reduced. However, *V* has to be large to obtain the best temperature sensing ability.

This situation, where optimization parameters are in conflict, is common in design.

To resolve this conflict, use can be made of the fact that a certain level of self-heating can be tolerated. The allowable amount of self-heating is a temperature rise that is just smaller than the temperature discrimination of the thermometer. After deciding the tolerable self-heating temperature rise, (8.5) then can be used to calculate the highest allowable *V* value.

Thus, the best possible *R* and *V* values can be found for a given design situation.

Following through model developments in the above manner greatly assists understanding of the various parameters and interrelationships.

Sensitivity exploration of systems that can modeled in transfer function format has been detailed at depth in [2]. This approach is highly applicable for systems that operate in the electrical regime but is less convenient when mixed regimes are involved. Systems behavior modeling tools, such as Matlab™ and IThink™, offer easy-to-use interfaces to assist in setting up a study without the need for deep expertise in the mathematics involved. More detail of sensitivity analysis is available elsewhere [3].

How far one should take this modeling approach depends on:

- How much time is available to develop a comprehensive enough model when the situation may not be at well known and there is need to get results in a hurry;
- How well the real situation is understood;
- How skilled the designer is in setting up sound mathematical models;
- What tools are available to make the mathematical task less tedious.

### 8.5.3 Design Sensitivity Analysis Using Experimentation

Instead of setting up models, the alternative is to build the actual system, or the relevant parts of it.

After setting all parameters of an adequate representational system to their nominal operating points, the critical parameters are varied under tightly controlled physical conditions.

Although it is sometimes feasible to vary more than one variable at a time, later separating their effects, it is advisable to vary only one for each test run. Variations are plotted against parameter value changes to see trends and sensitivities. The design is then upgraded and retested. Changing one value to reduce sensitivity may well increase the impact of another. A trial run of tests to establish such interactions is worth the effort before serious investigation commences.

This method is simple to put into place and needs little mathematical skill for its implementation. It is, however, very expensive in terms of time and cost of test resources. It is also not that effective when interactive parameters exist, as that needs numerous test runs to characterize the situation. For the more complex and costly tests, they need to be set up using the power of design of experiments (DoE) skills (see Section 11.6.2).

As an example of preparation for testing, consider the optimization of the design of a data acquisition system (DAS). First, a system schematic is developed that is blocked into organic units where test signals can be inserted and monitored (Figure 8.6).

A test plan is drawn up that shows the nature and order of the sequential tests. Calibration of test equipment is essential and should be carried out both before and also after testing.

To reduce the chances of failure during the study, it is advisable to exercise the system thoroughly before sensitivity investigation commences.

Output is recorded as each input is varied around its nominal working point. Plots of each set of values produce a set of sensitivity charts that can be studied as a whole to decide which features are to be modified by redesign.

One difficulty to be faced is that the system may fail during the test sequence. Repair can be undertaken to allow the tests to continue but care is needed to ensure system performance is not altered. Switching to use of a second backup system may seem to be a good idea where the original fails. This is not recommended, because the second system can have a different characteristic, making it hard to use the two sets of data in a seamless manner.

Carefully undertaken experimental technique and tight records are essential to avoid human error “noise” perturbing the results. As real system testing is an experiment to see what has been designed, it is likely to show up other unexpected effects.

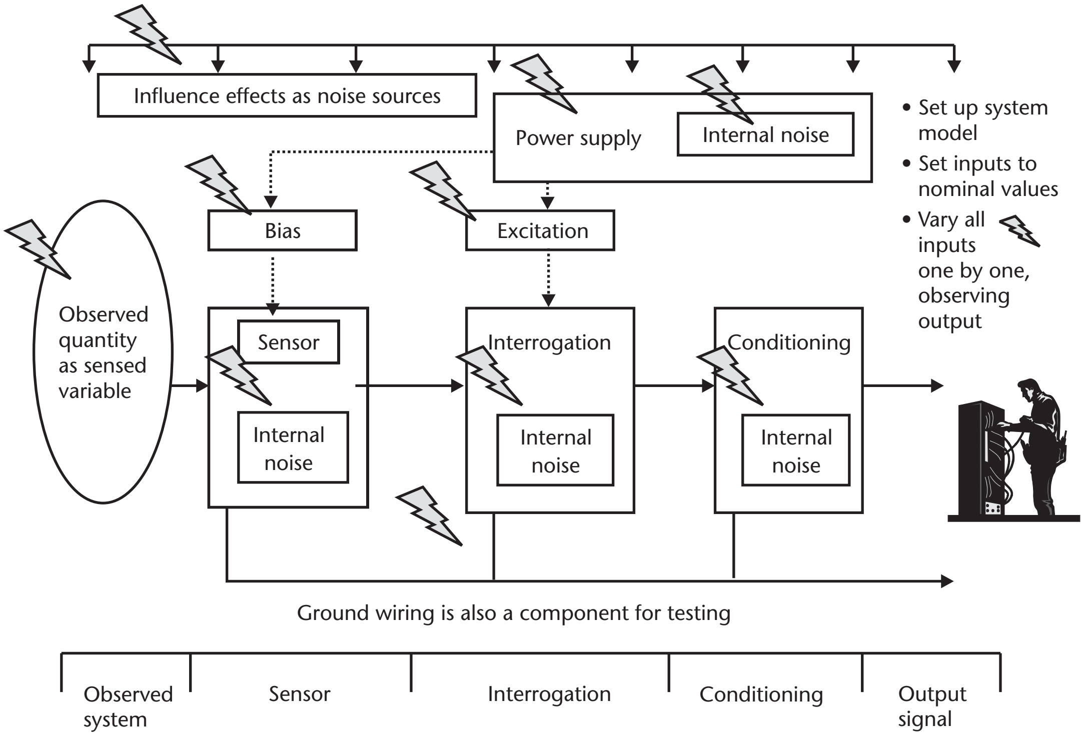


**Figure 8.6** Systematic optimization of a DAS unit.

The processing of data conversion during testing is less of a challenge than it used to be. Good software tools exist to convert raw data from DAS units into viewable results as fast as the data is generated. Real-time conversion is recommended, as rapid knowledge of the results leads to better understanding of the system and to improved discovery of design weaknesses and their correction.

## 8.6 Project Reviews

### 8.6.1 Purpose of Reviews

If all the people involved in development went their own way, they would undoubtedly stray from their targets, lose synchronism with the whole effort, and sit on problems until they were exposed, perhaps too late for low-cost correction. Even with lodgment of written progress reports in place, there is still need for face-to-face meetings, for that brings out issues that can go undetected in reports. This interaction takes place in a range of review meetings.

The purpose of review meetings is to formally investigate, in a logical manner, the state of activity for a life-cycle stage or an aspect of a design. These are usually run as a sequence of people reporting on issues according to an agenda giving the items for discussion. Reviews:

- Provide a formalized, preconsidered, audit of proposed and planned activities and their current position;

- Cover major issues;
- Integrate aspects of the project in a holistic manner;
- Firm up needs for corrective action that leads to plan variations or even replanning;
- Expose errors as early as possible.

Although it may not be the main aim of reviews, their activity keeps all concerned on their toes because this is where people external to the design team will become aware of poor progress and difficulties. Some organizations maintain a standing design review unit (DRU).

A preagreed agenda is usually used to give all concerned as a common baseline for the discussions. However, this practice can lapse into being a routine wherein those involved do not speak out on the difficult issues that should be addressed. The review leader should use tactics during the meeting that ensure an accurate report of the situation results.

### 8.6.2 Project Management and Engineering Design Reviews

Several reviews with different purposes can be identified over the system engineering life cycle [4]:

- Mission concept review;
- Systems requirement review;
- Systems definition review;
- Preliminary design review;
- Critical design review;
- Production readiness review;
- System test review.

A systems design review (SDR) is held to specifically concentrate on the outputs of a current design phase activity. Comprehensive checklists for an SDR are given in [5]. Table 8.3 is a simple list that shows the kind of issues that might be addressed in an SDR.

There are many project aspects to review; they cannot all be covered at the same depth. An overall list of activities would include:

- Requirements analysis;
- Functional design;
- System configuration;
- Operational performance;
- Interfacing;
- Environmental conditions;
- Ergonomics;
- Maintainability;
- Reliability;

**Table 8.3** Checklist for Systems Design Review

☐ Operational requirements defined
☐ Effectiveness factors established
☐ System maintenance concept defined
☐ Functional analysis and allocation completed
☐ System trade-off studies documented
☐ System specification and supporting specification completed
☐ Economic feasibility determined
☐ Systems engineering management plan completed
☐ Test and evaluation management plan completed
☐ Design documentation completed
☐ Logistic support requirements defined
☐ Ecological requirements met
☐ Societal requirements met

- Availability;
- Design for manufacture;
- Mechanical design;
- Testing, evaluation, and acceptance;
- Packaging, handling, and storage;
- Postdelivery support;
- Societal factors;
- Planning and scheduling;
- Training;
- Quality control and assurance;
- Financial;
- Tools and development environment;
- Documentation.

The highest level of review will be those about the project itself. They will be the responsibility of the senior technical staff such as the project manager or systems engineer. These are mostly held close to milestones. Attendees will be the representatives of the contractor and the customer.

The agenda of project meetings will be set to investigate issues at a higher, broader level than those of the engineering detail design work. Such meetings can last for many days and will usually involve bringing in staff from different locations or setting up teleconferencing by phone or videophone.

At these high-level meetings, the team leader will represent the detailed design teamwork, taking into the meeting any team members needed to cover specific agenda items. The design team leader will have been advised of the agenda and should prepare for this ahead of time to allow issues to be well considered by the team.

Typical issues that rise to this level will be how well TPM and the like are maturing, how well design is progressing to time targets, what integration issues need addressing over the project, staff allocations, and future senior-level meetings with the customer.

Internal design reviews are held, monthly or weekly, to suit the manner of management in place for a project.

The agenda and thrust of internal meetings is different (or should be) than those held when the customer is involved; for now, holding back bad news should be replaced by facing it and setting up solutions to difficulties.

Special, one-off, review meetings will also be held as needed. An example is the need to review an aircraft design when a first-weight estimate, using the formative information, showed it exceeded acceptable targets. That meeting was held in the style of a brainstorming session, with all specialists concerned called upon to show how and where they could save weight in their aspect of the overall development.

What has to be controlled in high-level meetings is the tendency for them to degenerate into general learning and reaction sessions. There the critical business of the meeting becomes seriously diluted and unduly lengthened by weak chairing that allows activity to stray from the critical aspects of agenda issues.

Ways to control this tendency are:

- Issue a detailed agenda well in advance. Insist items have well prepared attachment reports available and that any items needing discussion are made clear by a specific call for discussion as the meeting starts.
- Make it a rule that only items that are predefined can be discussed, unless they are notified at the start of the meeting for the "any other business" (AOB) time.
- Assume all items are accepted as given in the agenda attachments unless they are marked at the start of the meeting for discussion.
- Chair the meeting by allowing only issues to be discussed that clearly need the assembly to cover them.
- The chairperson should not be required to take notes of the meeting, for he or she will need their wits about them at all times.
- Make it clear that all members of the meeting as well as the chairperson have the duty to keep discussions tight and to the point, and to ask penetrating questions. These are occasions for revealing issues that are easy and less expensive to fix at the time!
- Have available audio-visual aids to support presentations and recording.
- Take care to read well below the surface of viewgraph presentations, for their excellence of creation can easily hide the reality of a situation.
- Keep minutes of meetings short, reporting only critical issues, actions to be taken, and who has the responsibility for carrying out each action.

The design team will also hold internal review meetings on a regular, usually weekly basis. The design team leader will organize and chair these. They can be less formal than project-level reviews and delve into more detail than would a project meeting.

These meetings concentrate on local internal design issues, progress being made, difficulties, costs, and any particular team support issues. It is important that sufficient time is made available and that attendees are encouraged to participate and reveal problems. A more detailed explanation is available on reviews in [6].

## 8.7 Summary

Once a first cut design has been developed, it should be revisited to optimize its operation and performance when used in realistic environments.

The reasons for optimization have been explained, as have the cost issues.

Alternative methods of investigating sensitivity using mathematical modeling or physical experimentation have been put into perspective using some examples.

The role and place of project management and design reviews has been discussed, providing pointers to their composition, activity, and issues that need to be addressed.

## References

[1] Bell, E. C., and L. N. Hulley, "Precision Temperature Control," *Proc. IEE*, Vol. 113, No. 10, 1966, pp. 1671–1677.

[2] Stubberud, A. R., I. V. Williams, and J. J. DiStefano III, *Schaum's Outline of Feedback and Control Systems*, Whitby, Ontario: McGraw-Hill Trade, 1994.

[3] Kleiber, M., and T. Hisada, *Design Sensitivity Analysis*, Encino, CA: Tech Science Press, 1993.

[4] Sage, A. G., and W. B. Rouse (eds.), *Handbook of Systems Engineering and Management*, New York: Wiley, 1999.

[5] MIL-STD-1521B, *Technical Reviews and Audits for Systems, Equipments, and Computer Software; Appendix B "System Design Review," Washington, D.C., USDOD, 1985.*

[6] Feedman, D. P., and G. M. Weinberg, *Handbook of Walkthroughs, Inspections, and Technical Reviews: Evaluating Programs, Projects, and Products*, New York: Dorset House, 1990.

CHAPTER 9

# Suitability and Operability Aspects of a Design

Appreciation of the design issues related to the developed system being able to do the right job, when called to do so, is needed. The chapter explains:

- Quality aspects of a design from the different viewpoints of stakeholders groups;
- The nature and scope of the special functions, or "ilities";
- Reliability assessment methods;
- Safety in design;
- Upgrades;
- Configuration management;
- System evaluation and T&E planning.

## 9.1 What Is Quality?

### 9.1.1 Definitions of Quality

The standard dictionary definition of the quality concept is that it is about the degree of excellence. A standard on quality gives the definition that it is the "fitness for purpose of a product or service," that being expanded as a "set of primary functions or the work that a product or service is primarily designed to do, for which there is a stated or potential need."

Attitudes of the key groups of people to quality differ considerably and need reconciling throughout the design development.

Where practical the policies, laws, regulation, and judgment practices relating to the quality concept are made the objective by using defined models and parameters that allow a more quantitative practice to be applied. Quality of software systems is covered in [1]. General design is covered in [2, 3].

### 9.1.2 Technical and Esteem Aspects of Quality

Quality has two quite different aspects, both of which need simultaneous design attention in a system development. These are:

- Use functions to be met—the intentionally designed functional tasks (here about need, and not so much about want);
- Esteem functions to be met—the attractiveness and feelings of desire to have possession (here not about need, but want).

The balance of effort expended on these for a product of service varies. In many large engineering systems, the esteem aspect is not emphasized that much, whereas in products such as measuring instruments or vehicles, it will be a significant design issue.

Additionally to these main aspects, the system will also need to conform to any product/service policies in force, such as relevant safety regulations and legal liability issues (See Chapter 10).

### 9.1.3 Viewpoints on Quality

The various groups concerned with quality of the development system have already been identified in Chapter 6. Refer to Figure 6.1 to see their working relationships. Summarizing, they are the:

- Users and purchasers;
- Full system contractors and subcontractors;
- Original equipment manufacturers (OEM) manufacturers and vendors;
- Designers;
- The public.

The key interests of these groups are now summarized with respect to how each sees quality.

Users of technical systems are influenced by esteem aspects to some degree but essentially need sound suitability and low risk of nonoperation. Niceties and elegance of solutions are not of much interest to them. They are more concerned with using the system to do a job; they need to make it work, idiosyncrasies and all, and they may also need to maintain and service it. It is also often seen that they expect to get quality that is way beyond reasonable expectations.

Purchasers represent the user's interests but can be far removed from actual use. In this case, they can easily be sidetracked from truly representing the user's needs. They need to make critical choice decisions, too often that being done by intuition more than by objective argument. Their choice can be biased to use a "good name" product and by apparently impressive performance numbers. They may well seek, for lack of a full enough understanding, unrealistic performance for the money. This being the case, they will often select systems on the basis of least cost as their purchasing policy, and in doing so they then may be accepting poor quality.

Contractors supply the system, and therefore seek to turn in a profit as the result. They take major technical and financial risks with the performance provided being clearly in their court. They need to supply just enough performance for the money or there will be no profit for doing the work. Little incentive exists for them to deliver a better than just adequate system. For long-term survival in the marketplace, they need to supply a system that is up to scratch in order to maintain goodwill. Contractors will not easily disclose how well tasks are being done and are inclined to not report impending problems to the degree that the customer would like.

OEM manufacturers, and other subsystems and component vendors, need to sell their specialized equipment into projects to maintain long-term business survival. They also must deliver just enough quality as is needed by the contractor. Many design decisions are not in their control yet they must provide the definitive nuts and bolts equipment. They would like to be sole suppliers of unique products, so delivering quality matters a lot to them if it achieves some market edge. Like all producers, they seek to minimize their costs to produce. To save costs and maintain proprietary secrets, they are reluctant to give quality statements on parts provided unless paid to do so.

Designer's systems rarely work better than they were designed to be. They like to get things right early as rework is costly, tedious to do, and is seen as a failure on their part. However, they are often too impatient to attend to quality matters as well as needed. Quality support work, such as keeping records, following policies, and training can seem to be a waste of valuable time to them. They are, however, challenged by optimization needs that often are quality-raising contributions.

Joe Public's emotions often drive issues less than do engineering and scientific reality. Politicians and other public leaders get caught up adding political factors that impact quality significantly. Their understanding of quality is quite varied. They will too often overrule best-quality practice for reasons of political expediency.

### 9.1.4 Satisfying Multiple Viewpoints

The various viewpoints must all come together for system effectiveness to be achieved. The quality of the parts largely decides how long a system will remain effective. If any one of the suitability factors is not up to the required standard, the whole system may fail. For example, a submarine that runs out of breathing air at the wrong time is a failed system. A washing machine that fails due to corrosion of a part is a failed system if the lifetime is less than expected.

How the various elemental issues of quality parameters fit together is seen in Figure 9.1. Each pathway needs satisfactory quality to ensure that the whole is satisfactory.

In the recent past, many commercial and defense systems were purchased for a turnkey system price, usually the lowest that met the requirements. The operational costs were placed into other budgets. As technology and systems developments reduced the time to service and the systems became more complex, it became clear that the cost to use them over their life was very significant. Whole of life costing is now a much more normal practice. Some contracts are let for supply and operation, thus also placing the whole of life costs into the initial financial considerations. The cost of various ownership scenarios have been considered in Section 8.1.

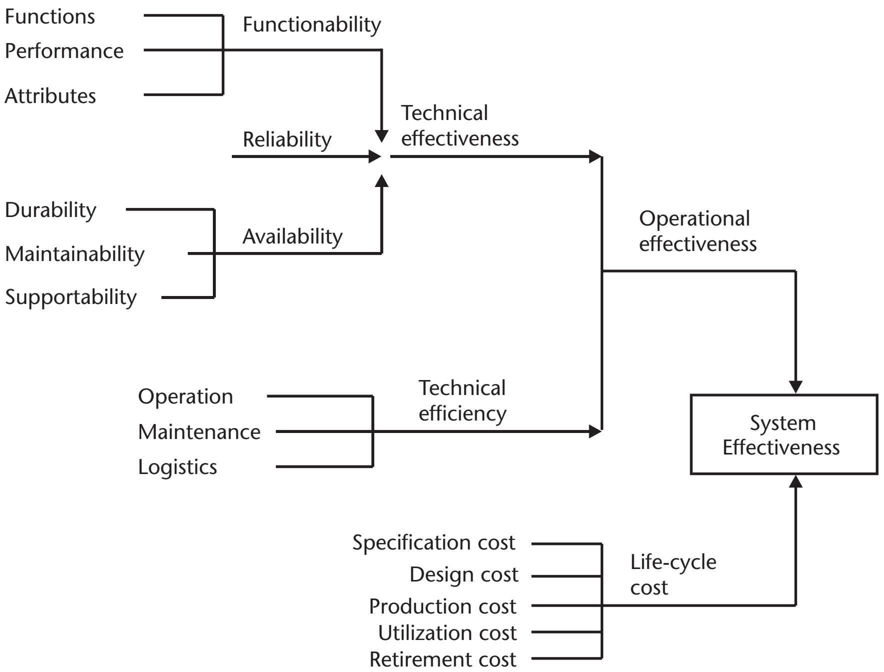


**Figure 9.1** Elements that form system effectiveness as a whole. (*Source:* Jezdmir Knezevic.)

## 9.2 The "ilities"

### 9.2.1 Why Systems Fail to be Effective

Numerous mechanisms can cause a system to not deliver effectiveness when called upon to do so. Their suitability for the given task has to be right. The following list gives an insight into the many facets that can deteriorate quality:

- Excessive working stress on components and assemblies, from internal and external sources.
- Small overload for long periods (incorrect design or use).
- Large overload for short periods (spikes, lightning, impacts).
- Overheating (from internal or external sources, fan failure, bad design, ventilation blocked by ignorance).
- Wearing out of parts.
- Mechanical wear (contacts, switches, bearings, connectors, slides).
- Chemical decomposition (electronic connections, silicon components, batteries, leads, corrosion).
- Vibration fatigue (small for long periods, large for short periods, unexpected vibration spectrum and duty cycle).
- Calibration expires, which is often not seen as a quality issue and is overlooked. Some equipment has a surprisingly short calibration interval. For instance, mechanical gyroscopes for submarine use have only a few days of

calibration life. Torque wrenches used to tighten nuclear reactor vessel top bolts need recalibration after a just a few pulls.

- Damage by human and other living creatures.
- Poor servicing practices (not done according to requirement, cheap materials).
- Deliberate maladjustment (sabotage).
- Unintentional maladjustment (by users in ignorance).
- Animals and insects (spiderwebs on optical elements; termites and animals like to eat cables; insects and animals fly into equipment).
- Interaction between parts.
- Corrosion, especially in conditions of wear, high temperature, moisture, and vibration.
- Heating of equipment attracts insects and animals.
- Poor human factors design.
- Handles and protrusions attract users to use them for foot holds, coffee cup holders, and coat hooks.
- Levers added to handles and switches that break them.
- Controls too small for ease of use.

The suitability of a system is a matter of the part it plays in a larger whole. Thus, the operational requirements play a large part in setting up reliability design for subsystems. These need to be teased out of requirements and other purposeful documents.

It is dangerous to rely on simply stated reliability requirement calls; these are often generated by people lacking sufficient understanding. They need to be verified before detail design starts.

Note that the term reliability is increasingly being used in the widespread sense of the overall system’s reliability and maintenance (R&M) regime; that is, doing the required task when called upon to do so. The term reliability is used also in a more specific sense for electronic assemblies.

As systems are made up of multiple millions of individual parts, their collective behavior can use Gaussian statistical methods with good effect. Electrical engineering was the first design regime to get the research attention that led to today’s excellence in reliability prediction.

Systems fail with characteristic lifetime forms. The so-called bathtub curve applies well for electronic equipment; see Figure 9.2(a).

Features about the burn-in region of Figure 9.2(a) are:

- Early life sees heating and chemical problems arise in the building nature of the electrical components, causing a certain amount of early failures.
- Extensive testing has proven that failures follow Gaussian laws of description.
- The electro-thermo-chemico nature of the basic semiconductor device has been shown to follow a strict mathematic relationship.
- Accelerated time testing of electronic components is thus possible by increasing the operating temperature of EE systems under test. This allows life

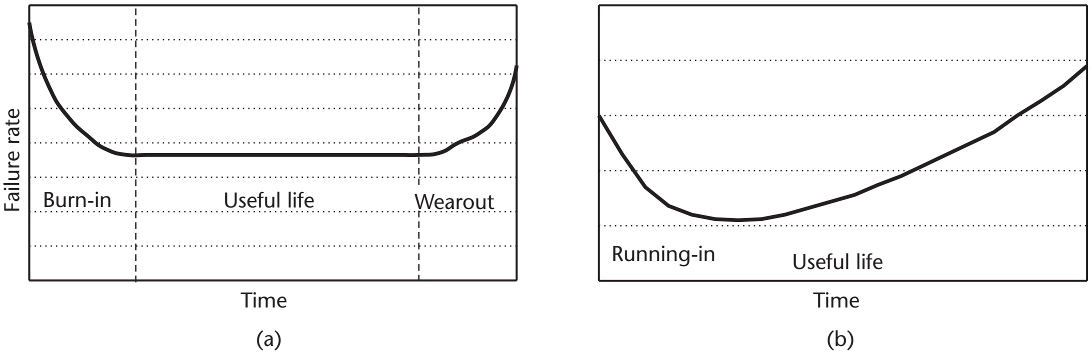


**Figure 9.2** Lifetime performance behavior in (a) electronic systems, and (b) mechanical systems.

prediction to be tested in a short time when component lives are in hundreds of years!

- Burn-in is used in the development of reliable systems to weed out a large proportion of failures. This is usually done at the parts, or subsystem levels. Often, however, this is left to the beta testing phase (i.e., when installed in the user domain)!

The lifetime performance curve typical for mechanical equipment is given in Figure 9.2(b). This is much more complex and problematic than for electronic parts and has to be handled on a component-type basis.

It may be necessary to carry out extensive life testing to establish the failure characteristics of parts. As lifetime values rise, it becomes increasingly difficult to get sound data due to the testing period needed being too long.

Suitability factors relate to ensuring the system is useable when needed and can perform its purposeful activity as called upon to do so. Purposefulness and suitability issues are often confused in high-level statements; they are not the same thing.

Suitability of a system is decided by many factors, including:

- Geographical location;
- Operational profile;
- Ambient temperature and other environmental parameter;
- Parameter cycling;
- Imposed and self-generated vibration;
- Shock, etc.

Transport, handling, and storage modes are sometimes critical to overall reliability. The actual conditions of operation in use are always of importance—helicopters in a desert recovery mission failed because during overheating, the engine fan filters were removed, letting sandstorm products into the turbines.

As systems become more complex and employ more parts, the probability that they are inoperable at any given time can increase to the extent that they are unable to perform their mission for a long enough time.

To a large extent, reliability is a characteristic of a design and can be improved by appropriate design strategies.

Reliability can be expressed as a probabilistic variable because failure is the collective result of the behavior of numerous, stochastically occurring, independent sources (see Figure 9.3).

### 9.2.2 List of "ilities" and Some Definitions

The many specialist engineering functions that together form the overall suitability are commonly called the "ilities." They are often interrelated; for example, "availability" is dependent upon "maintainability."

Some of these special functions are:

- Reliability;
- Availability;
- Maintainability;
- Interoperability;
- Compatibility;
- Logistics supportability;
- Transportability;
- Human engineering;
- Safety;
- Manpower supportability;
- Training;
- Electromagnetic compatibility;
- Parts engineering;
- Survivability/vulnerability;
- Integration;
- Contamination and corrosion;
- Value engineering;
- Diagnostics;

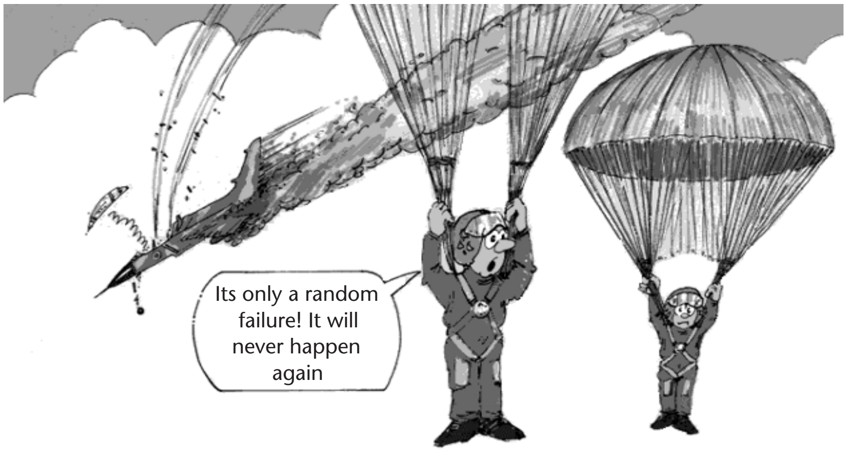


**Figure 9.3** Statistics describe the group behavior, not that of the individual. (*Courtesy:* Ian Knowles.)

- Power efficiency;
- Integrity.

Definitions of reliability abound:

- "Ability of an item to perform a required function under stated conditions for a specified period of time," Defence Standard 00-40 (NATO ARMP-1);
- "Duration of failure free performance under stated conditions,"MIL STD 785B;
- "Reliability may be defined as the probability that a system or product will accomplish its designated mission in a satisfactory manner for a given period of time when used under specified operating conditions,"Author's definition.

### 9.2.3 Maintainability and Availability

Most systems of some size will need to be maintained. Maintainability is the design characteristic that deals with the ease, accuracy, safety, and economy of maintenance functions. Maintenance strongly impacts availability, which in turn impacts overall suitability.

Maintainability is the ability of a product to be kept in effective service. Its must be traded-off against other design drivers such as performance and physical characteristics.

Maintenance constitutes a series of actions to restore or retain a product in an operational state. Best results here are the outcome of early design effort; it is harder to build this in late in the life cycle.

Two main kinds of maintenance approach can be used:

- Preventative maintenance (scheduled maintenance accomplished to retain a system at a specified level of performance by systematic inspection, detection, servicing, periodic replacements, e.g., automotive maintenance);
- Corrective maintenance (unscheduled maintenance undertaken, as a result of failure, to restore a system to a specified level of performance).

The time taken to repair or routinely maintain a system will depend on the maintenance time for each failed item; it will vary greatly. Maintenance can be a retrograde activity if not done well. Often the time to repair factor is absolutely vital, for instance the time it takes to get an electronic card replaced in a warship fire control system.

The time during which a system is not being maintained or repaired is called its availability. Availability is obviously a simple function of reliability and maintainability. It is measured in many ways:

- Inherent availability is the probability that a system, when used under stated conditions in an ideal support environment, will operate satisfactorily at any point in time as required;
- Achieved availability is similar to the above, but includes scheduled maintenance time.

Operational availability is the probability that a system, when used under stated conditions in an actual operational environment, will operate satisfactorily when called upon.

Because terms can have such subtle meanings at times we need to correctly interpret the ilities statements by referring to a definition of the term.

This brief account of special functions shows that their design is critical to success. Each has a considerable body of knowledge associated with it [4–7].

## 9.3 Types of Reliability Assessment

### 9.3.1 Overview of Reliability Theory and Its Application

Why is very high reliability needed from individual system components? As the number of components rises, it is to be expected that the overall reliability will fall. Space vehicle systems, for example, have so many individual items in them that making a system that will run for a five-year or more space mission would be impossible without great emphasis on their reliability performance. Individual systems components need to have a mean time to their first failure of many millions of hours of operation. They will never be called upon to operate for such long periods (there are only 8,760 hours in a year!); it is because failure arises according to the group statistical behavior that design needs such long periods of ensured operation from its components.

Because large sets of widely different sorts of components and numerous reasons exist for component failure, it is a reasonable assumption that all failures arise in a random manner. This leads to a main assumption that Gaussian statistics can be used to describe the distribution characteristics of system failure. This assumption is a good starting point, but needs expanding for sophisticated systems analyses. The theory of reliability assessment for electrical systems is well developed and disseminated, having been the subject of major R&D since the 1950s [4]. This has spread to use for systems in other design domains such as mechanical.

A good indication of the reliability of each block can be calculated relatively easily and that can then be used to determine if it is expected to be sufficient for the application.

Various publications, data services, and standards documents provide past consensus failure rate data for components and items—refer to [5, 6]. They assist users in building a reliability model of their system that provides a sound assessment of reliability performance.

Elements of reliability calculations are that the probability is usually stated in quantitative terms as a number (varying between 0 and 1, e.g., 0.995) specifying the number of trials in which one could expect a failure event to occur in a total number of trials. Reliability is usually quoted in failures per million hours, $\lambda$.

A reliability function is determined from the probability that a system or product will be successful for at least some specified time, $t$.

This reliability function $R(t)$, is defined as:

$$R(t) = 1 - F(t) \tag{9.1}$$

where $F(t)$ is the probability that the system will fail by time $t$.

If the random variable $t$ has a density function of $f(t)$, the expression for reliability is then:

$$R(t) = 1 - F(t) = \int^{\infty} f(t)dt \tag{9.2}$$

Assuming that the time to failure is described by an exponential distribution (from a constant failure rate with time assumption), then:

$$f(t) = \frac{1}{\theta} e^{-t/\theta} \tag{9.3}$$

where $\theta$ is the mean life and $t$ the period of interest.

The reliability of the component, or system as is shown later, at time $t$ is then given by:

$$R(t) = \int^{\infty} \frac{1}{\theta} e^{-t/\theta} dt = e^{-t/\theta} \tag{9.4}$$

where the mean life $\theta$ is the arithmetic mean of the lifetimes of all items considered, which for the exponential distribution is $M$, the mean time between failure (MTBF).

Thus

$$R(t) = e^{-t/M} = e^{-\lambda t} \tag{9.5}$$

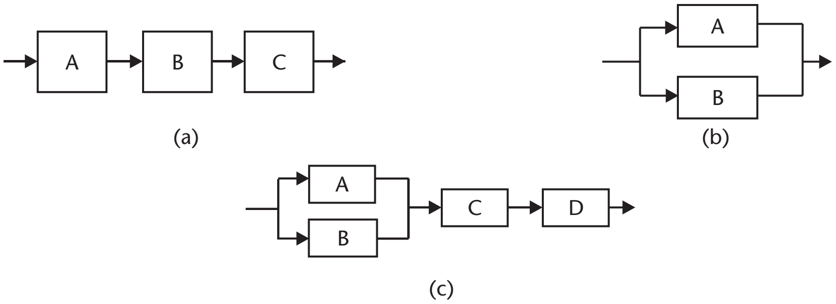
where $\lambda$ is the instantaneous failure rate. It is related to the mean life as $\lambda = 1/\theta$. Failure rate is also expressed as MTBF in millions of hours.

Equation (9.5) is a most commonly encountered reliability expression. It enables the reliability of systems of many components to be easily assessed.

Systems comprise sets of components so we need to know how to find the reliability of the whole set. It is relatively easy to calculate.

If all the components have to survive for the mission to be deemed successful, then the reliability model will be found to be a series network of component reliabilities as is given in Figure 9.4(a). Section 9.3.5 deals with other combinations.

The following calculation form then applies for the combined reliability $R$:



(a) (b)

(c)

**Figure 9.4** System component connection schema (a) series, (b) parallel, and (c) compound.

$$R = R_A R_B R_C \tag{9.6}$$

$R_{A,}$ $R_{B,}$ $R_{C,}$ are the respective component reliabilities. Note that as more components are added the overall reliability *R* can only fall. It is not possible in this kind of system to add a series component that will improve the situation. Individual components, however, can be chosen with a better reliability to raise the overall reliability.

Getting relevant data to use in reliability models can sometimes be quite difficult. It may be necessary to conduct in-house component testing of a specific component line.

Improving the reliability of a component almost always increases cost and its device description profile (DDP), for it will need to have an increased performance, larger mass, bigger size, and so forth.

To reduce overdesign creeping in, it is best to allocate reliability that is close to the normally available reliability of each component. The low-reliability components principally determine system reliability in series-type situations so it is not cost beneficial to waste resources improving the already high-reliability ones.

Published failure rates can be somewhat overrated. In the past, this has forced the use of overpriced parts to meet reliability targets. Better reliability understanding has resulted in more precise models and closer matches to a need.

It is necessary to consider that the simplistic assumptions made above are satisfactory when deriving the reliability model. For example, is the failure rate really constant for the situation at hand? Do the components to be used have the same failure rate characteristics as those given in databases?

Such considerations can soon lead to the need for experts to carry out the study, notwithstanding that the knowledge given here will go a long way in assisting a designer to attain a sound assessment of the level of reliability of a design and give pointers on how to increase it.

Despite its shortcomings, reliability analysis is a powerful and meaningful technique to:

- Aid trade-off studies;
- Identify reliability-critical items;
- Identify system design weakness;
- Design the reliability qualification test program;
- Provide input to the maintenance strategy.

### 9.3.2 Parts Count Method of Reliability Assessment

Many methods exist for assessing system reliability. The difference between them is the degree of the sophistication used, the effort needed to obtain requisite data and the precision obtained, and the uncertainty of the model produced. Some methods are now outlined in order of ascending improvement.

The parts count method is the simplest to apply—but the worst indicator! It is fine for making a crude, quick assessment. It is not used for serious assessments but does give a "finger in the wind" starting point for developing an understanding of the initially proposed system's strengths and weaknesses.

Its basis is:

- Count the number of components in the system;
- Multiply that number by an average failure rate figure for components;
- Convert that value to get the MTBF in millions of hours.

This is crude indeed, for it assumes all parts have the same failure rate and operate under the same conditions. This is obviously not the case in practice.

In the next-better procedure, the classed components count method, it is recognized that different component types will have different average failure rate figures. This is more realistic but takes a little more time and thought to apply. The process here is:

- The number of each class of component (not size value, but form) is counted;
- A table, by class, is set up (Table 9.1 is an example);
- The failure rate for each class is established from appropriate reliability data banks;
- The table is calculated through for each row;
- The total failure rate is summed—it is a series model situation;
- This is converted into MTBF and other indicators, such as numbers failing in a given time.

Taking this method further to a third procedure, we need to allow for the fact that each component in a class may not be operating at the same stress level. Varying stresses, for instance, arise in electronic systems due to differing voltages (that stress capacitance structures) and differing current levels (that give rise to self-heating of components) operating in each component.

This can be allowed for by adding a quality factor that effectively derates a component's reliability in the table. The example shown in Table 9.1 also has the quality factors added into the calculations.

The reliability quoted for a component is usually that for the component being made at the smallest cost for a reasonable lifetime. It will usually need to be derated to ensure it is not overdriven. For example, electronic resistors will run rather too warm to obtain best reliability if used at their declared nominal power rating.

### 9.3.3 Application-Based Method of Reliability Assessment

Some thought will soon reveal that the actual external conditions of use of the system, as well as its internal operating parameters, will significantly affect its reliability.

The MIL-HDBK-217 application-based method gives a detailed breakdown of the various aspects that will be found to be relevant to the overall failure rate $\lambda_I$, where

$$\lambda_I = \lambda_B \pi_E \pi_L \pi_Q \dots \pi_N \tag{9.7}$$

**Table 9.1** Example of the Classed Count Method of Reliability Assessment

| *Component* | *Qty* | *Base Failure Rate* | *Quality Factor* | *Failure Rate* |
|---|---|---|---|---|
| Printed circuit board | 1 | 6.1 | 1 | 6.1 |
| Thermistor | 1 | 0.026 | 10 | 0.26 |
| Resistor (discrete) | 10 | 0.08 | 10 | 0.8 |
| Resistor (trim) | 1 | 0.083 | 10 | 0.83 |
| Capacitor | 1 | 0.057 | 10 | 0.57 |
| Capacitor (electrolytic) | 1 | 0.0025 | 10 | 0.025 |
| DC/DC regulator | 1 | 0.066 | 1 | 0.066 |
| Connector | 2 | 0.23 | 1 | 0.23 |
| RS-422 encoder | 1 | 0.085 | 1 | 0.085 |
| Operational amplifier | 2 | 0.057 | 1 | 0.057 |
| Output driver | 1 | 0.057 | 1 | 0.057 |
| | | (Millions of hours) | Total failure rate: | 9.08 |

$\lambda_B$ is the base failure rate, which is also a function of temperature;
$\pi_E$ is the environmental adjustment factor;
$\pi_L$ is the learning factor for new products;
$\pi_Q$ is the quality factor relating to the degree of manufacturing control;
$\pi_N$ are additional adjustment factors.

How to interpret and use these factors to build a sophisticated model for a specific situation is explained in the Standard.

Some factors cannot be fully characterized by formal characteristic equation models. For example, reliability assessment for electronic systems used in land vehicles of various kinds defies strict formal mathematical description when the ground conditions are to be incorporated. However, rules of thumb (heuristics) can be used to decide appropriate quality factor derating values. For example (illustrative only; go to standards of relevance for the values to use):

- Bituminized motorway use 1;
- Back-country roads use 2;
- Cross-country four-wheel drive (FWD) use 4;
- Rough terrain FWD use 8;
- Harshest use, such as inside a battle tank, is 20.

Some factors are formed using quite complex relationships given in the Standard. These make use of formulae into which appropriate coefficients are inserted from tables and sets of heuristics.

### 9.3.4 Model-Based Reliability Assessment

Where a system is a major development, there is merit in building a detailed reliability model of the full system, incorporating elements of the methods given above in a more sophisticated manner.

Computer design support tool systems for electronic systems now routinely provide for reliability assessment as subsystems are developed using the tool system (see Section 11.5.2). Sophisticated libraries of component and failure rate data are provided for the user to tailor to their specific use. On-line access to reliability data is available.

### 9.3.5 Reliability Improvement

Improving reliability is largely a of matter design choice and the constraints of cost and component size limits. Raising the reliability will invariably increase costs in several ways:

- Cost to purchase better components;
- Design needs more time;
- Increased space is needed because more reliable components are usually larger;
- Better testing is needed to ascertain estimate with less uncertainty;
- More skill and care in assembly and maintenance needed, which takes time and better skilled staff.

Conflict arises between the design choices. Clearly, better made and tested parts will improve the design capability by lessening the probability of failure, but with increased cost penalties.

Given that a sound reliability design study has indicated there is need to improve the overall MTBF of the system, what can be done? Several options exist:

- Explore using newer data and better models! Component reliability data has increased in precision over the years. Data has to be conservative so low uncertainty of data values means lower reliability figures being used for components.
- Use components and technologies that have proven lower failure rates. Switching from discrete electronic components to integrated circuits makes a major improvement, as does the use of a better mounting technology.
- Using problematic components is courting disaster. New components will have only a short history, and therefore may not be adequately characterized.
- Lower the operating temperature. The failure rate of semiconductors doubles with each 10°C rise. This is well characterized by physical laws.
- Every extra individual component added (at least, in nonredundant systems—see below) reduces the overall reliability. Use higher levels of integration and a different design to reduce the parts count.
- Concentrate on improving units with low reliability that are in series paths.
- Apply component redundancy to the system design,as is now explained.

If two components are connected in parallel to do the same job, as in Figure 9.4(b), then the reliability of the system has been improved over a system having only one component path. This parallel connection then brings redundancy into the system.

Using parallel laws of connectivity, the overall reliability for two elements $R_A$, $R_B$, becomes:

$$R = R_A + R_B - R_A R_B \tag{9.8}$$

Given a system with $R_A$ and $R_B$, each having 0.95 reliability, the above calculation is applied to show that the combined system has a value improved from 0.95 for a nonredundant system to 0.9975.

$$\mathrm{R} = 0.95 + 0.95 - (0.95 \cdot 0.95) = 0.9975 \tag{9.9}$$

Using redundant systems have made space shots and safe aircraft travel possible.

In general, the total reliability model for a system will be a combination of both series and parallel connections. Figure 9.4(c) is a simple example of this. Its overall reliability calculation is:

$$\begin{aligned} R &= \left(1-(1-R_A)(1-R_B)\right)R_C R_D \\ &= \left(1-(1-0.95)(1-0.94)\right)\cdot 0.98 \cdot 0.999 \\ &= 0.9970 \cdot 0.9790 \\ &= 0.9761 \end{aligned} \tag{9.10}$$

It has been shown that the reliability aspect of design is critical to system success; yet it seems that many engineering design courses, including those in electrical engineering, give it little exposure.

Reliability control for a development can be a specialized design role; large projects will usually have specific work in place for this.

Without reliability studies in place in a project, there can be little guarantee that a system will be sufficiently effective. Many small team electronic designs are not sound because of a lack of interest in reliability assessment studies.

## 9.4 Reliability Acceptance Issues

### 9.4.1 Concept of Reliability Acceptance

It is possible to begin reliability analysis quite early in the development cycle. It should not be left to near the end point, for design changes will surely be needed to improve the reliability. Later improvement can be most costly. For example, if redundancy is essential there may not be the space or load-carrying capability to allow for the additional componentry without reducing other essential functions.

Physical reliability testing of whole units will not be possible until later stages are reached. It is, however, possible to carry out partial assessment studies early in the development. Early reliability assessments are for systemic guidance only; they help steer the design, giving assurance that it is heading in the right direction.

When computer modeling in computers is used as the main method for design, as in electronic development assistance CAD suites, then reliability and the associated thermal patterns of boards and ICs will be carried out largely automatically, once their data libraries are filled.

Once the physical system is available in a large enough form, after burn-in is used to clear early defects, and tests are run using statistical methods to design them. Test profiles used should be as close to reality as is reasonably predictable at the time.

When it is known that failure rate data will not be externally available, it might be necessary to set up special test rigs as early as possible; it takes time to get this type of data. As overall systems failure rates times can be in decades or years, special test techniques are needed to obtain accelerated failure rate data.

The statistical planning and interpretation for serious testing needs the skill of experts! Deeper discussions are available in [7–9].

## 9.5 Safety in Design

### 9.5.1 Safety as a Concept

A system that provides the required operational need and has an adequate level of suitability for a task can still be a poor one if it does not possess sufficient safety in use.

Safety of a system is another design area too often neglected in engineering training, the result being that many systems are not given the degree of consideration needed. Apart from the obvious life-threatening aspect, a lack of adequate safety can lead an organization into bankruptcy if litigation succeeds against it (see Chapter 10 for discussion of legal aspects of design).

Where does safety start in a design? Can it be added later? At what stage of the life cycle should it be addressed? The simple and categorical answer is "as soon as development commences." It is a design aspect that will only be fulfilled well enough if seen as a whole of development issue. It is a matter for all to take most seriously and not just leave for the person designated as responsible for it.

The organization as a whole has to take it seriously and develop a design climate that makes designers constantly conscious of safety.

The key issues of system safety are:

- Safety definition. What is safety, in a defined manner?
- Safety acceptance levels. What is acceptable safety, considering that absolute safety is not a reasonable expectation?
- Hazards, accidents, and causal factors.
- Organizational fundamentals.
- Management considerations.
- Standards of safety and safety assessment.
- Safety planning.

These issues are now addressed.

Safety as a concept has many interpretations:

- Totally zero rate of dangerous defects? (A nice idea, but impractical.)
- Absence of all danger? ("cotton wool" mentality).
- Acceptably unsafe? {This is the usual principle applied. Benefits outweigh the risks is a criterion. Different groups of people have different views on what this is. It is enshrined in most countrys' laws [e.g., U.K. law is the Health and Safety at Work (H&SW) Act 1974]}.

A large systems development organization will have policies and practices in place for its safety aspects of systems under development. Smaller organizations may not.

What is acceptable depends on whom you ask.

In the U.K., the as low as reasonably practicable (ALARP) principle is often applied.

In France will be found the globalement au moins aussi bon (GAMAB) principle that is based on a level of risk globally at least as good as the one offered by any equivalent existing system.

In Germany, they use the minimum endogenous mortality (MEM) principle, in which hazards introduced by the system should not significantly increase the mortality rate, due to technological facts, above the MEM.

In the United States, numerous safety principles are cast in law. For example, the threshold level value (TLV) used by U.S. Government Conference of Hygienists defines, "the airborne concentration of a material to which nearly all persons can be exposed day after day without adverse effects."

Note that all these statements are subjective—it is not possible to define safety by strictly formal means.

Joe Public has a very loud voice in this arena, but again with much subjectivity. The public perception of safety risk must be taken into account to suit the area of application.

For example, in rail travel the general public will tolerate many single fatality accidents much more readily than a single multiple fatality incident. Furthermore, the level of safety acceptable for road travel is way below that for air travel.

Electrical safety in the United States is covered by a standard that has matured over many years [10]. More general works on safety are in [11] and [12].

It also depends on whose safety is threatened; some groups are more tolerant than others, such as the Armed Forces, workers, civilians (e.g., commuters), and children.

It also depends on what type of system application the company design work is directed toward. If it is for electronic games equipment then it will not need the same level of attention as it does for parts of a submarine nuclear reactor. More detail is provided in [13] and [14]. Web sites exist where safety information and group activities are available [15, 16].

### 9.5.2 Determination of Level of Safety

Assessment needs a systematic procedure that results in comparative data. The process used must be well defined in documentation, auditable, and easily understood by users.

The process used will vary somewhat depending on which standard is mandated to be used. Figure 9.5 is an example of a defined process that leads to demonstration of safety on the ALARP basis [15].

Hazards, accidents, and causal factors are the main parameters of a safety assessment situation. For example, with respect to a computer used in an engine control system, there is need to categorize each of the following events:

- Failure of the control input signal transmitter to send the right signal;
- Loss of power supply to the drive motor that controls the engine throttle;
- Failure of throttle position algorithm in the computer;
- Incorrect positioning output being sent to motor;
- Engine over speed occurs resulting in engine parts bursting;

These are each categorized in terms of the:

- Causal factors that can be understood in terms of operation and studied for their likely effect on system safety (for example, wiring that is mounted too close to a significant heat source);
- Hazards that might exist that can lead to accidents (potential ingress of rain into a control box);
- Accidents that result from an unfavorable combination of the above.

There exist many statements on how to assess safety [15]. The designer's organization will usually indicate which is to be used. If not defined the team leader should not pick one arbitrarily, for the matter can be subject to the force of law.

The organization must:

- Identify safety responsibilities and put them in writing;
- Keep records of the transfer of safety responsibilities and must make sure that anyone taking on safety responsibilities understands and accepts them in writing;

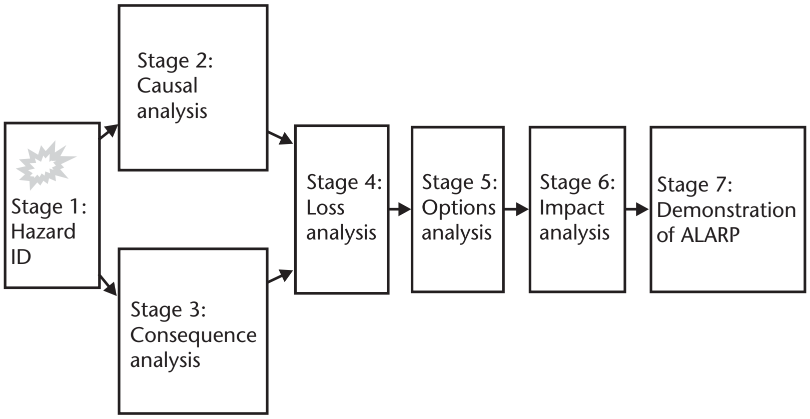


**Figure 9.5** Seven-stage process for system safety assessment. (*Courtesy:* Witchwood Engineering.)

- Ensure that all relevant and necessary information is transferred along with the responsibility for keeping an up-to-date hazard log and safety case.

A strong safety culture is needed throughout the organization. Safety must be a primary holistic goal. Safety must not be the only goal, for a system must be simultaneously safe and fit for purpose. Knowing when to stop requires skilled judgment. Stopping people using cars on roads will reduce traffic accidents but that level of utility is not acceptable!

How does an organization inculcate a sound safety attitude? It needs management commitment from the top that is backed up with solid and continuous action. A railway accident investigation reported that a concern for safety which is sincerely held and repeatedly expressed but, nevertheless, is not carried through into action, is as much protection from danger as no concern at all.

Training and resources are essential to make staff aware and work in step. Their safety awareness and skills need regular monitoring and constant improvement. All staff employed on safety-related tasks should be appropriately qualified and experienced. Safety-related standards set down criteria for defined safety roles.

Proven competence here means more than having a one-time paper qualification. Competencies should be regularly reviewed. Lessons learned should be fed back into the system.

Obtaining adequate safety in a development requires close cooperation with suppliers and subcontractors for their contributions must not compromise the level of safety needed. All tools and systems used to build and model the system under development need to be regarded with suspicion as to their internal operation. They may contain a serious safety defect waiting to emerge when certain deleterious combined circumstances arise.

Documentation and records will involve a:

- Safety plan;
- Safety requirements specification;
- Safety case;
- Hazard log;
- Design documentation;
- Validation (T&E) plans/results.

Several standards exist for engineering safety management; these include DEFSTAN 00-56, MIL-STD-882C/D, IEC 61508, and CENELEC EN50126.

A recently overhauled study gives a useful tutorial approach that is said to be easier to understand and apply than many of the safety standards used [15].

Safety planning needs to have traceability. What gets planned gets done, at least in some form. The safety plan provides detail of how safety risks will be reduced to an acceptable level. Questions to ask are:

- What are the main risks?
- How will we control them?
- How will we verify that they are controlled?

There is no need to produce a complete safety plan up front. However, set up the engineering safety management (ESM) for each activity before it gets too far along. Update the safety plan at the end of each stage. Keep improving the best practice as a matter of course.

### 9.5.3 The Safety Case

When a system has not been built and tried before, which is the situation for most new start projects, it is not yet possible to test that it is safe enough. In the past, the contractor or designer would claim it would be fine, providing limited audit evidence of their capability to assure this was so. This approach calls for much trust by the customer of the supplier's claims.

There is a trend now toward the preparation of a safety case. The contractor or design groups prepares and submits documentation that makes the case as to why their solution will be safe. This is based on many items including details of their safety management process, past cases and experiences, performance of safety case models, and more.

## 9.6 Upgrading a Design

### 9.6.1 Reasons for Upgrading

Time is the enemy of design stability. Given a sound design today, there will assuredly be need for redesign at some time before completion, or after its first version is placed into service. Chapter 12 takes up the matters arising from change.

Staying competitive, or responsive enough, to client needs requires the ability to carry out a redesign with rapidity. A sound base to work from is an existing well-documented design that gives a baseline of knowledge about the design detail, its lines of thinking, and basis for choices.

Reasons for change being needed in a design are many:

- Technology advances, allowing more functionality and capability to be built in;
- Spare parts disappear from the market;
- Customers need improved, or different, requirements;
- Increased reliability and safety are demanded;
- Efficiency of system operation is to be improved;
- Ecological issues demand less resource consumption and better ability for recycling obsolete system parts;
- Legal health and safety requirements change;
- Staff skills disappear;
- Smaller space and weight are needed.

Today, where time, cost, and performance are drivers, there is need for fast cycle time (FCT) reengineering. [9]. This needs rapid creation of effective leadership, multifunction teams, and people to be empowered; the core process will possibly need to be reengineered. This is achieved by setting up a systemic (and systematic) organization strategy, associated tools, and suitable metrics for tracking progress.

Goals of FCT are ongoing ability to identify, satisfy, and reward the meeting of goals in time. The activity needs to be consistent, reliable, and profitable. It is usually directed top-down, arising from greater goals than the design team's own initiatives. A suggested life-cycle process for FCT has been published [9].

This impacts original design; redesign is better done where sound design records exist for that first version.

## 9.7 Configuration Management and Other Records

### 9.7.1 Need for Configuration Control and Management

Systems are designed by many people, each making design decisions on regular basis. If they each were permitted to make whatever changes they wanted without overall control, the development would soon become chaotic to the extreme. Where design changes are customer driven there can be extra charges made for the work. Documentation is needed to track changes for these reasons [16, 17].

There often arises a need to make modifications to the system. For example, consider adding a radio communication system to an aircraft for a special mission. If this were added by an individual lacking adequate knowledge of the whole, it might lead to the aircraft seriously malfunctioning due to an unwanted EMI interaction.

Change situations are managed using records. This activity is known as configuration management (CM). This is needed in all stages of the SE life cycle, mainly in the acquisition and production periods but also after delivery. It is essential to support design of situations having:

- Long service life;
- Continuous development in place;
- Frequent modification;
- Safety critical nature;
- High demands on suitability and availability aspects.

If a full computer-based model of every aspect of the system existed, then it would be a matter of calling up the parts of the model to see what is involved and running simulations to see how the additional item would impact the whole.

Such detailed models are rarely available as they take vast resources to develop. Being more realistic, CM makes use of diagrammatic forms of systems representation that help the user to rapidly get a good feel for the situation. Sometimes the CM information base is held on paper but database tools also exist that are built for this task.

CM, in short, classifies the identifiable artefacts associated with the evolving system—documents, hardware, software, data, and models. This information is used to support engineering judgment of the impact of proposed changes. It aims to avoid costly mistakes of misspecification when changes are intended and to prevent unacceptable changes taking place.

### 9.7.2 Principles for Sound Configuration Management

A change control process is obviously essential. This is usually set up as part of the overall project management system. Figure 9.6 is a suggested change proposal management process.

CM process implementation begins with the design team carrying out all necessary documentation tasks. Dedicated duties needed, usually held as part of other posts, are:

- CM process author, who keeps the process up to date in organization manuals and databases;
- CM project engineer, who manages the technical aspects of the control system;
- CM librarian, who maintains the numerous forms of records;
- Configuration control board, the approval authority for submitted changes.

This activity is very labor intensive and imposes a large, but very necessary, overhead. It identifies items and allocates a unique code to each. It links items and interfaces.

Some applicable standards on CM include:

- MIL-STD-490A Specification Practices;

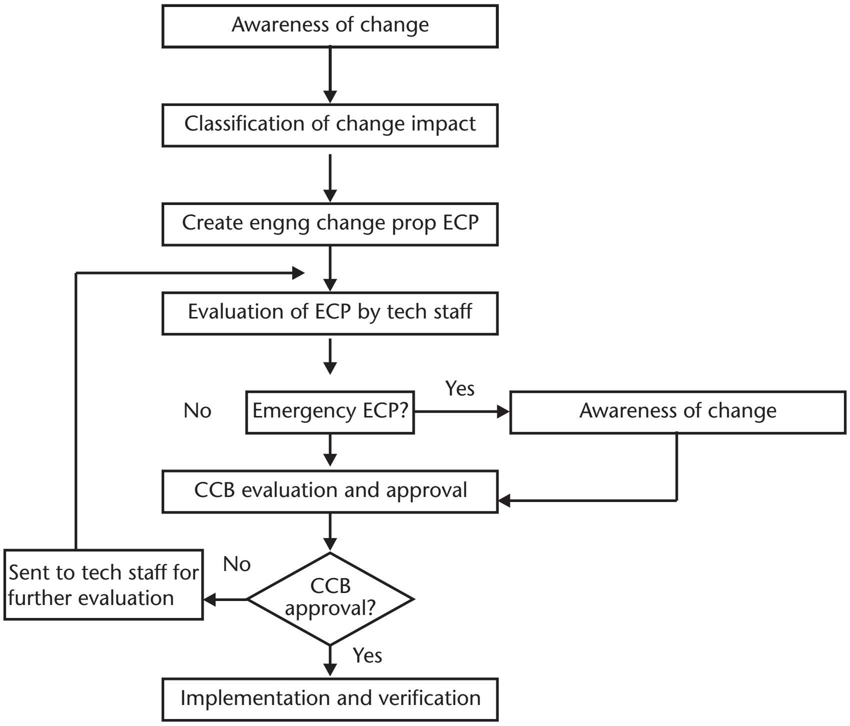


Figure 9.6 Suggested change of propsal management process [9].

- MIL-STD-498 Software Development and Documentation;
- MIL-STD-973 Configuration Management;
- ISO 9001 Quality Systems Models for Quality Assurance in Design, Development, Production, Installation, and Servicing;
- ISO 12207 Information Technology—Software Life-Cycle Processes.

Information is available on many Web sites about configuration management [17–21].

## 9.8 Designing for Disposal

### 9.8.1 Disposal Issues to be Addressed in Design

This chapter is on suitability and operability, so why is there inclusion of material on disposal?

Technical systems that are no longer needed are often simply left to rot. They may be scrapped and dumped if there is some force at play to make this happen.

Disposal, or phase-out, of systems and parts of systems is becoming more important with time. Automobiles, refineries, chemical plants, ships, buildings, white goods, household refuse, and so on are all now under varying levels of regulation covering their disposal practices.

If the system design does not foreshadow and allow for disposal, it can become an expensive issue. In some legislation, the cost of proper disposal is now legally placed back with the last owner of the system.

Here is a rather dramatic, yet simple, example. Lack of sufficient disposal control of a small, no longer needed, radioactive source used in a density measuring system led to the isotope source being scrapped inside its large lead safety container. Although it contained only a very small dose of radioactive material, it resulted in a metals recovery plant becoming expensively contaminated.

Some drivers to consider as original development is being undertaken are, with examples:

- Hazardous materials that exist in the system (isotopes);
- Legal requirements dictate certain actions (liquid wastes, heavy metals);
- Cost of disposal can be high (remote location, hazardous material such as asbestos, chemical wastes need incineration);
- Protection of proprietary information is needed (design secrets);
- Security of information is paramount and, perhaps, legally needed (personal information, company data);
- Process required is essential, but which is to be used? (How is disposal to be done?);
- Transition to its replacement needs planning and financing (reuse, refurbish);
- Records and documentation must be available (necessary information).

This topic is seldom covered in SE texts and it is not easy to find general texts on the subject. Most published texts on waste and disposal deal with hazardous waste, not technical equipment disposal.

## 9.9 System Evaluation

### 9.9.1 Evaluation to Customer Requirements

For a system to be satisfactory, all of the ilities need to be up to scratch. Overall system evaluation is needed to ensure the system will provide all-around performance to the customer's requirement.

As has been covered in Chapter 2, the overall test schedule for a subsystem should have been developed as part of the T&E master plan document, or its equivalent, that was compiled at the requirements extraction and management process.

The main drivers during the development engineering of systems (see Section 1.1.4) are cost, time, and performance (CTP). CTP risk reduction comes from:

- Saving time to design, service, or maintain service levels by timeliness and appropriateness of the right tests;
- Reducing program cost by exposing errors and preventing rework as early as possible;
- Reducing the likelihood of poor final technical performance in all feasible ways.

If sound systemic and systematic T&E has been applied throughout the development, then its outcomes should be tracking the customer's suitability and supportability requirements against predicted outcomes.

Testing is usually a distributed activity conducted by many different groups. It is not possible to test everything. Some parameters will be deemed to not need testing. Others will be assumed to be within specification through trust developed with suppliers and their certification processes.

Within the design team there will be issues that are tested by the team itself as part of their routine design development.

Then there are tests associated with the project's declared critical issues. These give indicators of how well the customer's requirements are being met.

Who should do the testing? This can be a contentious issue for this is a people-populated system that involves:

- Component suppliers (if they can be trusted and there is confidence in them);
- Subsystem suppliers (if they can be trusted and there is confidence in them);
- Prime contractors (they have different incentives to the designers);
- Procurement agents (they may not know enough and have the appropriate test facilities—enquire how);
- Customer's agents (can lack enough ownership of quality);
- Independent testers (they seek to be independent but may have other agendas).

When do we test? Each stage needs tests at the:

- Requirement definition stage (but what can really be tested then?);
- Component completion (who does it and to what test spec?);
- Integration stage (just who does this is complicated, for many aspects need representation);
- On delivery (both the customer and the contractor may feel the need to do tests but that duplicates work);
- In service (Setting up these tests is an expensive overhead);
- Throughout project life (what mechanism is used here?).

If there has been a sound holistic T&E process in place throughout the development, then many of these issues will have been addressed and decisions already made. If they have not, then all manner of disasters can arise. There was, for example, the case of a contractor asking for acceptance of some very expensive, specialized, RF amplifiers. When the customer went to test them it was realized that no adequate statement of requirement existed that detailed their use.

### 9.9.2 Test Planning and Execution

Testing must always have a clear aim and sound holistic plan to be effective and timely (see Sections 1.4 and 2.5).

The first step in preparing for testing itself begins with identification and grouping of the organic building block parts of the system under test (SUT). This should include checks of the need from the requirements documentation, the SEMP, from specifications provided to the design team, from the ConOps (Section 6.4), and from the TEMP. This will assist in ensuring that the information currently being used locally by the design team is truly consistent with now standing high-level requirements; they may have changed or the design may have drifted off-track.

Next, prepare an open system boundary limits diagram (see Figure 5.2) with all blocks and interfaces shown as discussed in Section 5.2.1. This should already be available but do check that it is still current. This is then converted into a closed system diagram by making decisions about suitable bounds for the test objective.

It is then time to set up charts for the test variables, ranges, and dynamics, and to subsequently select suitable test data points and decide on ranges needed in data loggers. This is also the time to select test processes. If testing is to be done manually, vary each input from its nominal value one at a time, recording the needed outputs. Alternatively, use may be made of automated test equipment (ATE) suites to speed up the process. These need programming work to be done upfront of the tests.

How data will be stored and processed needs to be addressed well before the test date. In order to be more certain that events are covered, that may be needed one day, testing often overdoes the data collection. In-flight aircraft testing has reached the situation where in excess of 200,000 active test points could be used. Typical test runs generate gigabytes of data per minute during a test flight.

A considerable amount of software systems can be tested without reference to the hardware it will support but it will eventually need to be integrated. To test them, many systems need addition of a DAS measuring system and creation of special test facilities. This can be a long and expensive exercise. For example, it took several years to fully instrument an existing aircraft for in-flight fatigue testing. Some 2,000 sensors had to be mounted on the wings and fuselage. They then had to be hard wired to a DAS unit placed in a gunnery bay.

Advanced T&E planning should have allowed for this kind of need, budgeting to create access to test items, test equipment, and manpower well ahead of time. It is, however, sometimes policy to not release resources early enough to build the facilities to be ready when needed.

Some testing tips may be of use:

- Testing is planned from the top down, but executed from the bottom up with test results being integrated to yield data in the critical issues.
- Book test facility and support resources well ahead and keep updating the booking.
- Plan for contingencies that can be foreshadowed. They may not arise but if they do, you will be covered.
- Need real tests at key times because models only represent certain aspects of the whole.
- Create test plans from a basis of sound experimental design to maximize use of resources.
- Decide the order of tests—vary one variable at a time; more can become confusing.
- Use simulations to investigate test expectations. Check the likelihood of there being unexpected nonlinearities and sensitivities to unwanted effects well before conducting the test.
- Run trial tests in appropriate test chambers to ready all concerned for the real test.
- Test small assemblies first and progressively assemble and test units until the top level is reached. Putting too many together at once makes it hard to find where defects exist.
- Use automation of tests and data reduction where possible, as it is more accurate and faster.

A difficulty to contend with is that there is often inadequate budget available at the time of tests. It may well have been planned for originally, but projects often run out of money as they near the end—the time when testing is most needed to assist final handover.

A suitable test schedule must be prepared that details each step indicating what equipment and settings are to be used. Don't stumble through a test letting it just happen; it may well be found later that critically needed test data was not observed.

A simple example test statement might be:

1.1 Stabilize the temperature chamber temperature at +35°C for at least one hour.
1.2 Record the voltages at FST test points TP1 through TP11.

1.3 Adjust the power supply voltage, measured at TP10, to read +27VDC + 0.01VDC.
1.4 Calculate the fluctuation sensitivity at each measurement point (TP1 through TP11) as the ratio of the voltage change, to the voltage recorded at a supply voltage of +28 VDC ± 0.01VDC, as a percentage.

Below is a simple checklist of test features for an electronic system (recall that such lists may be available as part of the organization's documentation):

- Power levels;
- Frequencies;
- Voltages and currents;
- Drifts;
- Gains;
- Stability;
- Linearity;
- Dynamic features;
- Assembly;
- Mounting;
- Service;
- Test points and additional circuits for calibration.

Once the test has been completed, the data is then verified and may need conversion into engineering units. A test report is prepared that documents the:

- Reference to documents that paint the background situation (defense reports tend to place this list up front, whereas others put them at the end, if it is there at all);
- Aims and objectives;
- Methodology of test;
- Data reduction method;
- Test facilities and equipment using serial numbers to identify specific items used;
- Verification process of test facilities, both before and after testing;
- Notes made during conduct of test;
- Results of tests, location of raw data and its form in reduced units;
- Notes of likely relevance (rogue readings, unexpected test conditions, power interruptions and the like, storms);
- Sign-off statement that shows the personnel involved and line of responsibility;
- Appendices.

The test results are evaluated by the appropriate people against the appropriate requirements statements.

Digital system testing is carried out using much the same process. As its basis is the binary electronic switch, testing is needed from that level upwards. ATE makes this fast and relatively easy to set up. Software test programs control the setting of states and ranging needed.

As complexity rises (i.e., the number of binary digital elements), the time taken to carry out the test becomes far too slow. For example, to fully test a PC processor chip would take 200 years at a 1,000-MHz rate. Special strategies are employed to facilitate such testing. This often uses up as much as 15% of the chip's real estate to build special cells inside it dedicated to testing without the need to bring out more connection points.

Testing needs to suit the size of product run. Books on testing tend to target mass production run sizes (10,000 upward) [8]. They detail:

- Automated testing stations;
- Purpose-built test tools under software control and processing;
- Sampling of items—discarding an accepted proportion at test, or by users;
- Speed of test being the essence—if fault cannot be found in 2 minutes, send it to scrap!
- Great care is taken in design to ensure low scrap rate—numbers involved can support the resource needed;
- Scale of activity can support very expensive test stations;
- Extensive prototype testing can be supported.

However, the testing of built-to-order systems only involves subsystems in relatively low numbers. In this situation, the small-scale volumes (100s–1,000s) cannot support the high level of design care and testing seen in mass-produced consumer products. This can easily lead to shoddy products having low reliability and difficult maintenance. Failed subsystems are often, rather then being scrapped, put to use with likely loss of reliability.

Defense systems can often be singled out as a special case. They need high availability and safety, long periods of storage, and hopefully the highest effectiveness. They are advanced in a technology when the design commenced but are often old, to very old, when they get into service. Only low volumes (10s–100s) of specific versions are needed. They will be used by relatively low-skilled users and maintainers and require maintenance and service in very tough environments that are at large distances from well-equipped repair depots.

Consequently, in defense system development, it is usual to have a large part of the overall project as investment in special test and training plant.

Compared with the testing of electronic assemblies for commercial systems, testing needed for defense systems can be quite different. For example, a decades-old ground-to-air missile system is supported by automatic system diagnosis equipment that carries out fault location down to the individual component level within its circuit boards. Having found the fault—multilayer circuit boards—their repair needs dental-style skills to drill down into layers to replace the faulty part. The layers and components are then rebuilt up by hand over the fault area.

Why do this costly work? The board design is at least 30 years old. To make a new board would require redesign using modern components and technology that could possibly cost around $100,000. It is cheaper and faster to repair the board.

## 9.10 Summary

The design of a system is about much more than making it perform the right job. It is also concerned with ensuring it will always work effectively when needed. That introduces many more design issues to be addressed. These largely concern the quality aspects of a design, in particular the special functions or "ilities" of which reliability is a dominant design thrust. The various methods of reliability assessment have been outlined, showing that it is complex specialized task. Several other, often overlooked, areas of design have been discussed, namely safety, upgrading a system, and making allowances for later disposal. More detail on testing systems and subsystems has been given.

## References

[1] Kasser, J., *Applying Total Quality Management to Systems Engineering*, Norwood, MA: Artech House, 1995.

[2] Park Sung, H., *Robust Design and Analysis for Quality Engineering*, New York: Kluwer Academic, 1996.

[3] Schlickman, J., *ISO 9001:2000 Quality Management System Design*, Norwood, MA: Artech House, 2003.

[4] MIL-HDBK-217, *Reliability Prediction of Electronic Equipment*, 1979, and MIL-STD-781C, *Reliability Design Qualification and Production Acceptance Tests*, 1977.

[5] O'Connor, P.D.T, *Practical Reliability Engineering*, Chichester, UK: Halsted Press, 2002.

[6] Pham Hoang, *Handbook of Reliability Engineering*, Heidelberg: Springer Verlag, 2003.

[7] Blanchard, S.B., and W. J. Fabrycky, *Systems Engineering and Analysis*, Upper Saddle River, NJ: Prentice-Hall International Inc., 1998.

[8] O'Connor, P.D.T., *Test Engineering*, Chichester, UK: Wiley 2001.

[9] Sage, A. G., and W. B. Rouse, (eds.), *Handbook of Systems Engineering and Management*, New York: Wiley, 1999.

[10] McPartland, J. F., and B. J. McPartland, *McGraw-Hill's National Electrical Code® Handbook*, New York: McGraw-Hill/TAB Electronics, 2002.

[11] Roland, H.E., and B. Moriarty, *System Safety Engineering and Management*, New York: Wiley-Interscience, 1990.

[12] Roughton, J. E., and M. J. Mercurio, *Developing an Effective Safety Culture: A Leadership Approach*, London: Butterworth-Heinemann, 2002.

[13] Brauer, R. L., *Safety and Health for Engineers*, New York: John Wiley, 1994.

[14] Hammer, W., *Product Safety Management and Engineering*, Des Plaines, IL: American Society of Safety Engineers, 1993.

[15] Railtrack, *Yellow Book*-3, Railtrack PLC, Euston Square, London, distributed by Praxis Critical Systems Ltd, 20 Manvers Street, Bath BA1 1PX, UK, 2000, http://www.yellowbook-rail.org.uk/site/resources/books.html.

[16] http://www.quality.org/config/cm-guide.html, the Safety Groups in United States.

[17] Jonassen Hass, A. M., *Configuration Management Principles and Practice*, Boston, MA: Addison Wesley Professional, 2002.

[18] Watts, F. B., *Engineering Documentation Control Handbook: Configuration Management for Industry*, Norwich, NY: William Andrew Publishing, LLC, 2000.

[19] www.icmhq.com Institute of Configuration Management, Scottsdale, AZ.

[20] www.cmcrossroads.com/bradapp/links/scm-links.html, Brad Appleton's links to CM Web sites.

[21] http://www.quality.org/config/cm-guide.html, resource guide to CM educational materials.

## CHAPTER 10

# Legal and Security Issues

Designers need to have an appreciation of the legal issues that they may encounter. Material presented here will not replace the need for the legal expertise; it is intended to point to matters to consider as a development proceeds. Covered are:

- Legal means for resolution of disputes;
- Common legal documents encountered;
- Regulations and approvals;
- Legal liability in relation to design;
- How to minimize the risks of legal action;
- Security of information and access to installations.

## 10.1 Impact of the Law on Design Outcomes

### 10.1.1 Legal Aspects

Some topics covered in this book are relevant to all stages of the SE life cycle. Legal issues are one such general area. It is placed toward the end of this book in the belief that, by now, the reader is more ready to address the topic than if it were placed earlier.

It is not usual to have material on this kind engineering design books, so why include it? Reasons are:

- A design may not be safe; this can result in litigation if a user is hurt or suffers a loss of some kind because of the system's existence.
- The design may not comply with lawful requirements and thus can end up attracting legal action against the supplier and its staff.
- The materials and processes used in the design may be not within lawful use.
- Design features may infringe other registered or patented designs.
- Details of your own invention may not be protected sufficiently to restrict its use by other prohibited parties.
- A contract covering the project will contain clauses that can lead to penalties.
- The designed system may be used within a legal process, such as an instrument used on forensic science, and thus need special design features.
- The designer may well be called one day to give account on his or her work, or have the role of an expert witness.

- Ethical considerations may apply that should not be breached.
- Security issues over access to privileged information will assuredly exist.

The common thing about all of these is that they can all too easily, and innocently, lead to such large levels of litigation costs and damages, or necessary rectification activities, that the organization can become insolvent through even a small project.

As it is impossible to be totally safe from legal problems, the wise thing to do is to manage the various risk situations as they arise, thereby minimizing potential difficulties.

It needs to be made clear that this account is not intended to, not can it, replace the services of appropriate legal specialists. Their services can be costly but can be kept low by being prepared at all times and seeing that design choices do not lead to legally disastrous situations. It is unsound practice to ignore legal issues until they arise in litigation.

As seen above, engineering designs can be subject to numerous legal requirements. At first, this may seem to be so worrying an aspect of design as to make an endeavor far too risky to entertain. Things come into balance once sufficient familiarity is developed to be able to know what kind of advice to seek, at the right time.

If the design team operates within a large organization, the legal aspects, at least some of them, will be managed by resident or retained lawyers. As lawyers are not usually an intimate part of daily design decisions, it is up the designer and team leader to be aware of issues that need to be addressed.

The smaller business organizations need to make a commitment to buying in strategic legal advice.

Law is practiced differently from county to country. Its normal processes are not considered here. It used to be that the applicable country for a legal claim was that of the origin of the design. As globalization sweeps through, it is to be expected that legal issues will increasingly become internationalized. For example, the publication of legally unlawful items on the Internet is now not only subject to the laws of the country of origin but to those of the country of application.

There was a time when government, especially when using defense equipment, did not need to adhere to many of the laws imposed on the civilians. That is changing. Today in the United States, for example, the creation of a new military test range required an assessment of its design and construction within some 150 different laws and regulations.

### 10.1.2 The Legal Practitioner in Engineering Development

Law is obviously a complex matter. It is no defense to be ignorant of its numerous tentacles, but it is pragmatically not possible to be fully conversant with all of the directives and processes involved. Experience in designs for specific applications will help ensure that something has not been overlooked.

As a simple guide, situations where reductionist-based arguments can be used are far less likely to lead to legal action than where subjective and problematic issues exist; they are formal in nature and thus have a common interpretation, leaving little room for different interpretations.

However, the bulk of living activity is informal and subjective and therefore is often open to different interpretations that can be driven by emotion and vested interest. Legal services are especially needed when designing equipment and systems for these kinds of projects.

Lawyers are educated and trained to set up arguments that are based on provable facts and logical arguments. The problem is that the difficult issues in which they will be called to assist are those where judgments will legitimately vary and the opinions of individuals may well be different.

Legal advice is used in an engineering development situation to:

- Assist people understand how the law works and effects their design decisions;
- Organize, monitor, and mentor the many routine legal practices required by law of an organization;
- Assist and develop protection of designs and intellectual property;
- Reduce the risk of legal difficulties arising later by avoiding contentious issues and keeping appropriate records;
- Represent one side of a dispute when things go wrong taking a defense or an action role.

The legal practitioner retained by an organization is there to protect the client's interests. As such, this means they may not be that interested in the individual employee's welfare.

A law firm is also a business and thus needs to cover its costs and turn in a profit for its senior partners. Lawyers can easily go further with their assistance than the client might consider as being sufficient.

Striking a balance between how far to go with legal advice to keep risk low enough is a tricky matter, for the issues involved are usually highly subjective. In many instances legal resolution, regardless of the process used, will lead to situations where one of the parties is clearly wronged by the other, but wise counsel indicates it is better to take the loss in the short term for longer-term justifications. In some cases, in the eyes of the client, legal processes do not result in outcomes desired; taking legal action needs sound advice, lest it be money and time badly spent.

Legal actions are expensive. To provide for them, professional indemnity and public liability insurance need to be considered and set up accordingly.

Large contracts commonly will often be in dispute somewhere within their structure. Teaming and other methods of mutually agreed cooperation are used to reduce the level of disputes.

### 10.1.3 Disagreement Resolution

Much of the legal work done for the organization is routine and internal. The right things done at the right time helps keep matters under control. However, disputes often arise with those controlling or trading with the development organization. A sophisticated set of procedures has evolved for settling disagreements.

The following three courses of action are those most used in conflict resolution.

#### 10.1.3.1 Moderation

At the bottom of the scale of the level of conflict between parties is to use a moderation process. Matters that are heading toward problems are discussed with an independently and mutually agreed person appointed to moderate the discussions.

The moderator has little real power to mandate a solution; he or she needs to be persuasive in an impartial manner.

The reconciliation process organized by the moderator assists the parties to see how they each might shift their standpoint to find a mutually acceptable situation.

This method can work well for early situations, for then either side has less to lose than if the matter is left hanging until later in the design cycle.

#### 10.1.3.2 Arbitration

Moderation may have shown up the problems, but the severity of feeling and emotion present has not led to conflict resolution by that path. The next kind of mechanism to use is arbitration, a process with some degree of mandatory ruling.

Here each side puts its case to a mutually agreed arbitrator who steers them to a solution—if one can be found in this climate of relative informality.

These situations can, however, lead to outcomes sometimes hard to accept for one or both of the parties in dispute. The arbitrator usually has some power to rule on the issue and mandate the outcome.

The legal authority of the arbitrator can range from a mutually appointed individual to a panel of national or international judges. If the situation is major, such as a national wage claim case by a union of staff, a factory environmental pollution situation, or family law problems, arbitrators are in session on an ongoing basis and may be appointed by force of national or international law.

Engineering contracts will often name the arbitrator to be used if it should become necessary. This person might be a solicitor, lawyer, professional engineer, or scientist. They should be expert in the subject and experienced in this form of dispute resolution.

There is a trend toward use of this method for the costs are less and decisions can often be made far faster than taking matters to the deepest type of litigation.

#### 10.1.3.3 Adversarial Resolution

The parties have met with the arbitrator who has been unable to get them to accept a suggested resolution. The two parties cannot be reconciled. Court action is threatened. One of the two appoints a lawyer and notifies the other that action is being taken. If that does not lead to an out-of-court settlement, the two representing lawyers continue taking the matter to court.

It seems to come as a surprise to those who have never been involved with legal dispute resolution, that legal practitioners in the Western tradition represent their client using predominantly the adversarial manner of confrontation.

Each side does not give an inch at the start, standing off from the opponent making strong threatening declarations of what will happen next if certain things are not done or accepted. The opponents can either come to a compromise in the solicitor's rooms or let the matter run its course into the courtroom—where the dispute goes on until the matter is resolved.

Resolution will often be reached out of court, either before or even during court proceedings. Strong reasons for this are:

- Costs to settle this way can be considerably less than a full court case where even winning parties may incur costs of some kind.
- Resolution can be faster than taking court action; matters can drag on for years.
- Confidential and personal details can be contained with greater confidence—a court action can become very public.

Litigation is mostly on the basis of one-on-one actions. An example might be where the system delivered does not meet the contractual requirements or is delivered late. In that case the customer takes action against the contractor. Conversely, the customer may not be prepared to pay for work contracted, so the reverse applies.

In most cases involving engineering projects the action is taken against the organization, not the senior executive or the individual designer. That situation is changing; senior executives and individuals now can end up in jail or be fined.

Bad decisions by CEOs and designers are not so easily litigated. There have been some cases of individual engineering designers being successfully prosecuted for bad professional work, so it does happen.

The norm is more for the person who carries the official responsible to be pursued. This could be the person that signs off work, starting at the team-leader level or higher. The organization's chief designer or engineer is often the person designated as the responsible party and thus can be charged with an offense.

The sheer size and financial capacity of the larger organization can often fend off small claimants' suits. Taking legal action against a large organization as an individual may well be won in the end, but the route to the winning post will almost always take many years and be very expensive and definitely psychologically wearing on the person involved. Later employment prospects may also be seriously damaged. Such a route should not be entered into lightly and upon emotion alone. It is often far more prudent to walk away from a situation trying to forget the situation and getting on with life.

There are, however, cases where the individual has a better fighting chance. The first is where there are public and other organizations that specialize in fighting the cases of individuals. Examples are human rights, employment, and equal opportunity commissions.

Law firms also give pro bono (for free) time assisting small claims courts and other mechanisms that seek to provide justice to the individual.

### 10.1.4 Group Actions

In comparatively recent times, the individual has acquired considerable legal clout via the so-called group action. This is where one or more law firms collectively represent a common case for a group of individuals ranging up to thousands.

Some group actions are well known, for they receive lots of media attention. Examples are the legal claims related to safer consumer goods; asbestos exposure compensation; aircraft accidents; and harm caused by medications and surgical implants.

The engineering organization may well see cases of defective operation due to defective design brought against it—there was a case of a series of defective television sets. Another instance was where a relatively young civil engineer was charged with loss of life after a railway embankment he had designed collapsed in heavy rain. His professional institution stepped to represent his interests, clearing him on the basis that it was his supervisor that was at fault.

Most engineering legal requirements for correction to products and systems are, however, likely to come from mandatory product recall situations backed by regulatory organizations (see Section 10.3).

Mass-produced products are likely to see the group type of action, for there many people individually become empowered. The same applies for technical systems that may pollute the environment.

### 10.1.5 Types of Legal Documents

In the course of engineering system development many legal documents are likely to be encountered. A marriage of two organizations involved in a project—customer/contactor, contractor to another contractor, and the like—will require contractual documentation.

There is no universal way to proceed. The sequence of events for development of contracts is now given as a guide.

A first meeting concerning business dealings will be relatively open and informal as both sides meet to consider a potential business relationship. At that meeting, or soon after, participants will sign some form of confidentiality agreement that allows and controls the flow of confidential information between them, and from them to third parties.

As the relationship moves closer to mutual activity, the next step is usually to prepare and sign a Letter of Agreement, Letter of Understanding, Agreement, Memorandum of Understanding (MOU), or Heads of Agreement—many terms are used. They are all similar in purpose in that they lay down the main heads of agreement that both parties agree to try to follow. These documents are not particularly legally binding for they do not contain sufficient detail for deep definition, nor are they given the same degree of legal consideration afforded to the contracts that come later. These short agreements are used to open doors and facilitate loose relationships that can blossom into the legal trading status. An example is an agreement to develop joint cooperation on research by members of a university R&D consortium, or an agreement between two organizations to explore a mutually beneficial opportunity.

As the cooperation develops, the documentation moves into the legally binding contractual level. These documents have the power of law behind them.

The usual method of document development is for a draft that is expressed in the technical manner to be written by the engineers or managers. A previous, similar, document is usually used as the model from which to work. The draft is given to both parties to consider.

The form of expression used by engineering practitioners is often not tight enough with respect to use of legally acceptable terms and forms of expression. Thus, it is usually necessary, and prudent, for legal advice to be applied to edit the draft into an acceptably legal form.

The draft is then seen by both sides for their lawyers and engineers to consider. It is not unusual for dozens of such rounds to be undertaken before both parties are prepared to sign. When all parties agree, the documents are formally signed and witnessed by the responsible officer of each organization. The construction of contract documents is a specialist area of law, so one should retain an expert with related and extensive experience.

When entering into protracted drafting, it pays to consider the likely use of the document. Engineering projects have a history of needing change once started so too much attention to detail at the start can be a waste of resources and valuable development time. It is often observed that the most salient speed limiting activity in the early project period is the pace of legal support.

When considering the risk elements for a contract situation, it must be remembered that there will also exist many other legal issues that constrain the design situation. It is easy to overlook those, for they may not be recorded in the contract documentation.

The engineer can expect to become involved with some of the following:

- Employment contracts;
- Employee nondisclosure agreement;
- Personal pension plans and the like;
- Termination agreements—in some cases these prevent a person from working in the same field for specified times ahead;
- Certificates of Approvals to hold and store sensitive defense and civilian documents;
- Contracts to deliver personal services, such as teaching;
- Publishing agreements with authors, contributors, and editors;
- Patent applications and registered design and trademarks.

## 10.2 Legal Drivers for Doing Best Practice Design

### 10.2.1 Risk of Legal Action

With many kinds of legal issues to be addressed, it is clear that not covering them properly might lead a project into costly litigation and severe loss of goodwill, reputation, and sales. This section deals with some particular areas that can need attention as part of routine operations.

At the international level the United Nations operates numerous agencies that maintain a vast range of services and regulations. Topics covered by the United Nations—which are so often heard in news reports—include:

- Atomic energy: IAEA;
- Labor: ILO;
- Food and agriculture: FAO;
- Education, science, and culture: UNESCO;
- Health: WHO;

- Development: IMF;
- Reconstruction and development: IDA;
- Finance: IFC;
- Monetary matters: IMF;
- Civil aviation: ICAO;
- Industrial development: IDA;
- Postal services: UPU;
- Telecommunications: ITU;
- Meteorology: WMO;
- Intellectual property: WIPO;
- Agricultural development: AFAD;
- Tariffs and trade: GATT.

### 10.2.2 Environmental Regulations

Environmental regulations vary from country to country; many are in force internationally. The appropriate laws generate critical issues that must be identified and met; see Section 2.5.2.

For example, automobiles need to satisfy the regulatory needs of the countries to which models are exported; countries often require an imported vehicle to be tested and certified by local test engineers. Once approved, a plate is affixed to the vehicle to that effect. A passenger lift system manufactured for one country may need significant design changes for another. Electronic goods require EMI standards to be met, and so on.

If the system operates routinely across several countries, such as do aircraft, it can be expected that international regulations will apply—but not necessarily uniformly. Local regulations may apply in tandem with the international ones.

Environmental regulations and enabling acts cover such issues as polluting chemicals, particulates, acoustic and EMI emissions, material consumed in industrial operations, energy efficiency, labeling, power cords, disposal at the end of its life, and many more.

In all cases it is desirable that the standards for such needs be couched in easily determined measurable terms. This is fine where objective measurement is universally accepted, acoustic sound levels being an example. Others are far from amenable and such words as "shall not be deleterious" or "shall be clean" make for interesting legal debate by lawyers at the client's expense. In some cases overspecification cases seem to be absurd—an EU dictate on the degree of bend of bananas comes to mind.

### 10.2.3 Health and Safety (H&S) Regulations

These relate to personnel health and safety issues in the workplace and for the equipment used in it. They are specific to countries but can also have an international component. For example, the use of a computer display and a keyboard requires additional operator support equipments to be provided, such as stands to get the viewing height correct and ergonomically designed seating. Another example is seen in the manufacture of printed circuit boards; these must not use certain chemicals in etching resists for health safety reasons. Specified ventilation is also now needed.

As well as controlling the materials used and environment, the regulations require an auditable process for maintaining a safe working environment. This usually requires the creation of H&S committees that organize regular meetings and inspections of the workplace. Large organizations will provide training and support for these functions and appoint officials to pace the system along. There must be a paper trail in place that sufficiently supports the case that H&S requirements are being met.

A trap for the unaware is to call up use of imported equipment that, while it conforms to an approved set of rules elsewhere, does not conform to local ones. Examples in the electrical regime are the method of Earth protection; cable colors; and the method of isolating the electrical mains supply from the power supply—some systems still have potentially lethal autotransformer methods instead of using separately isolated windings.

Once in use in workplaces, electrical safety checks of all appliances are mandatory at set periods. The system under design needs to facilitate such certification processes.

Some H&S issues can be a source of ongoing disagreement. For example, whereas there are many who feel there is no safe dose of radiation from a cell phone, the legal requirement is what should be met in their use in a design.

### 10.2.4 Product and Type Approvals

Local and national authorities will often require a new model of equipment offered for sale to be approved against their standard. Testing of every item individually, to the breadth and depth needed, is not feasible, so tests are made of representative example of the type or class; hence, one name is used: type approval. Such approvals may be needed for one-off systems or parts thereof.

Domestic appliances are examples of equipment needing to conform to local state, county, or national rulings. Regulations can also be localized.

Factors involved in products that may be subject to type approval. Some examples are:

- Energy consumption and energy use efficiency (electrical, gas, and carbon fuels);
- Water consumption (washing machines and dishwashers);
- Heat loss or transfer (insulating materials and enclosures such as refrigators);
- Construction timber and fabricated metal sections;
- Paints and finishes.

These requirements often mean prototypes of equipment must undergo extensive approval testing to establish their performance. This adds considerably to system development costs and to the time to deliver. Engineering design methods are steadily reducing these penalties by using such processes as pretesting certification based on the use of computer models and partially made systems.

### 10.2.5 Other Legal Drivers

As if the above issues were not enough with which to contend, still more exist of less well-known origins. Examples of these are:

- Product performance claims;
- Advertising statements, written and spoken;
- Media and entertainment censorship and classification;
- Safety belts for automobiles and rigging use;
- Footpaths and safety rails;
- Footpath surfaces.

The list is endless. Perhaps it is the overwhelming number that often deters adequate consideration by designers. Equipment sent for testing in independent test laboratories often needs rework because their design has not adequately addressed the necessary legal requirements.

## 10.3 Legal Liability

### 10.3.1 Nature of Legal Liability

A common basis for ensuring people's rights are protected with respect to use of products and systems is the principle of legal liability. A legal liability action (lawsuit) can be taken against the organization, CEO, or perhaps even the designer. Just what constitutes legal liability depends on the circumstance, the local situation, and the country in which it is being taken.

In the United States liability is determined as the adequacy of the provider's delivery of care based on the custom of other instances of like kind. If it is normal practice in a system used for a similar purpose not to, say, use an alarm for overheating, then there is a chance the new design lacking that safety feature will be judged as providing reasonable level of care.

Such problematic situations need lawyers to interpret matters on a case-by-case basis. Systems developments are rarely close reruns of past ones; the circumstances and applications change and so do their legal issues.

The use of precedent cases as the baseline for determination does not encourage fast enough adoption of the latest safety ideas. For this reason a case may also be judged on the level of "reasonable prudence" shown. In the example above, this line of reasoning would expect a safety alarm to be fitted as it is reasonable to do so.

Three issues relevant here are that the required updated technology must:

- Be available;
- Not cause more harm by its use;

- Be able to be used at a reasonable cost.

Some useful texts that give more information on legal liability are [1–3].

### 10.3.2 Case Studies of Legal Liability Claims in Products

An example illustrating the various points of liability is seen in the general practitioner doctor's need for equipment to support initial diagnosis [4]. In the surgery the use of a stethoscope is expected as it is readily available, causes no harm, and is reasonable in cost. The doctor is, at the other extreme, not expected to have a whole body scanner available or indeed to use it at that stage of the consultation, for it is not readily available, might do some harm, and is unreasonably costly. The scanner is used by being referred by the doctor. It is then the patient who makes the final decision for it to be used.

This means that the designer of technical equipment has to be aware of what is available and to put it to use; if not, and litigation results, the case is not easily defended. Using old technology and techniques in a design might attract litigation.

The often-applied Law of Torts requires the responsibility, and thus the division of damages, to be proven for all liable parties involved. Proving who is liable can be difficult. As an example, a large air blower used in a mineral slurry treatment failed when it overheated and its rotors seized. A cheap temperature sensor had been fitted as part of the delivered system and it had failed to operate to cut off the drive motor as the temperature rose.

Investigation by an independent consultant showed the sensor was of an inexpensive type. It had been individually certified but was not used to current best practice. It was, however, of the type used by other suppliers of similar blowers. It was also established that the particular temperature-sensing unit used was not provided as it was originally supplied by its maker but was a marriage of two parts that had not been recertified as the new whole. Just who was liable probably kept lawyers busy for some time!

Another example that illustrates liability in engineering systems was use of an automatic cement-weighing unit to batch the concrete mixes poured into a multistory building construction. After the necessary several-day test period needed for concrete samples, by which time the building was up the to ninth floor, it was found that the concrete poured into a lower floor column was way under strength. It had to be taken out and replaced.

An insurance claim led to a legal suit. Just who was liable was not easy to establish. The weighing system itself was impounded and checked over by an independent expert. It was found to be operating as expected, was within calibration, and did not appear to have been tampered with, or damaged. There were no seals on its calibration adjustments and the system had a log recording that it had been calibrated by an external approved agency that signed it off simply having been recalibrated on the date shown. A weakness was found in the practice of the calibration agency process, for they had no clear calibration process statement and, thus, despite signing off a recalibration, could not demonstrate what that entailed.

Who was at fault was probably never decided, but the calibration company had left themselves wide open to a claim by not sealing the calibration controls and lacking proof of what was actually done in a calibration.

To assist appreciation of the issues at stake in legal liability situations two, more detailed, cases studies are now provided that are based in real cases. They involve technical plant and equipment where engineering design is part of the legal liability situation.

#### 10.3.2.1 Technical System Failure at a Fairground

Consider an octopus ride in a county fair. It has several small pods with seats for two people; each pod revolves, turns about axis, and as it does that, the pods rise and fall as the whole structure rotates.

During motion, the gate opened on one of the pods, throwing two of the three people in it into the central structure. One died, and the other was seriously injured.

The system was impounded and an engineering investigator was called in to investigate what had taken place. The investigator loaded three bags of wheat into the pod to simulate the people. The ride was run. At much the same time and place as for the original accident, the gate of the pod opened throwing out two of the bags.

It was then established that several key technical issues were of importance:

- The ride was licensed to carry only two people in a pod (but three were in it, presumably to increase income).
- Under the centrifugal forces involved, the pod deformed with the simple slide-fastening bolt moving out of its clip to release the safety gate.
- The speed governor on the turning rate controller of the ride had been disconnected (perhaps to increase the number of rides per hour) and it was running over its intended speed.
- The manufacturer of the ride had earlier recognized that the gate bolt mechanism did not have a reasonable sufficient margin of safety and had issued instructions to replace the fasteners with a better design, for which the parts needed had been supplied free of charge for fitting by the ride owner. They were found near the ride.
- Before the fair had opened for business, a local authority representative had inspected the ride and declared it safe (despite the improved fasteners not having been fitted).

Liability can be investigated from four directions:

- *User:* Riders in the pod might have tampered with the bolt or undid it when in motion. This seemed not to be the case, for the locking mechanism holding the bolt in place was still set. The shaft of the bolt had moved linearly out of its opposite holder.
- *Operator:* This person running it was hired locally and in all probability had been given last-minute instructions on how to operate the ride. He also probably did appreciate that it was going faster than normal, for he had been instructed to keep the speed constant at the ordered speed. The operator had

also been instructed to accept three people per pod when the license strictly prohibited it. There were notices on each pod as to the number it could take. So did he know it was risking lives and not take action? This person was under orders. He was almost certainly not a structural engineer and therefore may not have sensed it was unsafe to use as instructed.

- *Owner:* Here would seem to lie the main liability. This person had not replaced the fasteners. The ride had also been set up to run faster; as centrifugal forces are proportionate to the square of the rotation rate, this was certainly not a wise thing to do. Instructions had been given to the operator by this person. He was also legally the owner and, therefore, highly likely to be the legally responsible person.
- *Local authority:* They had inspected the system as required by law and may not have picked up the fact that the equipment had been tampered with to increase the speed. This issue would have been resolved if the test certificate had a detailed check plan for the key safety items listed that had been commented upon by the inspector. On the other hand, it could have been that owner put it right for the inspection, reversing the changes after that. The use of seals on strategic places would have shown if this were so.

Given the above mix of facts, it is not hard to see that it is difficult to show where liability should be placed.

In the final event both the owner and the local authority were held liable to differing proportions. The operator was cleared of blame. Compensation was eventually paid to the aggrieved parties.

#### 10.3.2.2 Truck Drive Shaft Fatality

In this tragic accident a large Earth-moving truck was involved. It had a rotating shaft coupling the engine to a centrally mounted transmission box. Drive shafts in a conventional truck only rotate if the truck is moving. In this design, however, the engine unusually runs at all times to provide power to the hydraulic transmission. When the truck is stationary and the engine is running, the shaft will be turning.

A mechanic was working under the truck. Despite the notice warnings not to do so, he had removed the safety cover over the rotating shaft while the engine was on. His overalls got caught up with the shaft and he died from injuries sustained.

The key engineering issues established were:

- The design was recognized as unusual so the manufacturer had provided a safety guard over the shaft and placed several warning notices stating that the shaft can be rotating even when the truck is stationary.
- The safety cover was firmly bolted on but was not interlocked to shut the engine down if it was removed.
- The mechanic had undergone recommended servicing training for the truck but his employer had not recorded this, or the fact that safety considerations had been covered in the training.

So who was to carry the liability? Not so clear, is it?

The mechanic knew about the need to observe safety rules but had ignored them, so seems to be the only liable party.

His employer, however, could not prove the mechanic had been given instructions, so he was possibly open to a proportion of the blame, for he could not prove the mechanic did know of the consequences of what he did.

The maker perhaps should have anticipated this might happen—people will be people! For a small reasonable cost, it would have been easy to have provided a freely available electrical cutout on the engine when the cover is removed, so the maker was also likely to be seen as liable. Adding this safety switch would not have reduced the safety of the system.

The operator, manufacturer, and the owner were all found liable to a differing extent.

The legal processes used in settling legal liability cases are far from perfect, for much of it is usually subjective and lacking precise definition where it is most needed.

Difficulties that can be experienced are further discussed in [5], compulsory reading to gain insight into how the law profession works.

### 10.3.3 Preparations for Legal Liability Defense

The above examples show how legal liability will affect all concerned if a design causes harm in some way in its normal or abused use.

Designers need to be able to defend any design as being reasonable and that duty of care has been practiced. Some indicators on how to limit that risk as design proceeds are now presented. It would be ideal to have a lawyer in the design team to give advice on every decision made. This would seriously limit progress and almost certainly end up being noncompetitive. Instead, the designers must exercise judgment and make use of regular legal reviews.

The main line of defense will usually be the ability to demonstrate "sufficient duty of care" or that "due diligence has been practiced." Where a situation cannot be formally described in complete reductionist terms—most of those that give rise to litigation—the case will be argued on the basis of "reasonableness," a highly subjective cognitive concept.

Preparation for legal defense starts when the project commences.

Following normal reasonable design and keeping a suitable document trail are absolutely necessary. Without these it would be difficult to provide the evidence needed that will survive in, and support, the legal process. If adequate records are not made at the time, it may well be impossible to later find the documented evidence needed. This need will impose additional overhead on a project and record information that may never be called upon. Taking such precautions is, however, like taking out an insurance policy; one hopes it is never needed, but it is a comforting thing to have in place when it is.

The design team is not expected to provide for every possible circumstance in a design, as that would stymie creation and cost-effectiveness. Allowance has to be made for all situations that can reasonably be expected to arise.

For example, consider an automobile door design. It is reasonable for it to stay secure in normal operation and also under quite severe impacts. It can be argued that it is not reasonable to expect it to stay held shut if the car, regardless of the severity of impact in an accident as the body then deforms. If, however, the catch can easily be designed to hold fast under virtually all loadings, then that design feature is needed—which is the case for modern automobiles that use a catch closing over a loop, not a simple bolt sliding into a hole.

Key points of the defense against a legal liability suit are:

- Description of, and adherence to, a formalized design process by project personnel;
- Peer design review and approval of project design information and documentation—Section 8.6;
- Management of system safety by a formally constituted safety board with a sound and documented safety and design change process—Section 9.5;
- Reference and adherence to standards and regulatory requirements for the appropriate aspects of the design;
- Appropriate training for designers, with records of attendance and achievement in learning;
- Findings of independent quality audits conducted during the execution of project activities that confirm adequate duty of care has been exercised;
- Availability of the above evidence that is framed to suit legal requirements;
- Maintenance of records of appropriate calibrations and certifications—Section 9.7;
- Availability of information to show current practice used in similar designs—Section 12.1.1.

Table 10.1, modified from [6], provides a summary of points to be addressed when presenting information.

Just how far these various issues are each addressed will depend on the following factors:

- Nature of the project (such as defense, government, sea, air, land, utilities, commercial, personal, health, and so forth);
- Kind of system delivered (benign, hazardous, domestic, and factory);
- Environmental impact, guidance being found in the environment impact statement for the project, if one exists;
- Locality and extent of application (office, city, country, or international);
- Level of perceived public acceptance (automobile safety versus aircraft safety, natural environment, or low public interest);
- Lifetime of system use (days to decades);
- Business issues (profits made and risks to be accepted);
- Collective power for creation of a group legal action.

Clearly, legal advice is crucial when setting up appropriate processes that can be expected to avoid or well defend any legal case should it arise.

**Table 10.1** Summary of Legal Liability Defense Actions

| *Aspect* | *Defense Summary* |
|---|---|
| Design process | Design process statement described in project Systems Engineering Management Plan (SEMP).<br>Review records showing that project personnel have read and understand the process to be used for project design.<br>Evidence that the SEMP, as a contract deliverable, has been reviewed and approved by the customer, and that payment has been received by the company in return as that closes the agreement.<br>Evidence, in the form of test reports, that indicates the scope of testing conducted on preproduction and production items.<br>Evidence, in the form of Certificates of Conformance, pertaining to the quality of used materials and the material supplier. |
| Design review and approval | Evidence, in the form of documents and design review records that demonstrates how the work has been executed and that design information has been reviewed by peers within the project team.<br>Evidence that documents that design information has been independently reviewed and approved by personnel delegated with such responsibility by the appropriate senior executive—such as the Chief Engineer.<br>Minutes and actions records from the major project design reviews (System Requirements Review (SRR), System Design Review (SDR), Preliminary Design Review (PDR), Critical Design Review (CDR) and Test Readiness Review (TRR)) and the like, attended by customer representatives. Emphasis is given to the point here that the customer has been exposed to the design of the project from its earliest stages, and that necessary action has been taken to address queries raised during these reviews. |
| System safety | Project System Safety Plan, as the document describing how aspects of safety will be handled throughout the project.<br>Identify the project System Safety engineers/representatives, describing their lines of reporting, duties and responsibilities.<br>Project Failure Modes, Effects and Criticality Analysis (FMECA) report (or for other applicable safety methodologies used) which describes the failure modes considered for the system, their assessed criticality and likelihood, and actions taken, in particular those incorporated into the design to mitigate these failures.<br>Review examples of actual designs (drawings, schematics) illustrating the incorporation of safety features and how these relate to requirements defined in the project System/Subsystem Specification (SSS).<br>Records that test and support equipment used during the development and acceptance of the project deliverables that have been calibrated within durations, and to procedures, defined by appropriate certified test agencies. |
| Standards and regulations | Identify the Standards and regulatory documents referenced in the SSS and the Terms and Conditions of the contract.<br>Evidence that the SSS, as a contract deliverable, has been reviewed and approved by the customer, and that payment has been received by the company in return. The emphasis here being that the customer has agreed to the set of requirements for the system as described in the SSS, which reflect the intended need and usage of the system in-service.<br>This set of requirements reasonably includes all necessary references to Standards and Regulatory documents applicable to the domain or locality of operation—many localities have international implications.<br>Summary statement of how requirements have been managed on the project. In particular, show how requirements in Standards and Regulatory documents have been flowed down to applicable areas of the whole project design. |

**Table 10.1** (continued)

| | |
|---|---|
| Training | Records pertaining to training of project personnel in the knowledge and execution of the design processes employed.<br>Summary of the operation and maintenance training program developed by the company, for presentation to the customer.<br>Evidence that the Project Operator and Maintenance Manuals, as contract deliverables, have been reviewed and approved by the customer, and payment has been received by the company in return. The emphasis here is that the customer has assessed these manuals to be adequate for their intended purpose, namely the training of user personnel in the operation and maintenance of the delivered system.<br>Outline summary of procedures associated with the operation, maintenance and calibration of the system. |
| Independent audit | Audit of adherence to design process via personal interview of project engineering staff to ascertain their understanding of the process, and the tabling of evidence that the steps in the process have been followed.<br>Identification of where the project design process is documented, and how accessible information explaining the process is to personnel.<br>Audit of test records for completeness.<br>Audit of Certificates of Conformance for project materials and components.<br>Audit of quality audit reports compiled by the company for its material and component suppliers.<br>Audit of document and design review records to establish the completeness of the records, that only personnel with the authority to review and approve such information have done so, and that actions arising from external customer reviews (SRR, SDR, PDR, CDR, TRR) have been closed in agreement with the customer.<br>Establish the credentials of the project Systems Safety engineer/representative.<br>Audit of review records to establish the completeness of the FMECA.<br>Audit of test and support equipment calibration records. |

(*Courtesy:* Tim Welburn.)

A well-prepared case is a tool for fending off claims; a claimant will see that is will be hard to win the case where a sound defense plan is in place. A corollary is that a sound defense plan being in place is highly likely to avoid litigation in the first place, for the delivered system is less likely to incur difficulties due to the more watchful development process being used.

## 10.4 Product Recall

### 10.4.1 Nature of the Product Recall

When large numbers of the developed item are involved, then another liability situation can all too easily arise in the form of a product recall needed because of a design or manufacturing defect.

These are commonly seen advertised in newspapers for such things as defects in automobiles, consumer goods, toys, medicines, and foodstuffs. These notices are directed at the purchaser or user. Other, less noticeable statements, are those sent to wholesalers, franchisers, distributors, and retailers.

In the notice issued for the purchasers or final end users, the serial numbers and products names of the defective production lot are identified. The defect is then explained in lay terms and the recommended immediate action to be taken is stated.

Persons who believe they have a defective item are asked to call a given contact point to arrange replacement or rectification free of charge.

When it is not economic to rectify the item, the maker will recover it, compensating the buyer, as with, say, a bad batch of food.

In some cases it will be economic and satisfactory to make a modification to each item via a rework activity by provision of parts to be replaced or added by the owner, or as a factory operation.

### 10.4.2 Costing a Product Recall

Recalls can be surprisingly expensive exercises. The overall cost might well not only take a project well into a loss balance sheet but also place the organization into bankruptcy.

The easiest way to demonstrate what is involved and the associated cost is by listing the factors involved by use of an example.

Consider an item of medium cost and sales volume—such as a small, special-purpose, measuring instrument system. The bulk of the costs are for tangible items. Some items, however, are less easy to identify in clear-cut monetary terms, examples being the value of loss of goodwill and of disturbing normal operations.

A recall example is presented in Table 10.2 [7]. The defect here could have been that an electrical switch on the control panel of an instrument system was not of adequate rating for use in the situation where all tolerances add up to needing a switching current requirement exceeding the capacity of the switch installed in all of the product run. This problem could have arisen from such reasons as:

- Miscalculation in sizing the switch;
- Design creep in power demand as more features were added that were not recorded;
- Supply of the wrong part by errors of specification or purchasing;
- Ventilation had been reduced from the design value to save cost and size.

Rectification is clearly the least cost option but the loss is still very substantial, well exceeding the profit on sales gained in the first place.

This example demonstrates why so much attention should be given to early error detection and correction and in maintaining design control as it progresses. In this case the cost to rejig the design, prior to approval, would have been a mere $3,100, the larger switch possibly being at much the same nominal cost as the one used originally. Once allowed through to final manufacture, the simple design error cost the organization at least $2,249,180!

Examples of some simple (stupid!) errors that have been seen in recall notices are:

- A well-made electrical rice cooker casing had a small hole in it that could allow a small finger to enter and touch an internal live electrical terminal. It was rectified with a small plastic bung costing cents. How did that hole get there and remain?

**Table 10.2** Recall Versus Replacement Costs of a Recall Event

*The assumption is that 1,000 instruments have been sold and all need to be rectified. They sold for $5,000 each with a profit margin of 20% of sales. The problem was simple, being that an electrical switch capacity was inadequate and could overheat causing a fire.*

| *Item* | *Time Estimate (hr)* | *Cost ($)* | *Number of Units* | *Recall to Fix Option* | *New Exchange Product Option* |
|---|---|---|---|---|---|
| **Designing a repair fix** | | | | | |
| Engineer labor (20 hr @ $75/hr) | 20 | 75 | | 1,500 | 1,500 |
| Drawings, part lists, work instructions | 20 | 80 | | 1,600 | 1,600 |
| Cost of design rectification—if done early before production | | | | | 3,100 |
| **Spares** | | | | | |
| Spares costs | | 10 | 1,000 | 10,000 | |
| Labor costs (1 hr @ $80/hr) | 1 | 80 | | 80 | |
| Warehousing costs inwards receipt and issue | | | | | |
| Labor (2 hr @ $60/hr) | 2 | 60 | | 120 | |
| Tracking and storage costs—average of 60-day supplies | 480 | 0.5 | | 240 | |
| **Press Release** | | | | | |
| Media labor costs | 8 | 80 | | 640 | 640 |
| Newspapers/radios costs | | | | 15,000 | 15,000 |
| **Freight and Handling** | | | | | |
| From customer (worst-case overnight airfreight) | | 50 | 1,000 | 50,000 | 50,000 |
| Inwards receipt and tracking | | | | | |
| Labor—1 hr @ $60/hr × 1,000 | 1 | 60 | 1,000 | 60,000 | 60,000 |
| Tracking costs—$2/day average of 5 days to turnaround × 1,000 | 40 | 2 | 1,000 | 80,000 | 80,000 |
| Outwards dispatch | | | | | |
| Labor—1 hr @ $60/hr x 1,000 | 1 | 60 | 1,000 | 60,000 | 60,000 |
| Return to customer ($50) × 1,000 | | 50 | 1,000 | 50,000 | 50,000 |
| **Repair** | | | | | |
| Labor | | | | | |
| Disassemble—1 hr @ $80/hr × 1,000 | 1 | 80 | 1,000 | 80,000 | |
| Repair assemble and test—2 hr @ $80/hr × 1,000 units | 2 | 80 | 1,000 | 160,000 | |
| **Replacement Item** | | | | | |
| Replacement Instruments | | 4,000 | 1,000 | | 4,000,000 |
| **Other Costs:** | | | | | |
| Loss of production due to diverted staff—assessed as $1,000 per recalled item repaired | | 1,000 | 1,000 | 1,000,000 | |
| Replacement loan instruments (only to those customers which request loan item—estimated number of items 150 at cost of $4,500 each (including all depreciation, insurance, and handling costs) | | 4,500 | 150 | 675,000 | |
| Legal advice | | | | 5,000 | 5,000 |
| Total cost estimate of recall and repair defective instruments | | | | $2,249,180 | |
| Total cost estimate to replace defective instruments | | | | | $4,433,740 |
| Profit available to offset losses | | 1,000 | 1,000 | | $1,000,000 |
| **Minimum loss due to recall—that of rectification** | | | | | **$1,249,180** |

(*Source:* Tac Furnell)

- An automobile transmission that needed a total automobile model recall to change a simple tension spring key to reliable park brake operation—again costing cents for the part. How did a 6 Sigma manufacturing process allow this one through to all units?
- An electrical appliance with an unsafe Earth protection system that could only be rectified by use of an additional isolating transformer, so it was rendered unsaleable. Someone slipped in not understanding the lack of safety in use of autotransformers!

It is often the minute design issues that can so easily cause a recall. Similarly alarming costs can arise for low-cost, high-volume items—like circuit boards for consumer products, and for high-cost, low-volume items—like a fleet line of submarines or transport vehicles.

## 10.5 Expert Witness Activity

### 10.5.1 Role of the Expert Witness in Legal Cases

During a working lifetime, the design engineer may be called to give evidence, not in defense of his or her own design, but as an impartial person who “gives expert witness” to aspects of the designs of others.

This role has been called for by law [8]:

> If scientific, technical or other specialized knowledge will assist or to determine a fact in issue a witness qualified as an expert by knowledge, skill, experience or education, may testify thereto in the form of opinion of otherwise.

Even before any approach is received from a law office, to be an expert witness, the designer, or, better, the organization, has to have in place a clear policy for managing such legal involvements. They need to be approached with care and some enlightenment.

Rules of engagement for being an expert witness need to be clearly understood by both the expert and the person whose case is being supported. Reports and tests carried out by the expert can so easily be used out of context.

Options are:

- Not to be involved at all—but you may be the best person and a case may be resolved using your expertise that may not otherwise be.
- Take the truly impartial standpoint, meaning your testimony will be the same regardless of which side is retaining you—not as easy as it appears to be.
- Use a style, but not the substance, that favors your client.

The manner in which a court proceeds with evidence presentation is often not the same as scientifically debated issues are discussed. Qualification of a point is often separated from the simple yes or no answer.

For example, it is normal to be asked a question, when in the stand, like, "Given that you have seen details of the design of this custom-built electrified car, can it, in your expert opinion, reach 200 mph?"

On the basis of calculations already done, the engineering expert agrees but wants to add the qualification that it would, however, explode at the about the time it reaches that speed due to the very large heat losses dumped in the motor as it accelerates up to speed. The lawyer only wants a "yes" or "no." Answering yes seems to omit the important issue of subsequent failure. Counsel, however, may not want such qualification by you at that time but will ask for it as part of the reply to a later question posed to you. The process of truth presentation can be very slowly executed in the courtroom.

When coming under cross-examination, the expert witness has to be very sound in his or her thinking on the spot and under pressure. He or she needs to be able to answer all manner of questions, including some deliberately intended to disturb the expert's presence of mind.

It is a challenging, possibly scary, experience, with long periods of waiting to be called to the stand.

### 10.5.2 Hints for Being an Expert Witness

Taking on this role needs careful reflection regarding likely spin-off. The opposing counsel will try hard to seriously discredit your expertise, even to the point of twisting the truth by selective use of your answers.

The following pointers are of use for those who decide to be an expert witness [4].

Once briefed with your task, try to keep away from the lawyer you are assisting and from knowing too much about the case. Prepare only to give evidence on the aspect for which you are expert.

Before the trial:

- Evaluate language differences in use of terms and semantics of the technical domain remembering that the bulk of the court will be laypeople who may need simple explanations for issues or terms that the expert takes for granted.
- When preparing evidence, the issues are: who, what, where, when, why, and witnesses.
- All answers should be based on well-researched and scientifically sound principles.
- Opinions should be those of the expert only.
- The fee for service should be paid for in advance. Do not work for a contingency fee, as this allows the evidence to be seriously discredited.

When appearing in court:

- Arrive at the right place, in plenty of time, so as to be well rested.
- Speak clearly and slowly.
- Do not rush to answer; take time to think things through.

- Address the judge and the jury.
- Answer only the question asked of you. Where it applies, do not be afraid to say that you do not know the answer. Fudging or dodging the issue then is easily seen through and will assuredly lead to tough cross-questioning.
- Concentrate on answering the questions and not on how the case seems to be going.
- Take time to reply with a well-considered answer. Speed of reply is not important.
- Be prepared for questions on your qualifications and experience; some may appear insulting and get you ruffled.
- Try to stay confident in what could be a harrowing experience.

## 10.6 Security Issues

### 10.6.1 Overview of Security Needs in Project Design

Whatever the project, security of access and project information will usually be needed. How this is done will generally be made clear to new staff members as they undergo an induction course into the larger organization. Experienced personnel joining the team will also need to be acquainted with local security needs for processes and methods of control can vary between organizations.

Obtaining and maintaining project security is costly and it can take a long time to get approvals in place. For example, a defense security application can take months for clearance and cost thousands of dollars for the organization seeking access. Such penalties need to be planned into projects. For example, defense companies often set up an office outside of its main secure area to allow new staff members to begin with them while their defense security is being processed.

Key areas to consider will include those to do with:

- Use of computers;
- Access to facilities.

These are now addressed.

### 10.6.2 Security in Use of Computers

Computers are provided with access protection using a password. In team working each person can operate the same machine with a different password and not see the work of others on the machine. It needs to be remembered that access to files might, however, be possible by system maintainers so security is not entirely sound in standalone or file server–based systems.

Access to machines by external users is usually restricted through use of a firewall. These will not communicate certain data from and to external sources. Firewalls can restrict effective cooperative operations with external users. A firewall also assists prevent ingress of computer viruses.

All computers must have effective virus detection and correction; see Section 4.1.2.2. When taking a computer into a secure environment, the organization will usually require it to be cleaned of any viruses by running a virus check program. Bearing in mind that a laptop will usually have in excess of 20,000 files on the hard drive, it can take over an hour to be checked out. This needs to be taken into account when making visits. It will also usually be a condition that the computer is not connected to their intranet in any way.

E-mail messaging is now the widespread way for communication. Users often believe they are sending messages that cannot be read by other than the addressee. This is not always so—as President Nixon found out in the Watergate affair. In many systems messages sit on one or more servers of the ISP machine and they will also be passing through numerous computers situated all over the globe—just where it has passed and been stored can be very difficult to establish.

To maintain system continuity the ISP operator will usually be continuously creating backup archive files. This means many unauthorized people could have access to messages. Despite an e-mail application being set for a deletion time of a few days, files are often held for quite long periods of time. On one occasion some 100 messages of the author reappeared in his in-box from a year beforehand!

A server operator can have monitoring processes in place for excessive and unusual events in the file system. For example, university systems usually have monitors in place of users' file storage size; those that exceed given levels are investigated for abuse of use. Where inappropriate use of e-mail is suspected (and where appropriate authority is given—but is it always obtained?) people's files can be monitored and read.

To make e-mail communication systems secure, users are connected via dedicated local area and wide area networks using encryption and tightly controlled access to files. However, even that cannot be assumed to be totally secure.

Where highly secure file work is needed, such as at the "secret" level of defense classification, special computer builds are used that have a removable hard disk drive (HDD). This has to be removed from the computer and placed in an approved lockup cabinet inside the secure area at the end of each session. These HDDs are not permitted to be carried off-site and their movement from the secure cabinet must be logged and signed for.

In highest security installations it may be necessary to consider what has become known as the Tempest effect, detection of low level signals emitted by computers. As the keyboard is used, the electrical currents of the digital coded signals for each symbol are sent down the leads. These generate very low-level electromagnetic waves that radiate several meters. This effect is small but listening systems can be devised to read the data being keyed in from many meters away. Listening can also take place for antenna radiation. Optical tempest uses optical methods to detect acoustic pressure waves formed on the windowpanes by speech taking place in a room. This sounds like something from a James Bond movie, but relatively straightforward physics of low signal-to-noise ratio detection systems shows these are quite feasible systems.

Facilities of high classification might need to be set up in offices built inside a Faraday cage having special cabling and circuitry. Further information seems to only be available on some Internet sites (search on “tempest,” filtering out “Shakespeare” and “games”). Textbooks on the subject do not seem to be available.

An aspect of computer management that is often overlooked is that of ensuring complete deletion of files. This arises when files are no longer needed or when the computer is pensioned off or passed on to another user.

Removal of files using a delete command does not necessarily remove the file data. When this command is invoked, the file name information is removed and the data locations marked as being available for reuse by writing over them. Until they are overwritten they will still have original data that can be recovered relatively easily. The safe way is to reformat the HDD or better still to suitably destroy it. Similarly so, apparently deleted files on a CD-ROM might still be there for access by trained persons using specialized software.

Obviously paper records that need to be destroyed should be shredded and then burned for good measure. This is easy to do for small amounts of pages but large archives need substantial resources for this operation—it is not uncommon to hear of sensitive private or confidential records turning up at the local refuse dump.

Another lesser-known fact is that the reuse of a file as a starting point for a similar new file may carry with it, into the new use situation, data on the previous one. An example was the receipt by a staff member of his staffing contract by e-mail attachment. When printed it showed only his own details. Using an appropriate, commonly available tool toggle, the document was set to show all changes, and thus past detail, made to the original document as it was set up for another person.

Detailed information on secure computer facilities is found in [9–12].

### 10.6.3 Access to Facilities

Many organizations give access only to approved persons. Readers will be aware that this situation is increasing over time.

In many instances it is to ensure only those that subscribe to services are allowed to use them. Examples of this include special libraries, sporting facilities, clubs, and limited access areas in banks. To gain access, the person applies for membership, which may incur a fee.

Other limited access facilities are set up to protect the leakage of proprietary, government, or national defense information.

Most large commercial and defense companies will only allow access to staff offices by visitors who are authorized to enter, who sign in, and who are escorted by an approved staff member. Staff will usually meet people not possessing clearance in offices set up outside the security wall of the company’s premises.

As an example of a nondefense secure situation, an independent test facility was set up by a state government for gaming machine testing and approval. A typical annual turnover for the more than 2,000 gaming machines that would use the software and machines being approved, had an annual turnover exceeding $2 billion, so fraud in software code and machine operation is an ongoing, well-known risk. This facility needed to have a well-developed security system for visitors, delivery staff, and technicians and had to be set up to minimize break-ins and eavesdropping.

The activity needed what was known locally as a “police” level of security. All persons entering have to pass prior arranged detailed security checks. The laboratory itself—large enough for 20 computer machines and 5 staff—had to be electrically and physically screened in the walls and across the suspended ceiling space. Tight control was put in place of movements in respect of testing of machines and ROM chips sent in for approval testing.

Visiting defense facilities require well-processed approvals. In-country, national citizenship people need a sponsor within the organization to be considered for entry. Foreigners need to apply to their own national defense department, via a local defense department staff member, who then corresponds with the defense attaché staff for the country to be visited. That person makes the link to the sponsor at the country of the defense facility to be visited.

Approval can be tedious and take from days (rare!) to months to obtain; it may not be granted.

Frequent visiting is covered by the issue of a pass; signing in is still needed. Taking in mobile phones, laptops, recorders, and cameras is banned unless permission is granted. They should be left at the security office gatehouse.

Staff of organizations where security clearance is required by visitors should be well acquainted with the procedures, but that is not always the case.

## 10.7 Summary

It has been shown how lack of attention to many legal issues can heavily impact project development and its successful conclusion. The range of legal issues likely to arise has been outlined generating basic familiarity at a level that will point up when to call in legal advice.

Dispute resolution, common legal documents encountered and regulations and approvals have been introduced.

Designs have to be safe and meet a gamut of regulations. Legal liability is thus a key issue where even small design errors or misjudgments could bankrupt an organization by way of expensive lawsuits, or from the cost of rectifying system defects through the recall process.

What legal liability is, in relation to engineering design, has been illustrated using examples presented to indicate the complexity of situations. How to minimize the risks of legal action has been discussed.

A simple recall example was given showing how ensuing costs can easily exceed profits made for a sale of a product.

Security of information in computers and offices, and access to installations has also been covered in this chapter.

More detail is available in texts on the topics covered. Material presented here is not intended to, not can it, replace the need for professional legal expertise.

## References

[1] Phillips, J. J., *Products Liability: In a Nutshell* (Nutshell Series), Perth, Australia: Nutshell Books, 1998.

[2] Goodden, R. L., *Product Liability Prevention: A Strategic Guide*, Milwaukee, WI: American Society for Quality, 2000.

[3] Kinzie, M. A., and C. F. Hart, *Product Liability Litigation*, Independence, KY: West Legal Studies, 2001.

[4] Nicholas, J. V., *Relationship of Legal Issues to Measurement,* in *Handbook of Measurement Science*, Vol. 3, Ch. 34, New York: Wiley, 1990, pp. 1433–1472.

[5] Olson, W., *The Rule of Lawyers,* New York: Truman Talley Books, 2003.

[6] Welburn, S., *Management of Small Systems Engineering Design Teams*, Subject Final Report, SEEC, University of South Australia, 2002.

[7] Furnell, T., *Management of Small Systems Engineering Design Teams*, Subject Final Report, SEEC, University of South Australia, 2001.

[8] Black, B. A., "Unified Theory of Scientific Evidence," *Fordham Law Review*, Vol. 56, 1988, pp. 595–695.

[9] Allen, H. J., *The CERT Guide to System and Network Security Practices*, Reading, MA: Addison-Wesley, 2001.

[10] Northcutt, S., et al., *Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs), Routers, and Intrusion Detection Systems*, Indianapolis, IN: New Riders Publishing, 2002.

[11] Oppliger , R., *Internet and Intranet Security,* 2nd ed., Norwood, MA: Artech House, 2002.

[12] Phaltankar, K. M., *Practical Guide to Implementing Secure Intranets and Extranets*, Norwood, MA: Artech House, 2000.

CHAPTER 11

# Prototyping and Modeling in Design

An appreciation of the elements of prototyping and modeling in design is given in this chapter. It deals with:

- Activities that result in the first-build of subsystems and of the whole;
- What a prototype is as a key first implementation of a design at the detailed level;
- Reasons for producing a prototype;
- How prototyping is shifting from use of physical models to modeling and simulation in a virtual computer environment;
- As an example, how a proprietary tool suite is used to develop a major electronic system;
- How modeling is applied to virtually every aspect of a system design;
- Why computer-based models cannot totally remove the need to produce physical prototypes;
- Things to attend to reduce the risk of faults existing in prototypes.

## 11.1 System and Product Development Overview

### 11.1.1 Development as a Set of Activities

At this stage it is necessary to recall that the various manifestations of the system at each stage of the SE life cycle—for details refer to Section 1.1.2—commence with the development of a conceptual model of likely designs that might meet the customer requirement.

A select set of these candidate designs passes through a feasibility stage. Here is where more reality is added to the systems model, eventually permitting down-selection of those concepts that look sound. It will be found that the outcomes are possibly different to the original intentions. Adjustments are constantly being made to track the customer's now-updated need.

Once the design has been reticulated to the required depth of detail, the particular one to be built is selected and moved to detailed engineering design. This stage readies the development for manufacture.

By now the system is understood to the point where individual components and subassemblies are well specified such that metal can be cut and plastics molded. Parts are built and interfaced, software is ready to go, and a whole host of other very specific quantitative and operational issues are now defined. Manufacture then commences to produce the system for use. Operation then begins with users interacting with the system in real circumstances. After its useful life the system is pensioned off by destroying it, or by passing it on for reuse as it stands, or after a refit.

The concern of this chapter is the capture and transition of the design ideas as they were transformed into the detail needed to create the final system. This book does not attempt to cover the manufacturing stage, for that is, today, a most sophisticated process.

Here we take matters to the point where sufficient detail of a design is available such that it is reasonably safe to assume the manufacturing stage can proceed with minimal rework of the design. Activities that take place as a product is created are shown in Figure 11.1. This diagram represents development using physical prototypes, being the traditional manner for proving designs—later we will discuss the use of computer-based prototyping.

To develop appreciation of the activities that take place the following are the steps used in development of an electronic regime product, the printed circuit board (PCB):

- Call up the requirement from suitable documents.
- Create the system architecture for a suitable system.
- Select the technology to be used—PCB here.
- Select main components.
- Create a board layout for the placement of components.

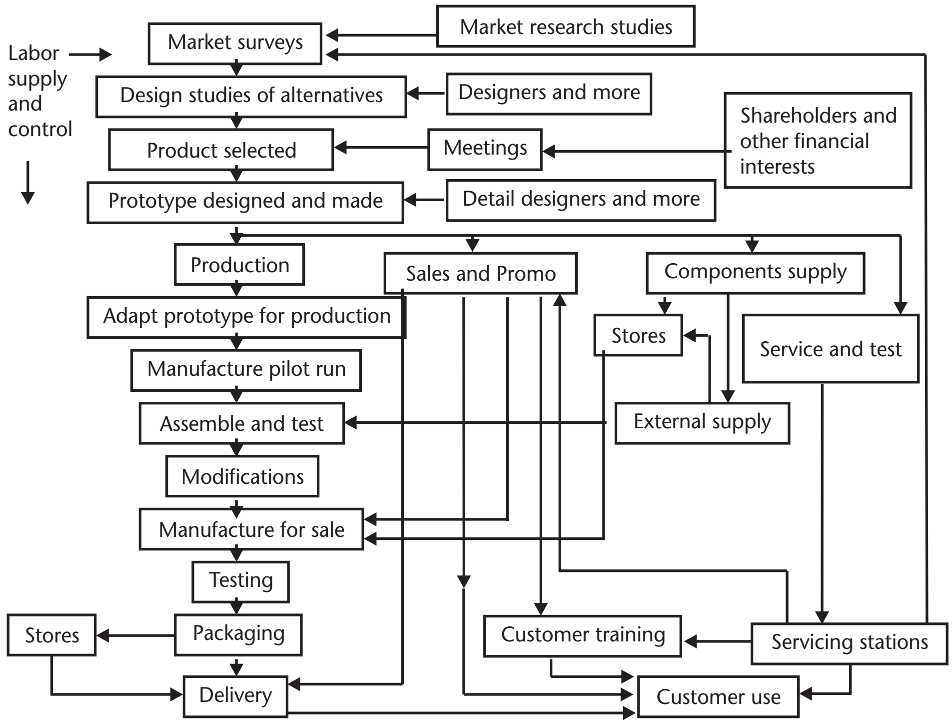


**Figure 11.1** Activities in traditional product development.

- Set up the wiring layout between proprietary components using computer-based tools to assist the board layout.
- Run computer tests of the system where tools are available to support design.
- Apply optimization techniques to tune the design.
- Create parts lists and order them.
- Send PCB design to board maker by e-link.
- Receive ready-to-use board and components.
- Load the board with components and apply solder.
- Use the first such assembly as the basis for physical testing and further optimization.
- If acceptable, finish the board in hardware form with paint masks and protection layers.

The integration of the paper design detail and the hardware has taken a well-established path that has been proven over, in this case, about 50 years.

Other regimes of design—mechanical, hydraulic, optical, chemical, electrical, and so forth—each have their own well-established methods and support techniques. Each also has been progressively better supported by the use of computer-based methods that allow prototyping using virtual models.

### 11.1.2 Designer's Viewpoint

Throughout the development cycle designers are intent on creating parts and assemblies that will:

- Perform the task set in the requirements statements given to them as their design goal.
- Be safe, add value, and not attract loss to their organization.
- Provide the reliability specified, in that their designs will last the distance.
- Use materials and time to the best advantage by an application of optimization techniques.
- Use their professional ability to innovate better, faster, and cheaper designs.
- Avoid the need for design rework at all times.

With systems, being custom in nature, design success is very much a matter of using innovation and invention to create the solutions for many newly seen design situations.

It is relatively easy for the experienced professional to create new options. Proving them is always necessary to maintain confidence that the novel pathway being undertaken is heading toward the right end goal and that decisions made will yield designs that will indeed work as needed. Optimization is needed to ensure that the designs are staying competitive.

Designers and the project managers all need to know if their work is holding up. It is like stepping across a rushing stream. The long step to the next firm foothold is taken with some trepidation, for the steadfastness of that next stone can be unclear before it is tried out with a real test. Means are needed to keep up a designer's confidence; this is done by the use of prototypes and their systematic testing.

### 11.1.3 Aims, Targets, and Milestones

A dominant confidence building method is the use of performance milestones set ahead of time. These do tend to be seen as being needed mostly at key financial events, but their real purpose is to demonstrate that performance is on the way to being reached.

At the highest level the program manager and paying customer are looking for evidence that a stage of the SE life cycle has been adequately completed. These milestone points are often referred to as "gates," for the project is not allowed to progress through one until a set of metrics has been satisfied.

Targets must be set realistically. Their ownership by the designers is usually best practice. No amount of chastising will make activity meet a target if it is unrealistic. Setting targets that exceed practical possibilities by too much only demoralizes staff.

The pace of a project and its progressive success rely heavily on suitable metrics being used.

These must be set up inside a holistic environment through the top-down definition in the earlier produced test and evaluation master plan; this is the source of definition of the high-level metrics.

A commonly used method of tracking the maturity of performance of key project variables is the technical performance parameter (TPM) method briefly introduced in Section 2.5.2.

A critical TPM is selected. Charts are prepared regularly for each TPM to show their:

- Final target performance value and date of completion;
- Current value;
- Predicted value at stated milestone time;
- Variation of the accuracy and uncertainty of the determinations above;
- Past values to show trends.

Figure 11.2 shows a sample TPM graph. The exact nature of such charts will vary with each project, but it is best if they are of the same format.

At design and project management review meetings TPM charts are used to drive discussion and set up actions where they are not tracking to plan, or are doing better than expected.

Data for forming a TPM in the early conceptual stages is obtained from calculation using models of the situation at the time and later from physical prototypes built to test and learn about that particular variable.

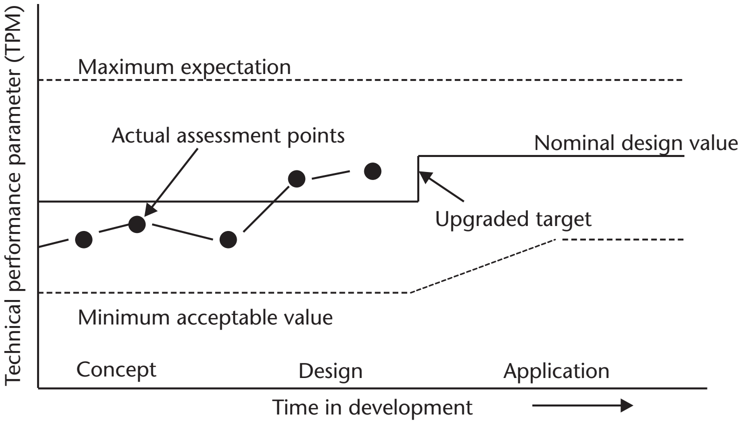


**Figure 11.2** Example TPM chart as it nears the final milestone.

## 11.2 Creating Prototypes

### 11.2.1 Role of a Prototype

The Oxford Dictionary defines a prototype as: "Original as a pattern for imitations, improved forms, representations, etc… Trial model or preliminary version of a vehicle, machine, etc." Reference [1] states this is a: "Synthesis step in which some part of the problem is developed to some level of completion."

Thus, a prototype is not necessarily a first-time assembly of the whole system but is often just a part of it.

The term *prototype* has various uses. Some technical versions are:

- First build that is fully made and delivered (Boeing 777 No 1 aircraft was sent to a customer for use);
- Fully made, but never intended for customer use (many automobiles now in museums and Concorde aircraft Prototypes 1 and 2 in England and France);
- Partial mock-up to investigate selected features (control room mock-up for a submarine);
- Rapidly made model from which to learn (software development uses this approach).

In former times a prototype was always made as a physical artifact. Today, however, it may well start out as a computer model, eventually becoming a real implementation after considerable testing and tuning.

A prototype then provides a time-stamped design statement of part, or the whole, of a development.

### 11.2.2 Physical Prototypes

In the physical prototype form parts of the hardware and software are frozen in design detail so that something real can be built for the first time.

Existence of a prototype provides a solid foundation for many spin-off processes. They allow useful things to take place:

- Design principles are verified as sound.
- Interfaces work properly where needed.
- Testing for compliance with requirements—proof of concept—is possible.
- Documentation for prior and following work becomes available.
- Service and support planning is facilitated.
- Production planning starts in earnest.
- Sales and marketing planning hardens.
- Discovery of unpredicted emergent properties can take place.
- Use in a scenario-based design situation provides a representation of part or the whole [hardware in the loop (HIL) use is an example].

Most of these roles can now be provided by computer-based prototypes, the exception being that a physical manifestation is still needed to see if they represent reality well enough—this fact is often overlooked when using digital models.

A physical form of prototype will usually contain more factors about reality than a computer model can, but it might still miss some key design factors. The best test is always final use in its actual application environment, something not always possible under controlled test conditions.

Physical prototypes facilitate real tests for such parameters as internally generated thermal heat rise and environmental parameter influence testing. Computer-based modeling is, however, often very capable of doing these functions.

There exists strong support for "iterative prototyping." Here the model, be it computer-based or physical, is progressively developed. This especially suits software development but it can be costly of resources in the physical item scenario because modification may require an extensive rebuild each time. Compare the simple need to change the value of a gain (gearing) element in the following cases:

- Computer model (change a data value);
- Electronic model (change a resistor numerical value);
- Physical electronic board (change the resistor);
- Commercial truck (rebuild the gear box and possibly the gear case);
- Chemical reactor (new reactor vessel and feed system);
- Number of participants in a war test scenario (outfit, house, and feed people).

## 11.3 Model-Based Prototyping

### 11.3.1 Role of Models in Prototyping

Computers have been used to form highly effective models of systems since the 1940s. Models of the behavior of ballistic missiles were used (via mechanical computational mechanisms and thermionic valve based electronics) in radar directed gun aimers that defended England from flying bombs during World War II—with such efficiency that the kill rate over Normandy beaches reached 994 out of 1,000 on one day, rendering the weapon ineffective.

As computer power has increased, there has been commensurate activity in building ever-more sophisticated models. Initially they had little power and could not compete with physical models. After decades of development, the situation now is that many products and systems can be modeled so well that their representation is good enough to use as a virtual replacement of the physical mode for most of the development activity.

A word of caution is needed. It must be emphasized that the use of computer models is very varied with respect to their fullness of representation. Only highly developed models can (almost) completely replace the role of the physical artifact; not even the most successful CAD-based design suites can be guaranteed to completely replicate the full extent of reality.

With effective use of a design tool suite, this may well produce a good enough system to deliver, but that cannot be known with sufficient certainty until it is built and used in the appropriate environment for the first time. Modeling reduces test error rate considerably but it rarely eliminates it.

The use of a computer-based model for design has considerable advantages:

- It can offer faster development of a sounder product.
- It allows reuse of designs for rapid redevelopment.
- Design sensitivities are easily studied, where tools support such modeling.
- Data is available for related design and development needs.
- Reliability studies can be carried out as if the real object were being investigated.
- The number of physical prototypes required is greatly reduced.
- Records of reliable information are available.

As has previously been mentioned, the design process that is soundly used progressively eliminates the many choices that exist at the start until all parameters are decided and the specific system has been realized. This process has been shown in Figure 5.5. As choices are made, they impact on other parts of the system; sound system reticulation and interface control seeks to ensure these impacts are understood and properly accommodated.

Reality, however, may well result in some surprises, for not all assumptions made are sound and engineering design is a mixture of science and art, so some degree of subjectivity usually plays a significant part. Prototypes are the means for identifying surprises before the system goes into service.

### 11.3.2 Characteristics of Models in Engineering Development

Models may take a variety of forms:

- Mental constructs (meta models);
- Physically existing assemblies (perhaps scaled in size and time of operation);

- Block diagram assemblies with connections;
- Formal math equations;
- Finite element (FE) solutions;
- Simulations using a multiple "change and see" approach;
- Knowledge-based systems (KBS) systems using rules-of-thumb heuristics to steer the design work.

Hybrids of these are commonly used.

Three types of model are used in development: physics-based, process-based, and iconic hardware items:

- *Physics-based models:* In these a real world activity, existing or not yet existing, is represented by laws of physics that are expressed in terms of mathematical equations. An adequate representation of the real world "open system" requires extensive mathematics that is not always available to the degree of completeness needed. Corners are often cut that can be later overlooked. Much of engineering practice has been modeled this way, but it has been long recognized that not all systems aspects can be handled by use of "hard" formal description. Adding in empirical data is sometimes needed; examples of this are found in flight dynamics of aircraft, temperature distribution on an electronic circuit board, wing lift, and other fluid flow designs.
- *Process-based models:* Here the modeled domain is represented by a set of rules embedded into an algorithm. This "softer" thinking approach is often superior to the hard-science model in terms of applicability and can yield a model where the nature of the problem defeats formal description. Examples of these types of models are the queuing of traffic in a road system; a logistics supply system in operation such as loading a cargo ship in best time; a manufacturing facility flow; and an expert system control room support system. This type can also accommodate the still softer human issues—but not that well—using systems dynamics (SD) modeling tools like IThink; see Figure 1.10.
- *Iconic model:* An icon is an object representing something. Here it is used to represent the physically existing model of something. Examples abound: wind tunnel scale model of an automobile, driver's seat mock-up, and a scaled down model for oil refinery pipe work. These, being handcrafted, are costly to make; easily destroyed or damaged in testing; cannot be altered with ease; need special crafts skills to build; and can only represent a small range of conditions. Once commonplace, they are now becoming a thing of the past as an economic means for supporting design. Computer simulation is overtaking the need for these for that alternative is often superior to any iconic model. Further, the computer model can also be placed into a virtual world environment to put the system under virtual test. For this reason there is now a diminishing demand for physical model testing facilities. Reduced demand pushes up costs, which can render them unaffordable. Some large wind tunnels, for example, have been closed down for lack of sufficient business.

Setting up a mathematical model to represent the first-level principle of the issue under investigation, as represented by known laws of physics, is rarely sufficient for engineering design use. The models must also represent the numerous second-level effects caused by the imperfections of real materials, design inadequacies, and external influence effects.

As has been discussed in Section 8.4.1, sufficiently adequate models rapidly expand to be complex, needing ever increasing effort to establish the particular equation coefficient values the model needs to be run.

Over time these have, however, been developed for some industries to the point where they can adequately represent the need—but at a cost that is not always evident, for much of the development has come from past projects and before that from university style research. Sophisticated models shown as selling demonstrators do not reveal how much effort has been expended in their development!

Some regimes have been particularly good for modeling realistic systems. One example is that of electronic circuitry, where sophisticated models and tools can deliver an almost complete virtual development environment. Computational fluid dynamics (CFD) and mechanical and manufacturing design also now have tool support for design and development that needs minimal final physical testing.

With tools new knowledge learned in their use is fed back to improve the model. The success of some tool packages may then give the impression that all engineering design can, and should be, model-based.

That is a fine aspiration, but there are many areas where such support is slower coming for reasons of complexity not allowing adequacy of modeling, or perhaps because the industry sector is too small to support the costs involved of developing the special tools it would like to use. In such cases tools are often adapted from other fields.

### 11.3.3 Changing Role of the Physical Prototype

The nature of the use and form of prototypes in engineering development is changing.

In traditional development the sequence “Design → Test → Fix” is used. Here a system element is first designed on paper. When the design seems to be sound, it is built to a level of completeness. Testing follows this. It is often then found that it does not work adequately and is subsequently modified and tested again (and again!) until it seems to provide the required functionality. This is often referred to as a process of “design a little, test a little and fix a little.” Some maintain this is a safe way to proceed for less is lost if errors are made.

The costs penalties of this incremental process are:

- Lost sales or penalties from being late to market or in meeting a contract milestone;
- Costs for the multiplicity of rebuilds and tests;
- Cost of heavily used testing facilities;
- Lost business due to smarter competitors being in place in a timelier manner;

- Possibly less attention to detail in design, for it can be detected and fixed without major embarrassment and cost. The test is used to find out what has resulted from design.

This methodology is still much in use by smaller design activities; by those who are in danger of falling behind with best practice progress; and by those who do not need computer-based development to remain competitive. While it does pick up errors early, it tends to go against the "fix errors early" philosophy for it encourages lax design discipline and less front end loading to be allocated. Work on paper or in the computer, however, is generally cheaper to correct than it is on physical objects.

The current alternative, the modern trend, is to use the sequence "Design (using a computer model) → Simulate → Fix/optimize the model → Physically test (occasionally)."

Here the physical test is used less often and, importantly, it is used to verify that the model is accurate and calibrated, not the other way round—that the design outcome is used to learn what needs fixing.

A model-based design can be iterated many hundreds to thousands of times in the period it takes to make a new physical test prototype artifact.

The benefits of the model based approach are exemplified in its use for designing the winning New Zealand *America's Cup* yacht. They formed the first design in CAD. This was iterated until it seemed to be a reasonable design. A test iconic model was fabricated and tested in the tow tank. This cycle was repeated around 8 times in 6 weeks. In that time they were able to carry out more than 6,000 iterations on the model, whereas they could only build and test some 10 tow models.

The model-based practice is commonplace in industry, where it is economic to support development of the computer-based model and its support environment.

Models have, in many cases, become a deliverable item that is continuously developed as it passes through each stage of the system's life cycle.

Many contractors will, however, be less inclined to deliver the model with the system, preferring to keep it as their own protected intellectual property. This practice of model retention thwarts the idea of a lifelong model being available for a project. Contracts need to state clearly that the model is to be supplied in a form that is complete, certified, and useable.

Prototyping should never be a "many surprises" activity because it is then incorrectly being used as "an experiment to find out what has resulted." How to reduce such a situation arising is summarized in Section 11.7.1.

## 11.4 Creating Models

### 11.4.1 Informal Use of Models

Much of engineering development only uses modeling and simulation (M&S—not S&M; that has a quite different meaning!) as a useful sideline support methodology. There, models are developed as and when they seem to be useful. In this mode of use they are more the tools of and by individuals than a part of the project's technical management at large. Models built in this mode will usually be found to not be:

- Integrated into the whole project;
- Documented well enough for follow-on use;
- Archived adequately and thus rendered unavailable;
- Using reusable architectures or project-approved architectures and languages;
- Properly verified, validated, or accredited;
- Guaranteed to be sound or complete enough;
- Seen as part of project deliverables.

### 11.4.2 Basis of Model Formation

Models of real world systems can be formed of the fluxing entities of a design situation. They will either cover distributed continuous flows (stresses in the skin of an aircraft; weather patterns; pollutants entering a water channel; thermals in an electronic circuit board) or be channeled flows, wherein the "substance" flows in distinct channels and/or with varying discrete arrival times (manufacturing materials flow; public transport movements; digital control system).

Complex situations will use hybrid combination of the above.

Flows in a model are represented by different descriptions of behavior:

- *Deterministic:* Future behavior is formally predicted from knowledge of the model on a single point basis. Example—Given the laws of heat flow, the temperature rise of thermometer allows upcoming values to be calculated at the point of the system space.
- *Stochastic:* Future behavior can also be predicted, but only for the behavior of a group of values having a known statistical relationship behavior. Example—The height of individual transport vehicle drivers who will next use the driver's seat cannot be predicted, but the spread of heights for the set of likely crew can.
- *Chaotic:* Mathematical expressions can handle some forms of chaos using different means to the above. Example—Work activity in an SE process often follows progress descriptions similar to a pile of sand grains that is sliding down from the top—and that has been formalized as sand-pile chaos.

Models need a stimulator (driver, forcing function, excitation input) to make them represent a given situation. The resulting system behavior thus depends both on the characteristics of the stimulator and the model itself.

Stimulators are of several forms:

- *Time-driven:* Example—Equations that are as a function of time, as in heat transfer. A suitable time interval and discrimination are required. The time variable can be sped up or slowed down in mathematical models, which is not always possible in physical prototypes. This is useful for the prediction of future behavior and for understanding events that are seemingly stationary.
- *Event-driven:* Example—A process-oriented model, such as operators conducting an assembly operation in which their task has one kind of variability and the arrival of parts they need has another.

### 11.4.3 Developing Prototyping Models as Deliverables

In model building subsystem models are integrated progressively to cover increasingly broadened complex situations. Models at each level are built using the same set of basic concepts, but vary in degree and application. They are classified into a hierarchical system.

At the bottom level there is more certainty in subsystems operation because more detail is available.

Models representing the overall system tend to be more costly to build (if they are good!) and provide results that give a statistical certainty about the capability needed. They also will usually involve human issues. They cannot give the same level of detail as those lower in the hierarchy but need to use lower level information in a condensed manner by selecting and summarizing what is needed.

For example, an internal combustion engine modeled at the detailed design level will be complex giving the output power to engine speed relationship and also providing for the thermal characteristics, fuel supply, vibration, and other regimes that affect the detail of performance. At the "whole of vehicle" level, the engine model used may well be a simple, first-order, linear model that relates engine speed to power for the state when the engine is above idling speed.

Development of large models needs a clear M&S policy containing procedures, rules, and standards for the project. This has been called a Federation of Models by the U.S. Department of Defense; Figure 11.3(a) shows the hierarchy they have published. Variations of this exist [Figure 11.3(b)]. While the terms used in those diagrams are defense-oriented, they readily can be modified to represent commercial activities.

The sequence in setting up a model now follows:

- Set up the architecture of the system in terms of the fluxes of energy or mass (treat as closed system by setting boundary limits as needed).
- Assign blocks to system functions that can be described in terms of black boxes.

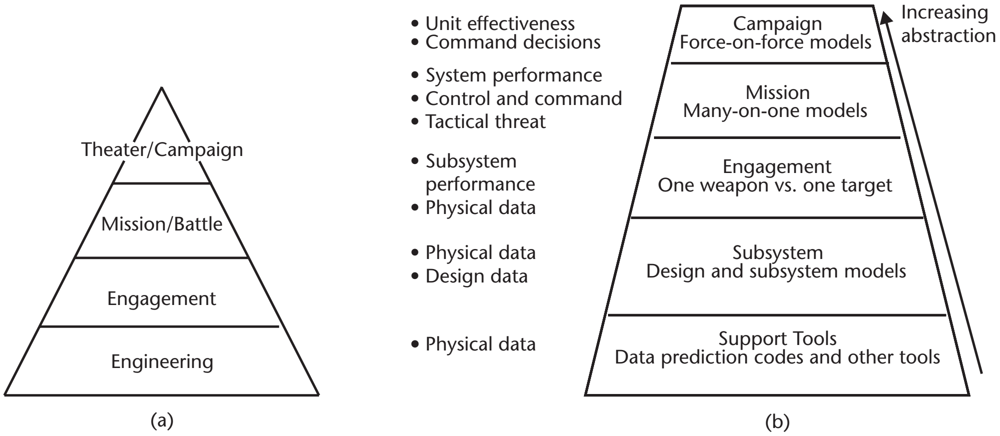


**Figure 11.3** Hierarchy of models: (a) U.S. Department of Defense, and (b) BAES UK. (*Source:* [2].)

- Assign a suitable equation for the output/input relationship for each black box.
- Assign suitable coefficients to characterize the equatinos into a specific application.
- Integrate the whole equation set.
- Run the equation set in a suitable modeling tool with appropriate stimulating functions.

Many tools can be used to support the above process; examples are MatLab, Labview, and IThink.

Tools to support the related management activity of the engineering are covered in [3].

Distinction is needed between the black-box model and the white-box model.

In the black-box model the output/input relationship is the same as it would be in the physical situation. However, the internal operation is not necessarily modeled in the same way as the internals of the real system. It is not always possible to set up access points inside the model structure to tap into internal operations. Changing the external environment conditions imposed on a black-box model will not necessarily be able to provide answers to influence parameter effects.

In the white-box model the internal workings are modeled as they actually function in the real system, thus allowing for access to internal nodes to give partial behavior. These models are much more demanding to build but are often not needed in M&S applications.

Aim for simplicity in model building. Models should be no more complex than is necessary to extract the information needed. They should be built after the requirement for the model is well understood.

Models are never a total representation. They will always be built to exhibit certain aspects of behavior, and have certain limits of dynamic performance. Static regime models have their uses but most used are those that allow dynamics to be investigated—they are much more complicated to build than static regime models.

### 11.4.4 Unified Modeling Language

The Unified Modeling Language (UML) is a third generation objected-oriented modeling language now in vogue [4] for use from the concept stages of engineering development onward.

Three approaches to modeling used to form this are:

- Object modeling technique;
- Booch method;
- Object-orientated software engineering.

Features included in this methodology (for example, from the Rational® form) are:

- Object model;
- Use cases and scenarios;

- Behavorial modeling with state charts;
- Packaging of various entities;
- Representation of tasking;
- Physical topology models;
- Source code organization models.

The backbone is an object model built as a graphic using standardized symbols and shapes. Relationships and classes of operations are assigned to gradually build up a concept model that can be used for other uses such as state-charting to investigate the flows and timings. It has its own vocabulary and grammar; as with all tools, it takes time to become familiar with the formal language used.

Software engineering makes use of rapid prototyping via models. Whereas this does not cover all of the range of energy domains needed in general engineering systems, many of its contributions are useful in engineering design at large [5, 6].

### 11.4.5 Model Protocols and Environments

The characterization of M&S environment protocols uses the following metric entities:

- Shared data consistency;
- Real-time interaction;
- Scalability;
- Extensibility;
- Bandwidth;
- Reliability;
- Latency;
- Heterogeneity.

There exist many kinds of communication systems that can support mixed entity, distributed systems environments. Some well known ones are:

- SIMNET—Simulator networking (United States, IEEE);
- DIVE—Distributed Interactive Virtual Environment (Swedish);
- Bricknet—Virtual Environment Toolkit (Singapore);
- EM—Environment Manager (United States);
- NetEffect—development, support and management (global);
- RING—For use in dense occlusion situations with restricted visibility (United States);
- Spline—Scalable Platform for Large Interactive Network Environments (United States).

Protocols used in M&S shared data environments are also numerous:

- DIS: Distributed Interactive Simulation;

- ISTP: Interactive Sharing Transfer Protocols;
- DWTP: Distributed Worlds Transfer and Communication Protocol;
- RAMP: Reliable Adaptive Multicast Protocol;
- VRTP: Virtual Reality Transfer Protocol;
- HTTP: Hypertext Transfer Protocol (the Internet is example of its use);
- TCP: Transmission Control Protocol (used in common email systems);
- UDP: User Datagram Protocol;
- MMS: Manufacturing Message Specification.

Setting up M&S systems obviously requires specialist IT staff and support and considerable experience.

### 11.4.6 Verification of Models

Models need to pass through several stages of evaluation to reach the point where they can be relied upon for integration into the system at large.

Verification, validation, and accreditation (V,V&A) are the cornerstone activities for ensuring a model is a faithful representation and that it can be used with confidence that what is built from it, or uses it, will have a sound and well understood basis.

This process is sometimes also called independent verification and validation (IV&V).

The terms and practices used have logically developed from software engineering, computer models being themselves formed in the software medium.

- *Verification:* The audit activity of a model begins with verification, the process of determining that a model implementation sufficiently accurately represents the developer's conceptual description and specification. In short, does it model what was intended? Does it do the right job? This step is done largely by study of the needs expressed in the various statements, such as requirements and other high-level planning documents.
- *Validation:* This is the process of determining the manner and degree to which a model is an accurate representation of the real world from the perspective of the intended uses of the model, and the level of confidence that should be placed on the assessment. In short, is it engineered well enough to do the job?
- *Accreditation:* Knowing it does the right job by a sound method, the next step is to grant the model formal certification that it is acceptable for use within a specific boundary.

Obtaining a clear understanding of the specific purpose can be a problem. Models are all too easily used in other contexts where they are not entirely appropriate. This step is sometimes called certification. In short, this is the stamp of approval for use in a given situation. Does it meet the user's needs? What are the situations in which it can be used?

These steps seem clear-cut but rarely are able to be done in a totally crisp and formalized basis for large systems. The "truth" will often be pushed to its verification limits, which then shows up defects as the process is probed more deeply.

It is important to extensively exercise models in their testing. It is easy to set up tests that appear to show the model is working well but do not stretch the model to its limits.

For example, testing an electronic warfare (EW) package using a one-on-one engagement is not a suitable test for vulnerability of an aircraft flying into a war zone where many more threats will be presented.

Underpinning the effective operation of models are the data standards used. Support elements for this are:

- Data engineering (technical support for various data exchange formats);
- Authoritative data sources (identification and description of data sources);
- Data quality (tools are used to facilitate access, review, and assess data);
- Data security [data security technical support for high-level architectures (HLA), data standards].

Many large-scale models are implemented within distributed networks using hardware in the loop (HIL) operation with geographically separated computers. In such cases data for the model may not be timely.

Data latency is the time delay between the occurrence of an event and the arrival of the response to that event at any given point in the modeling. There will always be some delay due to propagation time in computers and links. Latency must be small enough for the simulation to appear to be the same as the real thing.

As an example, a LAN optical fiber propagates data bits at 186,000 miles/sec: this introduces a delay of 5.4 ms per mile. A 1,000-mile link will have at least 5.4-ms delays.

Tank and ship system elements work satisfactorily in large distance modeling systems, for there the dynamics are comparatively slow. Aerial engagement is far harder to get working well, especially if it is not operating on the same LAN.

## 11.5 Physical Prototyping Practice

### 11.5.1 Testing of Physical Prototypes

This section deals with physical prototyping practices. A considerable amount of prototyping is performed in the physical form.

The physical prototype is tested by immersion in a suitable test environment. Problems arising can include:

- The length of the test period in which the design activity must wait can be considerable (some tests need months).
- Special testing facilities are needed (for safety reasons testing of explosives in tropical environments requires the test item to be placed in specially designed,

contained explosion, environmental test chambers set up remotely to the monitoring control console).

- The cost of test facilities will usually be large enough to require considerable lead time in budgeting and manufacture (many programs will not permit such expenditure until the item is near to ready—when it is too late!).
- Data logger systems are needed to capture data, not only of normal test parameters, but also for catastrophic situations. (Deciding what to log can be problematic, so it is usual for excessive amounts of data to be recorded of which only a fraction is ever used.)
- Not all tests can be carried out simultaneously (the serial nature of the different testing regimes needed often builds into a lengthy test period).
- The prototype may well fail in some way during testing, thereby complicating test continuance (a rather too common occurrence!).

Ways to avoid some of these limitations are to use multiple prototypes in the test program but then manufacturing variations need careful control to ensure the tests are of the same item—see later in Section 11.6 where scientifically designed tests are discussed that can assist this situation.

Examples of some test facilities are:

- Basic, commonly used, environmental test chambers for small items like electronic modules, these becoming massive in size for testing major rocket engines under simulation of conditions seen by the burning rocket shooting up into the reducing pressure and temperature of free space;
- Wind tunnels with 20-foot apertures, operating at Mach 4, where the local town electrical supply has to be managed to meet the multimegawatt demand of the fans;
- Forty-ton tank vibration test platform for simulating ground motions of the tank;
- EW test facility integrating the real aircraft EW system, ground threat emitters and multiple flying guided missiles simulated to be flying at the aircraft;
- Load cell test facility needing standardized programmed load changes as time passes over a 3-day test period.

The use and availability of major physical test facilities are changing. Formerly their use would be tied up with a test object for months.

For example, a wind tunnel would be used to test a flight model placed in the throat. Data logging gear would take weeks to set up and verify. At the end of each test run the physical model would be remade and the test undertaken again. Turnaround time for a physical model development would be measured in terms of weeks.

With the advent of model-based design, the designer only needs verification from time to time but wants it promptly, for today's design program cycle times are greatly reduced.

The design agency works with the test facility staff to ready the computer controlled test equipment. When all is ready, the model is rapidly set up and a test undertaken. Pretesting of subassemblies can be used to eliminate errors early. The more that can be pretested before being assembled into larger units, the better.

For example, a major vacuum cleaner maker was experiencing 16% returns from customers—mostly for motor faults. A motor testing line was created that exercised all motor units measuring 10 key variables (motor electrical current, brush commutation sparking, body heat rise, bearing noise, vibration, and more) over a 12-hour period, some tests being under prolonged full power conditions. This weeded out most of the problem motors, reducing the appliance return rate to 2%. The economics of pretesting are usually quite favorable for its use.

What to pretest:

- Components (by supplier and possibly by self);
- Circuit boards (in-house, or at OEM, using board test beds);
- Assemblies (in-house, or at OEM, using special test beds);
- Subsystems (in-house, or at facility using full systems simulators).

Evaluation of prototypes needs to be well thought through. Where possible, use independent evaluation facilities.

The commercially available industrial instrument evaluation process and those of major independent test houses are evaluation models to consider. Steps involved in an evaluation program follow:

- An evaluation program is agreed in writing between the sponsor and the test organization.
- The test program is undertaken (for as long as the test article is still capable of being tested; many do not make it through the full test period!).
- A draft report of the evaluation is prepared.
- All parties concerned are given the opportunity to provide comment.
- A tuning of the report takes place.
- The final report is released to those privy to it.

### 11.5.2 Prototyping Practice in the Electrical/Electronic Regime

As an illustration of the power of advanced M&S systems used in detailed design consider the design and development of an electronic system using a well-developed tool set [7]. Several vendors offer design suites of this kind.

This particular tool set provides integrated support for design activity in several key areas:

- Overall system design;
- Silicon chip development work;
- Verification of the design;
- Mixed signal system design (analog and digital);
- Performance engineering (the ...ilities and optimization against influence parameter);

- Enterprise management (process improvement to ensure best practice and top proprietary know-how is used).

A necessarily brief outline of the main functional units of each aspect now follows.

- *Overall system design:* Proprietary tools support development of the overall architecture with design information flowing in a virtual operation. These include tools for application specific integrated circuits, logic gate arrays, digital and analog design, and verification, all working through a simulation backplane. The vendor provides tools that can easily interface to the client's own tools and those of other suppliers. Library support is provided by the vendor for electronic component information and data management. Figure 11.4 gives the layout of the tool suite.
- *Silicon development work:* Designs of circuitry in silicon allow for floor planning, timing analysis, RTL design, and logic synthesis. Models can be imported for subsystems. A design-for-test unit sets up synthesis using a test generator to detect faults that are graded in their severity. Board-level design and verification are supported.
- *Verification of the design:* Within the board level the design tools support rule checking and procedural audits of high-level schematic circuits. This is carried out in a synthetic environment. Designers using the various implementation technology units have access to this. The vendor can provide libraries of logic modeling and the necessary design kits for the production processes of the various silicon foundries that will be used for manufacture of the circuits.
- *Mixed signal design:* A design can be entered into the synthesis environment in mixed signal forms. Simulation is supported using well-established tools including Spectra, SPICE Plus, and Verilog along with facility to plug the whole into the user's own simulator. Debugging is provided with easy to use graphic interfaces.

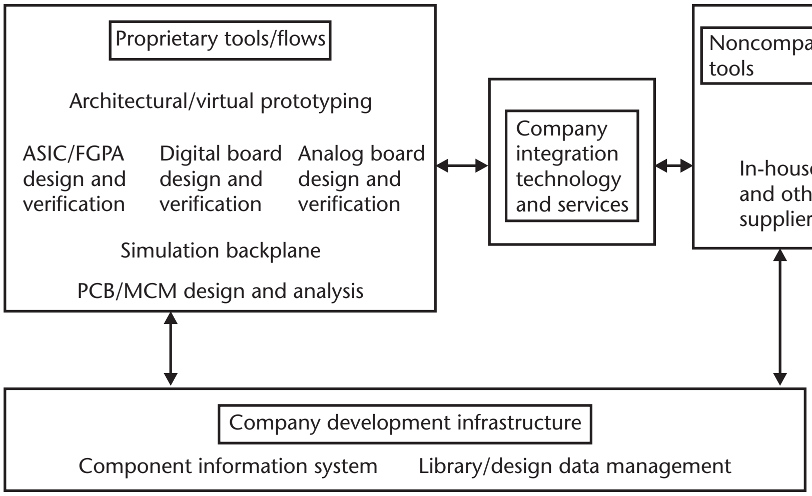


**Figure 11.4** Layout of tool suite supporting electronic systems development. (*Courtesy:* Cadence Systems.)

- *Performance engineering:* The topology and timing performance of the evolving system is explored using functional design and constraint derivation. Physical design is also explored to establish and use its constraints. The system can be reviewed for thermal, reliability, EM, and signal integrity by a performance domain analyzer unit.
- *Enterprise management:* Having established a base line process in the above modules, the competitive user will want to maintain process improvement activities that keeps the design at the leading edge of best practice. Improvement teams in the user's organization work with vendor, in-house, and third-party tools to intervene with process improvements that are carried out to a clear plan set up and administered by the design team's manager.

This rapid overview shows the sophistication of modern design support suites. They are obviously expensive to purchase and install. Significant time and training of already experienced electronic systems designers is needed. Vendor support is essential for economical set up; these are not always plug-and-play systems provided on an installation CD-ROM!

Three examples of the power of using electronic system support tools are now provided.

The first is from the early days of integrated electronic design tool suites (Hewlett Packard, around 1985). Their Design Center system was created with several workstation units allowing the team of some 10 electronic, mechanical, and production professional engineers and board layout experts to work collectively on sophisticated multiboard system developments.

The maker's statement of performance reported that a multiboard system was designed in a few weeks rather than needing many months and the usual many corrections as prototypes were made.

Upon first time physical manufacture the assembly only needed four vias (a postmanufacture wire placed across parts of the circuit to correct for missing connections) to obtain correct operation. This was significant progress in the state of the art of that time. The state of that art has moved on considerably since.

A more recent 1996 example of time saving—"from 7 months to 7 weeks to 7 days," as it has been titled by Cadence, involved an automobile control system design starting its improvement cycle in 1992.

The first use of the tool suite for a design had it ready for full-scale production in the millions in around 7 months. Some 70 microcontrollers were used in the system containing 8-bit logic that needing considerable handcrafting. Systems elements involved were CPU, ROMs, RAMs, ADCs, and clock regulators. In it Motorola and Cadence Design Systems were combined to reduce the time taken for this.

That success was followed by the first round of process improvement in 1994, when they created a 7-week design cycle. A second round of process improvement in 1996, using a new methodology, took the time to design major systems down to a mere 7 days—and with less designers involved. These gains were largely due to major reduction in time needed for correcting errors.

Another example comes from Fujitsu experience. One of their 1993 projects had 23 PCBs that was built using 6 application specific integrated circuits (ASICs), 12 programmable logic controller (PLC) systems, and several complex microprocessors. A new team of 60 engineers was assembled. Some had experience of traditional ASIC design but others were completely new to the techniques.

A new methodology based on a CASE tool working in an integrated tools suite was used. The team was given training and assistance by consultants and was organized as a matrix organization.

From start to finish, design took just 3 months! The first design run had most PCBs and all ASICs working satisfactorily.

It is left to the reader to seek out the latest performance of toolset performance from vendors and users.

It is clear that tools are essential to being competitive today. They also allow far more reliable systems to be developed than formerly could be done using long hand methods traditional methods.

## 11.6 Experimentation and Its Use in Design Evaluation

### 11.6.1 Hit and Miss Testing

Hand in hand with prototype development is testing.

All too often tests are set up at the last minute to support approaching milestones. If there has been no adequate planning, the tests will not have been properly thought through and an ad hoc methodology is likely to be hastily put into place.

This informality can carry penalties:

- Test facilities are not available so other less suitable ones may be pressed into service.
- Issues that should be tested for subsequent follow-on design, early discovery of design errors, and later process improvement can well be missed.
- Test resources consumed will not be used efficiently.
- A poor test result, so late, may become public at the time of greatest exposure and detrimental project impact.

These risks can be greatly reduced by the use of a test and evaluation master plan as has been outlined in Section 2.5.

### 11.6.2 Scientifically Planned Testing

It is often observed that even in good test plans the efficiency of testing does not always use the power that can be provided by scientifically based design of experiments (DoE) methods and tools [8, 9].

Medical research, food testing, agriculture, and environmental research make extensive use of DoE; it is usually part of the undergraduate curriculum of those fields. It appears, however, while engineering designers are given elementary courses on the statistics applicable for testing mass production items, they are seldom given DoE instruction.

Engineers are generally familiar with the basic theory of the Gaussian statistical distribution and its use in sampling for defects on production lines, for curve fitting, for finding regression features, and so forth. DoE takes this basic knowledge much further to give an investigative tool for unraveling complicated issues by setting up efficient and probing tests.

Testing events often possess, with respect to their variables, many degrees of freedom and noise data.

Starting with a single degree of freedom—one variable—the characteristics of linearity, error deviation, probability distribution, best fit lines, and so forth can be investigated using foundational Gaussian statistics.

Adding in degrees of freedom to the situation allows more factors to be compared but needs extension of the theory as has been done under the discipline of DoE (originally set up at depth for agricultural application—hence the apparently strange names used in that area—like "binning").

By separating out test parameters as targeted degrees of freedom in the calculation, the random error can be left as a small residual noise error that relates to the uncertainty of the measurements.

It is possible to rank many parameters of a test situation according to their comparative goodness, this being usually of more value than having absolute and very precise measurements for a smaller number of parameters.

The methods of DoE are best deployed by experienced statisticians working closely with the engineering designers who know what they wish to extract from a test and what can be set up and resourced.

While the theory is complex, it is now contained in tools such as Minitab® that make the calculations straightforward; the mathematics used is almost transparent in their use.

The developed skill needed for DoE application is to be able to pick the right strategy and data inputs; this needs considerable familiarity with methods. While this skill can be obtained by the detailed engineering designer, it will usually not be justified to be learned for the relatively few times it is needed. Large organizations, with well-developed test groups, will usually have the necessary staff skills on board.

To appreciate the power of using DoE methods, consider the need to decide, by physical testing, which of two fighter aircraft types is the best for executing a given precision flying operation.

The ideal test would appear, at first sight, to be to fly the test mission several times, with the same pilot and both aircraft. That is how most engineering testing is done, for it eliminates much of the unwanted variance in the test facilitating the difference between test runs of competitive items under test to be clearly differentiated.

Repeated flying of the test in this example certainly would obtain the necessary number of samples to yield a sound mean and standard deviation having low uncertainty. This would also give the statistical distribution for the results.

One variable of the test is then varied and the whole suite of tests is run again. This builds up a solid understanding of the item under test and allows each test condition to be well understood, but it can be expensive to do and is not the best use of test resources. In many cases the number of flights allowed by time and budget constraints is minimal.

The repeated tests method can be used for cases where the item under test is reasonably stable in its environment and the cost of each test run is minimal and freely available. In complex and expensive test scenarios (a flight test can easily cost $60,000 per hour!), this is not a valid approach.

The problem with the simplistic test plan approach is that whilst it does give some useful and accurate data it is most wasteful of test resources.

By necessity the tests here may well need to take place over different days and thus have different flying conditions. Pilot skill will be an important variable for a single pilot will usually be more experienced in one of the aircraft types. It may also be that the exactly same aircraft could not be used each time due to scheduling and maintenance restrictions.

Where the number of test runs must be limited to a handful, the need is to extract more understanding about more variables even if the precision of the test results is low.

In this aircraft example the prime need is to decide which of the two aircraft is best to use, not how well it does the job.

DoE methods are used to calculate the test requirements for a mixed set of test runs that purposefully randomize the unwanted variables of weather, aircraft used for each type, and pilot skill.

The number of runs used is dictated by the resultant test plan that emerges. In some cases it might well be found that just one more test run greatly increases the findings; or that almost half of the tests envisaged have little bearing in the result.

Use of DoE tools assists setting up plans in a matter of minutes—where the techniques are understood.

As a guide, DoE methods come into their own where:

- Several test parameters are involved.
- Significant unknown randomness exists in the system variables.
- Quality of test results is of less interest than learning how the many variables influence the overall situation.
- Complexity of variables is apparent.
- Costs to test are major and limiting.
- Reasons behind an exhibited behavior are hard to uncover.
- Test runs are limited to a few and separated by allowable limits of accessibility.

If in doubt as to the application of DoE to test construction consult an expert. They can quickly sum up if their methods are needed; advise what they can do with their tools; suggest how many tests will be needed and how they should be set up and run.

## 11.7 Interfacing Prototypes with Manufacture

### 11.7.1 Creating Prototypes That Integrate

If development has been supported by sound SE practices, such as have been explained in previous chapters, the first-built of parts should interface correctly with few problems. The key factors that will decide how well they integrate will be:

- Requirements generation has been made intelligently with sufficient resources devoted early to develop accurate, unambiguous requirements statements.
- Interface partitioning has been done well and maintained such that the number and complexity of interfaces has been kept low and that they are clearly described.
- System changes during the development process have been well managed with all approved changes notified in time for design corrections to be incorporated.
- Test and evaluation plans have been set down and kept up to date such that appropriate tests of the right parameters have been made.
- Materials and components supplied are to the required specification.
- Documentation has kept up with progress making system assembly clear and unambiguous.

With all of those factors passing muster the design should pass its milestone with minimal difficulty. This said, the fact is that they usually will not all go as planned. Last minute changes need be made in haste to meet deadlines.

This is a time for extra caution for in such circumstances compromises will be made and poor records set down.

Discipline is needed to track back through the design process documentation to establish the reasons for faults. They need to be traced and recorded because a source of a fault may well be of key importance elsewhere as an unwanted source of expensive rework.

## 11.8 Summary

This chapter has covered the central prototyping and modeling used in design. It has explained what a prototype is as a key implementation of the design or a part of it.

The reasons for producing prototype designs have been covered.

Discussion has covered how prototyping is rapidly shifting from use of physical models to extensive use of modeling and simulation in a virtual computer environment.

An outline of a major electronic design tool suite has been given to show how M&S has been applied to virtually every aspect of an engineering systems design.

It has been shown why computer based models cannot totally remove the need to produce and test physical prototypes.

How to reduce the risk that prototypes do not pass their milestones has also been covered.

## References

[1] Sage, A. G., and W. B. Rouse, (eds.), *Handbook of Systems Engineering and Management*, New York: John Wiley, 1999.

[2] Davies, D. R., "Using Structured Modeling Strategy to Build Validated Computer Models," *Proc. 2nd T&E Int. Aero. Forum, RAeS*, London England, June 25–27, 1996, American Institute of Aeronautics and Astronautics, AIAA-96-3335-CP, pp. 25–33.

[3] Dhillon, B .S, *Engineering and Technology Management Tools and Applications*, Artech House: Norwood, MA, 2002.

[4] Fowler, M., and K. Scott, *UML Distilled: A Brief Guide to the Standard Object Modeling Language*, Reading, MA: Addison-Wesley, 1999.

[5] Kai, C. C., L. K. Fai, and L. Chu-Sing, *Rapid Prototyping: Principles and Applications*, River Edge, NJ: World Scientific, 2003.

[6] Cooper, K. G., *Rapid Prototyping Technology*, New York: Marcel Dekker, 2001.

[7] A necessarily brief outline of the main functional units of each aspect now follows.

[8] Montgomery, D. G., *Design and Analysis of Experiments*, New York: John Wiley, 2001.

[9] Coleman, H., and W. G. Steele, *Experimentation and Uncertainty Analysis for Engineers*, New York: Wiley-Interscience, 1998.

## CHAPTER 12

# Change and Future Trends

An appreciation of the elements of change in the application of SE is given in this chapter. It deals with:

- The concept of best practice operations;
- How and why systems need change;
- Technology forecasting;
- Process reengineering;
- The individual in change environments;
- Likely, near-term changes in design practice and support.

## 12.1 Improvements

### 12.1.1 Best Practice Operations

The efficiency of systems development is continuously improving as better ways to carry out the tasks are evolved. The all-important cost, time, and performance factors are, somewhat surprisingly, being optimized as a whole, for although they seem to be conflicting goals, better processes have been implemented that can improve all of them simultaneously.

The organization's chief engineer and team leaders are expected to routinely apply improvements to reduce rework, shorten delivery times, and enhance supplied performance.

The whole operation is expected to be up with the latest standards of best practice. Just what the substance is of best practice claims ranges from serious studies that compare the performance of industry sector leaders through to little more than spin statements about how an organization practices it.

The term is often bandied around as a smoke screen for poor practice! Some organizations are not prepared to divulge what makes their process best practice by asserting it is the company's proprietary crown jewel in their battle for marketplace share.

The elements of what constitutes best practice are discussed in many places [1]. One study [2] lists the key elements to be:

- Improvement in the cost, time, and performance factors on an ongoing basis;
- Closer interaction with stakeholders;
- Better use of technology for strategic advantage;

- More flexible operations giving more ownership to staff of the processes and practices;
- Continuous learning, coalition team building, and improved participation.

It is clear that these are mostly related to the systems engineering aspect of a development. Section 12.3.2 covers the basics of setting benchmarks (also referred to as baselines, or breakpoints) in best practice studies.

Throughout this book discussions have concentrated on raising design team activity to the best practice level. There is also a constant need to look ahead using that proverbial crystal ball to see what is coming that can be used to improve the overall state of best practice. This final chapter rounds out this book on that topic and how the change that accompanies best practice is managed by organizations and individuals.

### 12.1.2 How Systems Change

Three classes of observers of change are those that:

- Sense it is happening and want to be part of it;
- Sense it happening but do not want any change;
- Do not seem to notice it is occurring.

When the experience of the newly educated engineer is just beginning to grow after graduation, the changes taking place around him or her are usually not understood in a sufficiently holistic way. Changes are more likely to be seen as isolated events. As experience in contemplating what-if situations and skills at implementing innovation develop, the senior reflective practitioner better senses the whole and can see how to inject change for good. It is thus helpful to appreciate the fundamental ways in which change might arise in system behavior and practices and how some degree of look-ahead is employed.

The most widely seen mechanism of change is the steady expansion of an already started thrust. The near future in this scenario can be predicted using extrapolation of prior characteristics. Here the past trends of a practice or technology capability are plotted against time and a curve fitted to the data. This law is then used to extrapolate events to yield expectations of what can reasonably be expected to happen next.

For example, the increase in capability of semiconductor performance is well known and Moore's Law has held well for several decades. Extrapolation of the law suggests, but does not guarantee with 100% confidence, that more capability is still to come. This is evident in the ever-increasing speed of the personal computer.

Extrapolation is based on having access to a sound collection of data plus an understanding of the many factors that generate that data. It works best for small excursions into the future but becomes less reliable as the time frame is extended.

This extrapolation process can be overly stretched from a weak basis of past history and thus its use needs to be taken with caution for it is only a prediction, not a fact. One example of excessive use is the prolific use of the radioactive material half-life decay law. The observed period of the phenomenon has only been just over a century, yet it is used to date (backwards) 40,000 years or more time periods.

Existing technologies and practices based on physical materials can use this method to good effect if applied carefully. Human issues, however, are far less reliable in this regard, for they can be so volatile.

The start of the predictable kind of change is a crystal-ball mechanism for predicting the shape of things to come as a virtual implementation of a principle or method well before it can be physically built.

Ideas of what might be done are first floated by visionaries, such as the scenarios of science-fiction writers and cartoonists. They put the seeds of high-level ideas together (often not in the right relationship but nevertheless prophetical) to invent a novel means of doing something in their kind of virtual world.

In 1878 *Punch* magazine published a cartoon, shown in Figure 12.1, with a caption:

> By the telephone, sound is converted into electricity, and then by completing the circuit, back into sound again. Jones converts all the pretty music he hears during the season into electricity, bottles it, and puts it away into bins for his winter parties. All he has to do, when the guests arrive, is to select, uncork, and then complete the circuit; and there you are!

This statement is laughable in terms of how the cartoonist appears to suggest it could be implemented. However, it does make sense in terms of someone drawing on the ideas and practices of the day to invent a new application—but not at the detailed engineering level. In this case it was known in lay terms that the recently introduced telephone (by Bell from 1875 onward) could convert sound into electricity, and that electricity was indeed being stored in Leyden jars at that time.

The conversion efficiency of those early telephone units needed powerful, then nonexistent, electronic amplifiers to give workable signal/noise ratios; that did not become available until the 1920s! The Leyden jar was the first form of the modern

**Figure 12.1** *Punch* cartoon of 1878 suggesting the use of electrical music storage.

capacitor. It, however, only stored one signal element (analog at around 10) at a time, thus requiring millions of them to store the content of short string of sound signals.

Further, the method would only be feasible if the jars could be made to hold their given charge level for more than the second that such a crude capacitor exhibits.

However, the idea has been sown and would keep being refreshed in teletechniques until, finally in the 1940s, the Germans built the first field useable, wire sound recording machines.

That it is not clear how an idea could be actually engineered, or if it were even needed, is a mere incidental at the start of an idea. Some commentators suggest these cartoons were actually mocking the apparently outlandish ideas that someone had dared to suggest. This still happens!

As another example of visionary inventions, consider the evolution of television. One of the best original ideas prior to 1900 for its implementation suggested use of a mechanical scanner to transduce an image into electrical signals [3]. The development of the best early ideas for television systems has been traced to as early as 1880 [4]. The best idea, by Sutton, was sound, but it specified selenium photocells as the scanner detector. Today we know that their dynamic response time is far too long for that implementation to work but the idea had been given some dimensions and in fact a similar method was the heart of Baird's approach of the 1930s.

Another, more modern, example is seen in the development of the now ubiquitous CD-ROM technology. A small team of Philips engineers were given the apparently impossible task of creating the first optical storage disk in the early 1960s. They implemented it with a 12-inch diameter disk and a gas laser source the size of a shoebox. The key thing was that their work proved that an apparently impossible thing to design and make could actually be done. That started off progressive improvement that resulted in the almost incredible level of miniaturization and reliability in use today.

It does not seem to be that difficult to develop ideas of what might be possible one day. When and if they will happen are the hard things to predict.

The second change mechanism is the one that can confound the extrapolation method. It is the totally unexpected mutation of the current state.

Mutations are commonly found in life and are a major cause of dramatic change in system characteristics. These cannot be predicted; they just arrive. Emergent properties are in this class. What is interesting to reflect upon is that they are often so obvious only after the event. While mutations are common on the life sciences, they are rarely seen in the physical world of the technologies. They can be, however, explosive in the human operational world.

Change is a fact of life and it always has been. Managers, in particular, need to be familiar with the elements of change in their industry and with the methods of change management.

Change management can be plagued by problems arising from those in control. Some leaders are inclined take the apparently safer conservative path of decision making, following the fashion with little investigation of their own. They also often hang on too long with old methods using the argument that is has worked in the past for them.

The inertia that exists in large organizations can impede change progressing. To change the culture in a large organization requires time and considerable boldness of action by a few.

In recent times much has been made of the reengineering of organizations. Many readers, being at the receiving end of its downside, are expected to be well familiar with the processes involved. It is not unusual for several reengineering cycles to be put into place in an organization in as little as 2 to 3 years!

## 12.2 Technology Forecasting

Having seen that change mainly takes place as an extrapolation process, let us return to the issue of predicting the future technologies and practices.

Using extrapolation of sound data it seems, at first sight, reasonable to predict what services and products will be wanted, what technologies will become available, how labor will change, and even how the stock market will perform.

In the 1970s the discipline of technology forecasting emerged in many universities in support of the need for staff carrying out this role in large organizations. The mathematics supporting this developed to a very sophisticated degree being able to combine data of hundreds of statistical parameters [5, 6].

Surveys of various kinds are conducted to find out the consensus of thinking. The Adelphi technique discussed in Section 7.3 is one method used. Large organizations maintain specialist forecasting study groups.

Does it work? Some say it does, but mistakes can be made because, in spite of all of the sophistication now available, it is still based in prediction. Extrapolations and visionary technologies can be carried out with livable risk levels; it is the unexpected mutations that can seriously upset the predictions. The fall of Communism in Russia was an example of an unexpected event that had a great impact throughout the world.

Limitations of technology forecasting will always be:

- Have the right parameters been chosen for the study?
- How far will extrapolation of data hold?
- Can the predictive visions be assimilated into the hard mathematics of the processes used?
- What unforeseeable events will emerge as unpredictable events?
- How much confidence can be associated with findings?

Overall, predicting the future can be an uneasy pursuit. Some classic understatements and errors are found in the history of technology. For instance, in 1955 an eminent physicist published on his foreseeable future [7]. He wrote of the then newly discovered germanium transistor that its smallness of size and weight *might* lead to one useful development: “It is possible that a short range ‘walkie-talkie,’ light enough to be carried regularly, may in the course of a few decades replace a good deal of telephony over wires.”

He was indeed right, but he missed seeing the semiconductor's more major role in computing. At that time the best electronic computer (ENIAC) was made using thermionic tubes, the many binary units needed filling several floors of a warehouse.

Another failure to predict changes that followed was made by a major IT company which, when studying the likely uptake in the European market of the now ubiquitous automatic teller machine (ATM), came to the conclusion it would not be accepted by the public to the degree needed to support development.

Futures studies and technology forecasting are, therefore, necessary activities. Results must be used with caution. Their value is as an exercise of methodological contemplation based in plausible ideas that may well be possible if carried out. To proceed, a hard-nosed business case must be made and the level of financial risk decided. Defining the future of technology is very risky and expensive.

## 12.3 Process Reengineering

### 12.3.1 Indicators of Need for Change

Let us now delve into the change mechanism inside the organization. To be able to sense the need for change, it is necessary to understand the forces that might be at play.

What brings about organizational change? Several clear push-and-pull factors might give rise to it:

- Failure in the market is becoming apparent for a product or service (by which time, however, seeing it clearly can be too late for change to make a real difference).
- Need exists to remain competitive as other companies move on. This is a key reason for change.
- New management methods are inserted to increase the time, cost, and performance factors for a size of yield that is attractive to share holders. This should be happening for a successful operation as well as a failing one. At least 25% gains are said to be needed to provide sufficient incentive for organizations to insert major changes. Small initiatives are usually of less interest, except as ongoing contributions to process improvements.
- Wise leadership is keeping up with change when the profits are good. Perceptive management is not complacent in good times. In privately owned and other organizations the owners/leaders may well sit on the success and ride downward with it to bow out when it suits them.
- New laws and regulations dictate necessary changes to implement.
- Societal and political forces come into play.
- New potential market(s) appear for the organization due to:
  - Discovery of a new principle;
  - Release of a new technology;
  - Favorable political and economic situation;
  - Demand created by marketing.

The engineering designer may feel these reasons are somewhat removed from his or her level of influence. The design team leader, however, is likely to become involved in the managerial activity as higher management sets reengineering plans in place that they must implement.

Bearing in mind the inherently chaotic aspect of large organizations and their organizational situations ranging from, at the best, Complex-Coalition through to the worst case for management, the Complex-Coercive state (see Section 1.3.1), managers are usually facing a major challenge that has few close precedents to lean on for inspiration.

Whether they hit on the right strategy for that point in time is often a matter of chance. What transpires is partially set by luck; markets, the economic climate, and people's behavior that can wildly change the "forgiveness" factor that often masks mistakes made by managerial staff during reengineering operations.

With respect to the difficulties it is of interest to reflect on Conway's 1968 Law, from the Sperry Rand organization. It states:

> Given any design team organisation, there are classes of system design alternative that cannot be pursued effectively by such an organisation (being of the large and complex type) because the necessary communication paths, which equate to the relationships of its organisational structure, do not exist.

An organization will stamp out an image of itself in every design it produces. The larger the organization, the less flexibility it has and the more pronounced the phenomenon becomes.

There is also need to clearly distinguish between process improvement (evolutionary change) and process innovation (revolutionary change).

Many well-tried management methods are available for pacing improvements. They are published regularly as the week's bestseller, despite their usually being single intervention theme management fads that are often not transferable or sufficiently holistic.

One sound way to consider for use is the "islands of certainty" concept. Figure 12.2 is a diagrammatic representation of this methodology; an outline of that is now presented.

An overall mission statement is generated as the high-level goal of the improvement program. An example could be to increase the reliability and comfort of a passenger railway system while improving safety of use by passengers. This will be set in these forms of high-level purposeful terms, not as technical performance parameters.

Subsystem aspects of the whole are then isolated. Some of those typical of a railway system are shown as the illustration. Critical issues for each of these subsystem aspects are identified and a set of measures of effectiveness (MOE) metrics assigned to each—as discussed in Section 2.5.2. Visionary, yet realistic, end-goal values and times are suggested for each of the end-point metrics.

It is then time to carry out a baseline study to establish the current values of the chosen critical issue metrics. This is a vital and essential step. Some programs ignore baselining for fear of having to reveal poor data to higher management and because it consumes considerable resources. Merely guesstimating the starting point values,

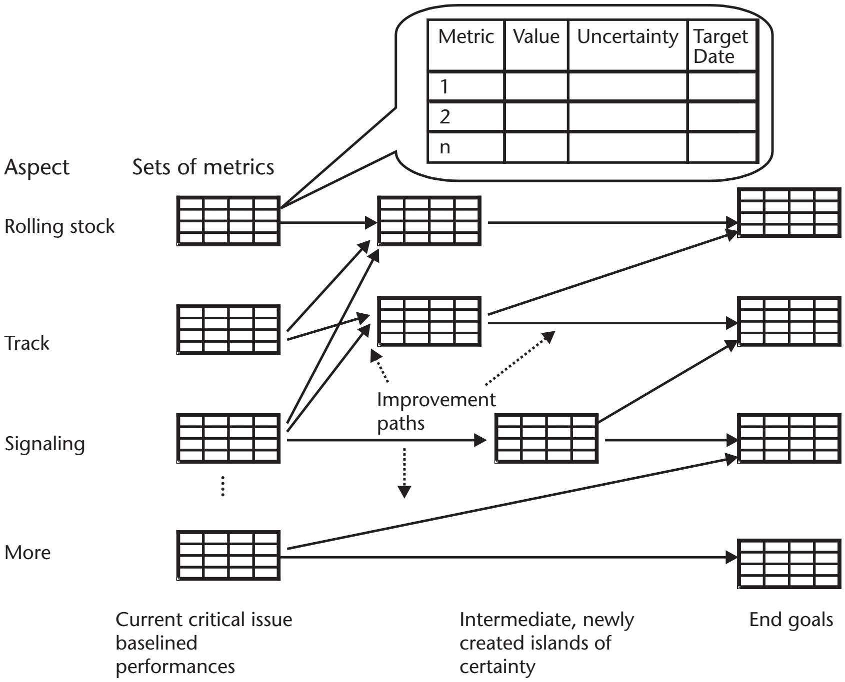


**Figure 12.2** Process improvement using "islands of certainty."

or not providing them, is a bad practice because true comparisons cannot be made and the extent of improvement is not verifiable.

For each metric value it is necessary to allocate an uncertainty bound. Having a nominal value is insufficient in itself, for the spread of values may be far too wide to allow control.

That formative work all in place, the next step is to place target islands of certainty along the route from the start to the end goals. Each Island provides a target that, when reached, can be relied upon by the other aspects of the improvement program. As each island state is achieved, the process improvement changes needed to reach it are taken into standard practice. In this way best practice evolves contributing gains over time.

When all metrics are improved on time, to the end goals set, the target improvement state will have been reached.

The method provides targets for designers and managers to strive and provides data on how well the improvement program is progressing at any time.

### 12.3.2 Benchmarking

It is evident that an early step to improvement must be to know how good the process is at the current time. One method for doing this has variously been known over the past few decades as benchmarking, baselining, or break-pointing. Each of the parameters of this exercise "Represent the achievement or excellence in one of the facets of value" [1].

The EU Benchmarking activity [8] states that the application of benchmarking involves four commonsense steps:

- First, understand in detail your own processes.
- Next analyze the processes of others.
- Then compare your own performance with that of others analyzed.
- Finally, implement the steps necessary to close the performance gap.

Several levels of evidence discovery in benchmarking activity can be employed [9]:

- Internal (a starting point for learning that is low cost, simple to do, and essential to learn how to conduct those following);
- External, competitive (examination of the products of processes of others, which opens the mind and may reveal the state of the competition);
- External, compatible industry (cooperation with other companies will be easier if the products are not directly competitive, yet similar in nature);
- External, generic transindustry (these include many disparate products with features of relevance);
- Combinations of the above.

Carrying out benchmarking exercises can bring a mutual advantage to the industry at its national and international enterprise level; this has encouraged organizations to cooperate in benchmarking. All involved can potentially gain from being within a stronger sector.

A simple way to make the comparisons needed is to use the industry intercomparison, also called industry monitor, methodology.

In this a neutral body (such as a government agency, professional society, or university group) takes on the task of signing in membership of cooperating companies for a study. They work together to establish appropriate segments and metrics. A general survey instrument is generated that requires each member to submit their specific values for the metrics, with uncertainties assigned, for the organizer's eyes only. All provided data is highly confidential from other members of the group and elsewhere.

This data is processed to provide generic statements of the mean and spread of values of the sets of metrics.

Each member subsequently receives the collective survey mean values and spreads (these are not sensitive parameters) plotted along with their own data. This allows them to gauge their performance against that of the whole group.

The weakness in this method is that many potential members do not trust the confidential agreements, feeling that their performance data will leak to competitors.

Benchmarking will involve data transfer between organizations that can impinge on moral, ethical, and legal issues. Codes of practice exist for benchmarking activity, that of the American Productivity and Quality Center (APQC) being one to view to appreciate the issues [10].

This code lays down eight principles to be addressed during a benchmarking exercise. These are, in abbreviated form:

- *Legality:* Stick to lawful and ethical methods for gathering information.
- *Exchange:* Give information back as good as you get; be honest and avoid misunderstandings.
- *Confidentiality:* Do not disclose information without permission.
- *Use:* Information gained is not to be used for other than agreed purposes without consent.
- *Contact:* Maintain agreed points of contact and do not disclose names.
- *Preparation:* Prepare questionnaires and send them in advance to minimize time needed by the other party.
- *Completion:* Follow through to agreed timetables.
- *Understanding and action:* Treat the benchmarking partner as you would wish to be treated.

The use of benchmarking is spreading, with the EU being slower to adopt the methods than the United States. Many well-developed accounts are available [11–14].

Software system baselining is covered by numerous documents available from the Software Engineering Institute (SEI) [15]. Using "benchmarking" as a keyword, many sources of information are available via the Internet.

## 12.4 The Individual and Change Management

Generally reengineering programs are driven by the senior staff of organizations and thus it is will be as a directive at the designer's level of contribution.

On the other hand, ideas for doing things better at the design and manufacturing level are often realized by the individual who is immersed in the practicalities.

Sometimes the parent organization is unable or unwilling to accommodate the entrepreneurial drive of those staff for the following reasons:

- They are not doing their assigned job.
- Risks from having their new ideas floating around inside the main line of thinking are not needed.
- Insufficient funding is available to assist development of new ideas.

Often the outcome of such negativity is that staff members resign and set up in partial competition with the organization. Often the whole team leaves!

To prevent the risk of this kind of competition and to retain the ideas, organizations will sometimes seize on the entrepreneurial opportunity assisting its leaders to set up a new, small, reasonably autonomous operation. This will be allocated its own budget according to a well-developed business plan. Means will be used to maintain an overall controlling link, such as it being a subsidiary company.

Process improvement is an ongoing activity. Changes in how things are engineered and made are not new; it is the pace and openness of reporting that are different today. Design team members need to keep up with the issues of this book for the ways and means of design are constantly being upgraded.

It has been shown in this book that SE is not just for the senior engineering staff to follow; its practices are relevant to the design role as well. Keeping up takes valuable time that employers are not always willing to make available to its staff.

It is common practice not to release key staff for training for that will retard their work program. Some organizations do provide in-service training within their staff development policy, but the amount given (a few days per year) is often insufficient to master the many changes taking place.

The result is that the individual detail design engineer needs to consider making a personal sacrifice to obtain worthwhile advancement. Sensing the timing of key breakpoints in the sector's changes can be material to career advancement [16–18].

SE practice and theory is well served by the International Conference on Systems Engineering (INCOSE). Membership is not expensive and entry is freely available. It is suggested that membership of INCOSE be seen as a second membership to that needed for a person's foremost professional pursuit.

Within INCOSE a strong technical community is formed of technical committees that are divided into working groups and interest groups. These are found listed on the Web site of INCOSE [19] along with their charters and members.

INCOSE organizes annual conferences that are attended by many hundreds of delegates. The 400 or so papers presented each time are packed with SE knowledge of all types. The January International Workshop is another regular event. This weeklong activity is where the many technical committees and working groups come together for face-to-face consolidation and work on their ongoing developments.

The *SE Journal* is the primary journal publication of INCOSE. A regular newsletter, *Insight*, is sent to members; it publishes news and articles on SE and SE events.

The best way to enjoy the benefits of this organization is to join a suitable technical committee activity as that rapidly introduces one to the governance, programs, and people who pace along the global SE.

Additionally to the broad-based SE needs for self-advancement, it will be necessary to keep up with specialty areas such as safety, reliability, modeling, and tools. Again attendance at suitable conferences, short courses, and meetings is a good way to pump up the personal stock of knowledge.

Books on SE appear at around three or so per year. They duplicate little material, being more about the experience of the author's ideas on interpreting SE.

A casual reading of the latest relevant standards documents is needed. SE is now supported by many of these. They are packed with information that may be useful to improvement of detail design activity in its increasingly holistic context.

## 12.5 Likely Changes in the Foreseeable Future

To round out the contents of this book, it seems appropriate to set down some trends as they are appear to the author at the time of writing. Dangerous to predict perhaps, but hopefully stimulating!

### 12.5.1 SE as a Discipline

Academic engineering teaching leadership at large has been slow to recognize the importance of the breadth and scope of SE needed to be a good engineer. SE schools are rare and mostly have only a tenuous hold on their resources position.

Unfortunately, the deeper learning and research contributions needed for career advancement on the campus go against the development of strong academic support evolving for SE. It has yet to establish itself as a suitable campus discipline in a climate that attracts only the specialty, in-depth kind of scholarship.

A soft, multidepartmental approach is needed to attract academia to develop strong SE schools that would assuredly deepen the understanding of its content if more recognition where afforded to the topic.

Industries do not help that much since they and academia have rarely found how to provide sufficient mutual gain from the injection of greater industry commitment.

The SE teaching movement can be traced to serious beginnings in United States in the 1960s [20].

That first wave of interest did not break into traditional engineering groupings of the campus at large. Today SE is still rarely taught as a whole undergraduate degree. It is usually offered as a postgraduate program that, more often than not, is led by industry experienced persons, not by career academics. These courses thus tend to not stimulate the deep knowledge development that career scholarly academic underpinning supports, as it has in the mainline detailed engineering disciplines like electrical engineering.

There is little evidence to show that this situation is changing. Persons championing SE schools on a few campuses of the technological nations are still pioneers fighting resource and intellectual recognition battles.

Training—some of what they do could be classed as education—is being left to industry to provide, for they, seemingly being short-term driven, do not show that they appreciate the power of long-term academic research and teaching. Universities have been established by major SE corporations. These are not well accepted into the academic society, but perhaps they are the result of academia not being able to make the necessary change in its narrow disciplinary thinking.

Detail design engineers will, therefore, continue to need to seek out specialist courses to gain the new knowledge needed, to attend profession society meetings, and to read many journals and books.

What is evident, however, is that some undergraduate engineering programs are being given new courses/subjects that expose the potential graduate to the holistic viewpoint and some practices of SE at work.

### 12.5.2 Modeling in Design

Models in computers are now firmly part of normal engineering design practice.

By way of contrast, the concept of downloading applications to feed modeling work was still in its infancy in the 1980. Using extrapolation, it is to be expected that continuous development of tool suites and tool-based thinking in design work is here for some time to come.

Well-integrated toolsets are gradually appearing and some systems developments are now close to being totally set up in the virtual computer world. The Joint

Strike Fighter project used a flight simulator of incredible sophistication to learn how to tune the flight control software—before it had made its maiden flight.

The supply of models of a delivered system to the customer can be increasingly expected to drift into standard practice. These will be running over the whole life of the system continually being upgraded. This will mean even shorter design times for systems that are evolving to near optimal states.

Capability in using tools and models will become the main forte of the best practice designer. The application of mathematics will slide away to the specialist and be of less importance to the engineer, as it has in statistical application, IC, and plant control engineering. The hard-nosed employer is little interested in staff being able to derive models from first principles. What is needed is proficient and accurate use of well-developed models to reach engineering solutions, thus satisfying CTP factors.

### 12.5.3 Staffing

Reducing numbers of detailed specialist designers will be in the cards. Tools will take in much of their expertise. What is needed is a broader education of engineering designers that assists them to cope better with the many SE issues as are given here. TCP factors, laws, globalization, and societal demands all will impact more on the flexibility needed in the detail designers remit. He or she will increasingly be required to cover the broader issues of systems design.

### 12.5.4 Computing

Distributed, concurrent working will continue to grow in sophistication and extent of application. Broadband Web operations will spread, allowing the small team to work and interface better alongside the major developer's operations.

The power-to-cost ratio of computing systems will continue to increase giving designers more access to, and use of, powerful models and tools.

Increased use of AI methods will make tool use faster and (apparently) more intelligent. Image searching, using specialist area ontologies (sets of rules about images for a topic), will soon join symbol-based searching on the Web, thereby allowing images to be located easily.

Information needed for a design will become available from well-organized publishing sources. The hard-copy filled library will fade out to be replaced by the virtual library that is visited from anywhere.

Support knowledge for design will increasingly be better presented, cover more topics, and be more efficiently located, accessed, and used.

### 12.5.5 Enlightenment

Possibly the greatest impact of this book will be to open the mind to SE thinking in the future activity of the reader. Experience of SE thinking and practice being onboard will constantly reveal where much of today's office, design, and management practices are less than efficient.

The main defective practices that can be expected to be now recognized as daily activity at work takes place are:

- Poor inheritance of prior knowledge in projects;
- Creation of orphan systems that have little history that can be used to support or reuse them;
- Lack of SE thinking as groups go about their own work with insufficient interfacing to the work of others that are key to their mutual success;
- Insufficient allocation of front end loading resources to keep late errors under early control;
- Excessive rework taking place due to deficiencies in the holistic aspect of planning;
- Much of the work done is not used due to lack of decisive decision making and a sound SE thinking foundation of what should have been done;
- Insufficient support and encouragement for lifelong education of staff by an employer;
- Failure by people to report difficulties early enough to allow for less costly correction;
- Humans still seen as reductionist machines in systems development when their human characteristics can be a key to success.

The quotation (see Figure 2.3) from some many years ago still sums it up: "A Systems Engineer is a good engineer, only more so."

This book provides information on the "more so" aspect of being that better engineer.

## 12.6 Summary

This final chapter took the reader from setting up better practices based in SE ideas to the changing issues that impact the work of the designer. The concept of best practice operations has been outlined. How and why systems methodologies and practices need to change has been covered to assist understanding of why relearning is constantly needed. The nature and scope of technology forecasting has been presented. Process reengineering practices are summarized to show how methodical processes can gain progressive advantage. The place of the individual in the change environments was the subject of another section. Finally the likely, near-term trends in design practice and support are summarized.

## References

[1] Sage, A. G., and W. B. Rouse, (eds.), *Handbook of Systems Engineering and Management*, New York: John Wiley, 1999.

[2] Dertouzous, M. L, R. K. Lester, and R. M. Solow, *Made in America: Regaining the Productive Edge*, Cambridge, MA: MIT Press, 1989.

[3] Sydenham, P. H., *Measuring Instruments: Tools of Knowledge and Control*, Stevenage, England: IEE and Peter Peregrinus, 1979.

[4] Sheirs, G., "Historical Notes on Television Before 1900," *SMPTE J.*, Vol. 86, 1977, pp. 129–137.

[5] Porter, A. L, et al., *Forecasting and Management of Technology*, New York: Wiley-Interscience, 1991.

[6] Millett, S. M., and E. J. Honton, *A Manager's Guide to Technology Forecasting and Strategy Analysis Methods*, Columbus, OH: Battelle Press, 1991.

[7] Thomson, G. P., *The Foreseeable Future*, Cambridge, England: Cambridge University Press, 1955.

[8] EU Benchmarking Program, http://www.benchmarking-in-europe.com/1024.htm.

[9] Harrington, H. J., and J. S. Harrington, *The Complete Benchmarking Implementation Guide: Total Benchmarking Management*, New York: McGraw-Hill, 1996.

[10] American Productivity and Quality Center, http://www.apqc.org.

[11] Camp, R. C., *Benchmarking: The Search for Industry Best Practices That Lead to Superior Performance*, New York: ASQ Quality Press, 1989.

[12] Drezner, J. A., and R. A. Krop, *The Use of Baselining in Acquisition Program Management (MR-876)*, Los Angeles, CA: Rand Corporation, 1977.

[13] Johansson, H. J., et al., *Business Process Reengineering: Breakpoint Strategies for Market Dominance*, New York: John Wiley, 1993.

[14] Spendolini, M. J., *The Benchmarking Book*, 2nd ed., New York: AMACOM, 2003.

[15] Software Engineering Institute, http://www.sei.cmu.edu.

[16] Sherwood, A., *Breakpoints: Making Career Stages Work for You*, New York: Doubleday, 1986.

[17] Aucoin, B. M., *From Engineer to Manager: Mastering the Transition,* Norwood, MA: Artech House, 2002.

[18] Eisner, H., *Reengineering Yourself and Your Company: From Engineer to Manager to Leader*, Norwood, MA: Artech House, 2000.

[19] International Conference on Systems Engineering, http://www.incose.org.

[20] Whole issue reviews systems engineering from many viewpoints, *Engineering Education*, April 1970.

# List of Acronyms

| | |
|---|---|
| **2D** | two-dimensional |
| **3G** | third generation |
| **ALARP** | as low as reasonably practicable |
| **AOB** | any other business |
| **APQC** | American Productivity and Quality Center |
| **ASIC** | application-specific integrated circuit |
| **ATE** | automated test equipment |
| **ATM** | automatic teller machine |
| **BOK** | Body of Knowledge |
| **CAD** | computer-aided design |
| **CAD** | computer-assisted drafting |
| **CASE** | computer-assisted software engineering |
| **C-C** | Complex-Coercive |
| **CD-ROM** | compact disk |
| **CEO** | chief executive officer |
| **CFD** | computational fluid dynamics |
| **CI** | critical issue |
| **CM** | configuration management |
| **CMM®** | Capability Maturity Model® |
| **CMMI®** | capability maturity model integration® |
| **CNC** | computer numerical control |
| **ConOps** | concept of operations |
| **COTS** | commercial-off-the-shelf |
| **CRT** | cathode ray tube |
| **CTP** | cost, time, and performance |
| **CV** | curriculum vitae |
| **DAS** | data acquisition system |
| **DDP** | device description profile |
| **DID** | data item description |
| **DOD** | Department of Defense |
| **DOE** | design of experiments |
| **DNU** | develop new products |
| **DRU** | design review unit |

| | |
|---|---|
| **EDA** | electronic development activity |
| **EMI** | electromagnetic interference |
| **ESM** | engineering safety management |
| **FAQ** | frequently asked questions |
| **FCT** | fast cycle time |
| **FE** | finite element |
| **FEA** | finite element analysis |
| **FEL** | front-end loading |
| **FEM** | finite element methods |
| **FFD** | functional flow diagram |
| **FL** | fuzzy logic |
| **FTP** | File Transfer Protocol |
| **GaAs** | Gallium Arsenide |
| **GAMAB** | globalement au moins aussi bon |
| **H&SW** | health and safety at work |
| **HDD** | hard disk drive |
| **HIL** | hardware in the loop |
| **HLA** | high level-architectures |
| **HR** | human resources |
| **HRM** | human resources management |
| **IC** | integrated circuit |
| **IEEE** | Institute of Electrical and Electronic Engineers |
| **INCOSE** | International Council on Systems Engineering |
| **IP** | intellectual property |
| **IPPD** | integrated product and process development |
| **IPT** | integrated product team |
| **ISO** | International Standards Organization |
| **ISP** | Internet service providers |
| **IT** | information technology |
| **ITEAP** | integrated test and evaluation and acceptance plan |
| **IV&V** | independent verification and validation |
| **JIT** | just in time |
| **JPL** | Jet Propulsion Laboratories |
| **KB** | kilobytes |
| **KBS** | knowledge-based system |
| **KISS** | keep it simple stupid |
| **KPI** | key performance indicators |
| **LAN** | local area network |
| **MEM** | minimum endogenous mortality |
| **MIL** | man in the loop |
| **MOE** | measures of effectiveness |

| | |
|---|---|
| **MOU** | memorandum of understanding |
| **MTBF** | mean time between failure |
| **OEM** | original equipment manufacturer |
| **OT&E** | operation test and evaluation |
| **PAT&E** | production acceptance test and evaluation |
| **PC** | personal computer |
| **PCB** | printed circuit board |
| **PLC** | programmable logic controller |
| **PM** | project management |
| **PMAP** | project performance maturity assessment plan |
| **PMBOK** | project management body of knowledge |
| **PMI** | Project Management Institute |
| **PMP** | personal maturity plan |
| **QFD** | quality function deployment |
| **R&D** | research and development |
| **R&M** | reliability and maintenance |
| **RAM** | random access memory |
| **RF** | radio frequency |
| **RH** | relative humidity |
| **R&D** | research and delevelopment |
| **R&M** | reliability and maintenance |
| **RMS** | root mean square |
| **SD** | systems dynamics |
| **SDR** | systems design review |
| **SE** | systems engineering |
| **SEBOK** | systems engineering body of knowledge |
| **SEI** | Software Engineering Institute |
| **SE-CMM** | Systems Engineering Capability Maturity Model |
| **SEI** | Software Engineering Institute |
| **SEMP** | systems engineering management plan |
| **SEP** | system engineering process |
| **SoS** | systems of systems |
| **SSM** | soft systems methodology |
| **SSS** | system/subsystem specification |
| **SU** | simple unitary |
| **SUT** | system under test |
| **T&E** | test and evaluation |
| **TEMP** | test and evaluation master plan |
| **TLMP** | through life management plan |
| **TLV** | threshold level value |
| **TOP** | triangle of pairs |

| | |
|---|---|
| **TPM** | technical performance parameter |
| **UKMOD** | UK Ministry of Defence |
| **UML** | Unified Modeling Language |
| **USB** | universal serial bus |
| **V,V&A** | verification, validation, and accreditation |
| **WWII** | World War II |

# About the Author

Dr. Peter H. Sydenham, B.E. (Hons.) and M.E., University of Adelaide, Australia, and Ph.D. and D.Sc., University of Warwick, United Kingdom, began his career through an electrical trades apprenticeship. He subsequently held engineering, scientific, and academic posts in defense engineering science and also in applied geophysics before joining the University of South Australia as the inaugural professor and head of the School of Electronic Engineering in 1980.

In 1992, he cofounded the Australian Centre for Test and Evaluation (ACTE) in the chair of systems engineering and evaluation of the Faculty of Information Technology.

Dr. Sydenham is a director of Global Systems Engineering Consulting Pty Ltd, work that requires him to commute between Australia and the United Kingdom. As a visiting senior research fellow at the University College London, he assisted the teaching of systems test and evaluation and thesis supervision. He lectures on systems engineering and evaluation to U.K. companies. His major long-term activity is as a coeditor-in-chief of MeasureMentor, an on-line knowledge service on measurement systems.

He has published numerous books, primary papers, consulting reports, and technical articles on measurement systems, history of technology, instrument systems design, systems test and evaluation, and general science. He holds, or has held, posts of many learned journals and societies. His second-higher doctorate was awarded for contribution to the structure of measurement systems and its efficient engineering. In recognition of his contributions in T&E, he was presented with the Richard G. Gross award of the International Test and Evaluation Association (ITA) in the United States.

# Index

# Recent Titles in the Artech House Technology Management and Professional Development Library

Bruce Elbert, Series Editor

*Advanced Systems Thinking, Engineering, and Management*, Derek K. Hitchins

*Critical Chain Project Management*, Lawrence P. Leach

*Decision Making for Technology Executives: Using Multiple Perspectives to Improve Performance,* Harold A. Linstone

*Designing the Networked Enterprise,* Igor Hawryszkiewycz

*Engineering and Technology Management Tools and Applications*, B. S. Dhillon

*The Entrepreneurial Engineer: Starting Your Own High-Tech Company,* R. Wayne Fields

*Evaluation of R&D Processes: Effectiveness Through Measurements*, Lynn W. Ellis

*From Engineer to Manager: Mastering the Transition*, B. Michael Aucoin

*Introduction to Information-Based High-Tech Services,* Eric Viardot

*Introduction to Innovation and Technology Transfer,* Ian Cooke and Paul Mayes

*ISO 9001:2000 Quality Management System Design,* Jay Schlickman

*Managing Complex Technical Projects: A Systems Engineering Approach,* R. Ian Faulconbridge and Michael J. Ryan

*Managing Engineers and Technical Employees: How to Attract, Motivate, and Retain Excellent People,* Douglas M. Soat

*Managing Successful High-Tech Product Introduction,* Brian P. Senese

*Managing Virtual Teams: Practical Techniques for High-Technology Project Managers,* Martha Haywood

*Mastering Technical Sales: The Sales Engineer's Handbook,* John Care and Aron Bohlig

*The New High-Tech Manager: Six Rules for Success in Changing Times,* Kenneth Durham and Bruce Kennedy

*Planning and Design for High-Tech Web-Based Training*, David E. Stone and Constance L. Koskinen

*Preparing and Delivering Effective Technical Presentations, Second Edition,* David Adamy

*Reengineering Yourself and Your Company: From Engineer to Manager to Leader,* Howard Eisner

*Running the Successful Hi-Tech Project Office,* Eduardo Miranda

*Successful Marketing Strategy for High-Tech Firms, Second Edition,* Eric Viardot

*Successful Proposal Strategies for Small Businesses: Using Knowledge Management to Win Government, Private Sector, and International Contracts, Third Edition,* Robert S. Frey

*Systems Approach to Engineering Design,* Peter H. Sydenham

*Systems Engineering Principles and Practice*, H. Robert Westerman

*Team Development for High-Tech Project Managers*, James Williams

For further information on these and other Artech House titles,
including previously considered out-of-print books now available through our
In-Print-Forever® (IPF®) program, contact:

Artech House
685 Canton Street
Norwood, MA 02062
Phone: 781-769-9750
Fax: 781-769-6334
e-mail: artech@artechhouse.com

Artech House
46 Gillingham Street
London SW1V 1AH UK
Phone: +44 (0)20 7596-8750
Fax: +44 (0)20 7630-0166
e-mail: artech-uk@artechhouse.com

Find us on the World Wide Web at:
www.artechhouse.com