Installing IEC 61508 and Supporting Its Users - Nine Necessities

Felix Redmill
London, UK
Felix.Redmill@ncl.ac.uk

This was an invited paper, given at the Fifth Australian Workshop on Safety Critical Systems and Software, Melbourne, Australia, 24 November 2000

Abstract

The international safety standard, IEC 61508, presents several challenges to its users - who are often not familiar either with safety engineering and management or with introducing a new standard.

This paper first explores the background to the difficulties that companies experience in using the standard. It then discusses the difficulties that the standard poses, in the context of how a company needs to respond to them. It defines nine principal requirements for installing the standard and supporting its users, and shows that the principal responsibilities - for acquiring knowledge and understanding and taking action - fall on senior management. It turns out that the nine necessities are not unique to this standard but are fundamental to the installation and support of any new tool.

1. Introduction

During the period 1998 - 2000, the seven parts of the international safety standard, IEC 61508 [1, 2], were ratified. During that time there have also been many attempts to use the standard, and the available evidence suggests that these have met with difficulties. Even attempts to read and understand the standard seem to have had a low success rate.

The standard contributes to these problems. For example, it is based on a number of technical principles that are new to many of its readers; it implies more than it states, so that readers are unsure of the extent of its requirements; and it does not introduce itself either fully or clearly, with the result that readers do not understand the context of the standard's requirements prior to being called on to implement them.

But the unfamiliarity and imperfections of the standard cannot be used as an excuse for bad safety engineering. Unfamiliarity must be grappled with. Imperfections must be understood and compensated for. With safety-related systems being produced and operated in numerous industry sectors, a standard on good safety engineering is required, and IEC 61508 has been internationally accepted as such a standard. A new standard in which all the known deficiencies are resolved could not be produced overnight, and even if it were, it would be found to contain other, unforeseen problems. Company management must understand the problems and deal with them. Not to do so, and yet to attempt to install a substantial tool like IEC 61508, is to squander human resources, money, and time. To many companies, the standard poses the problem that it is difficult to understand and use. The response needs to be, not to use it badly, but to learn to use it well.

If a company needs to change its practices to adhere to IEC 61508, the standard has strategic implications on that company. Moreover, effective installation and use of the standard requires strategic decisions to be made and strategic plans to be formulated and put into action. So implementing the standard requires knowledgeable and committed involvement of senior management.

Whereas this paper discusses some of the difficulties that the standard poses, it does so in the context of what a company needs to do in order to achieve effective installation and use.

Indeed, the main purpose of the paper is to define the principal requirements on a company, and in

doing so it identifies nine 'necessities' that must be in place. These range right across the company. The first eight define what is required, and, recognising that they amount to the need for a coordinated infrastructure, and that such a thing does not occur without planning, a ninth necessity is defined as putting the infrastructure into place.

The paper is not a textbook. It does not provide instructions on all that should be done or on how it should be done. Rather, it attempts to show that the installation and use of a standard (or any other tool) should be considered a process and defined and managed as such, and it offers guidance on how a company should tackle the process. What are emphasised are fundamentals like knowledge and understanding. 'Come on,' some will say. 'Of course we need to know things. We know that. But tell us what to *do*.' But even though the dissenters know *that*, they have not gone out and acquired the knowledge, so they have no basis for understanding - with the consequence that they are not controlling the standard's use. The obvious is often neglected - and this is, or should be, well known, for industry is littered with expensive tools which either lie on shelves like children's discarded toys, or are misused to costly effect, because no one took the trouble to learn about them. Yet, history repeats itself, and IEC 61508 is testimony to that. So this paper emphasises knowing and understanding, showing that their acquisition is the responsibility of senior management. The paper offers advice on how the knowledge and understanding should be applied, but it is beyond its scope to explain in detail every step that management should take. When knowledge and understanding abound, there should be no need for a paper on what needs to be done.

The next section offers an experience-based view of the ways in which companies have approached the new standard. Section 3 presents the initial eight 'necessities' and Section 4 the ninth. Then, Section 5 offers a discussion of what the necessities imply.

2. Background To Use of the Standard So Far

Some companies - usually large ones - are motivated to use IEC 61508 because of their knowledge of the standard's influence when in its draft stages. They are aware that in the safety community the standard is considered to be important, and they believe that it will dictate the trend of safety engineering. So they want not only to improve their methods in line with what they suppose to be current good practice, but also to be able to claim adherence to a standard that will give them credibility - and one which may even be required for basic acceptance - in the marketplace.

Frequently this awareness does not permeate the entire company. Often it is quite usual for middle management to leave the acquisition of information about the standard to working-level engineers. In some cases, this may be adequate for limited use, but, given the standard's considerable scope, in both its use and its implications on the company, this is irresponsible and dangerous.

How can there be confidence that there are no misunderstandings of what the engineers believe they have learned? To whom do they turn when they need help in interpreting parts of the standard? Who decides which parts of the standard are applicable in a given case? The standard is so large that in any project both selection of what is relevant and tailoring to local needs are essential, but in no case of my experience has careful selection been carried out and in no case has tailoring of the standard been done.

Often there seems to be no systematic recognition that these issues are problematic, and the implicit solutionis an attempt to apply the standard's principles without attending to the standard wholesale. But this throws up two significant problems. First, the principles are seldom well understood - in particular, safety integrity levels (SILs) are confusing, and the great and often disproportionate emphasis placed on them can result in their causing more problems than they solve.

The second major problem is that the standard's technical principles do not explicitly point to all that is required for good safety engineering: for example, there is no explanation of putting a safety management system in place or for preparing a safety argument to demonstrate the achievement of the required risk reduction. Casual or uninformed application may omit these and, with management not participating fully - and sometimes not at all - in the implementation and use of the standard, they may not be considered until the time of assessment, when their absence can have serious and costly consequences. The required level of safety may be achieved, but the second goal of safety engineering

is not met - it cannot be demonstrated to have been achieved.

The above observations are of activities in companies, mostly larger companies, in which there had previously been an awareness of IEC 61508. But many companies, perhaps the majority, which have tried to understand the standard had no previous knowledge of it. Such companies are often small, with a management team that is concerned with production and selling rather than with changing practices to accord with new standards. They are not attracted to a seven-part four-hundred-page document which to them is not only difficult to read but also obscure in its purpose and of dubious advantage. From what they hear, it requires them to change the way they do things, but they can see no reason for this as they have been making their product for many years and its safety has never been in question. The only reason that they feel obliged to find out about the standard is that their customers are calling on them to adhere to it.

Typical examples of such companies are those whose products, until recently, have been based entirely on electromechanical components, but now include programmable chips. Their software expertise is small and may consist of a single 'software engineer' who is often a writer of code rather than an engineer. Often the software is inadequately documented, there are no records of the tests carried out, and there is no evidence of validation. In the past, safety-engineering techniques have not been used, and product safety has been assumed to be implicit in reliability. Moreover, and importantly, the lack of good software engineering principles and practice means that there is a large gap which needs to be filled before any new safety engineering practices can be effective. Given the limited resources of such companies, filling this gap is likely to be a difficult process - improving quality in software development has proved to be dependent not only on developers learning new skills and techniques but also on the commitment of knowledgeable management.

At first the suggestion (or demand) that such companies should adhere to IEC 61508 may be considered an annoyance. When the document is to hand, its size turns annoyance into disbelief and anger. And when those in the company discover the standard's message, either by reading parts of it or by hearsay, the anger turns to fear and threat. If their slim understanding is correct, they believe that they will have to introduce a whole range of new practices or go out of business. Indeed, their perception is that if they cannot prove that their current products meet the standard - and they recognise that they may not be able to do this - they may go out of business anyway.

But their knowledge of risk analysis and the other technical requirements of safety engineering is small. Their understanding of what it takes to introduce a new standard, new practices, and, indeed, a safety management system, is likely to be negligible. If they understand the extent of their problems, they are bewildered and overwhelmed. If they do not understand the extent of their problems, as many do not, they may feel bewildered and overwhelmed anyway, but with the added handicap of unawareness. The management of many such companies is, understandably, less interested in introducing the standard than in being seen (or thought) to adhere to it.

The problems of the two types of company discussed above are similar, though those of the latter group are deeper and more difficult to resolve. The smaller companies have fewer managers (who are often less committed to the standard), a smaller knowledge base, fewer (if any) expert staff, and less flexibility in making time available for training and attending discussion seminars. Yet, for any company wishing to employ the standard effectively, the requirements are the same, even though the degrees of difficulty in meeting them are different for the various types of company.

The requirements are not only for installing the standard in the first place but also for supporting its users and ensuring its continued effectiveness. The nine fundamental 'necessities' are both managerial and technical, and experience gained from a number of perspectives suggests that the problems being experienced by all types of company result from a lack of one or more of them - or, at least, can be framed in terms of them.

To say that the problems are caused by a lack of one or more of the necessities does not mean that users of the standard or their management are invariably culpable. In many cases they are, but in many respects the standard itself has contributed to the difficulties, for example by its size, its architecture, its failure to introduce itself adequately, and the fact that it simultaneously introduces not one but a number of principles that are unfamiliar to its users.

The next section introduces the first eight necessities and discusses the problems thrown up by the standard in the context of them. The following section introduces the ninth necessity.

3. The First Eight Necessities

3.1. Understanding the Standard's Purpose and Scope

For any initiative to be effective, it needs to be the subject of strategic thinking. Any tool - and the standard is a tool - must be applied within its intended scope and for a purpose to which it is suited. For this to be done, management need to understand such fundamentals as the standard's intended purpose and scope. Does it apply to this company? Even if it does, do we want or need to use it? Is its use essential in order to satisfy our customers, or the regulators? If not, should we use it anyway? If we do, should we apply it to all our projects, or products? If not, to which is it appropriate?

If the standard is eventually applied effectively, it will generate a culture - a safety culture - in which risk-based thinking dominates. Then, its processes will be applied to all projects and products, even if adherence to its clauses is not required. But, to begin with, a proper appreciation needs to be developed for when, how, and to what it should be applied.

To those with an intimate knowledge of the standard, asking such questions may seem trivial. But those who are not so familiar with it, and particularly those who are being shocked into using it, would do well to pause and ask - and answer - them. Only then will they be likely to apply the standard correctly. Such questions are essential to defining the context of the standard's use and are therefore strategic in purpose. They need to be addressed by senior management.

Unfortunately, many readers do not easily derive answers to such questions from the standard. Although Part 1 starts with an Introduction followed by a clause on Scope, readers seem not to achieve a clear understanding of the standard's intention from these. Many readers come to the standard out of necessity rather than with enthusiasm, and a more reader-friendly and informative introduction, perhaps with diagrams, would be useful. A simple but comprehensive and well written introduction could still be made available, free to all who want to find out about the standard. It could be placed on the internet as well as being made available on paper.

But managers who want their companies to use the standard, or want to know if they should, would do well not to wait for such formal guidance. They need to seek advice where they can. They need to pose the right questions and may need help in doing so. And they will almost certainly need help in finding answers in which they can have confidence. A strategic approach is required, and they should not abdicate or delegate this responsibility.

Taking a strategic approach to introducing the standard is not a nicety. Effective use will require not only new project activities but also new business processes. It will demand new knowledge and skills and impose new responsibilities, and it will require these to be integrated across new organisational structures. In this respect IEC 61508 is not merely a document that tells people what to do; its strategic implications need to be understood by senior management.

3.2. Understanding the Content of the Standard

Within the broad scope of its application, there are the detailed clauses of the standard. These range across the entire system life cycle and address all aspects of safety, from initial hazard identification to independent safety assessment. Some are normative (must be adhered to, if relevant) and others informative. To plan the use of the standard, it must be determined which clauses are relevant to the case in hand, and for this all the clauses must be understood. Every clause states a requirement, and if the requirements are to be discharged they must be understood in detail.

Thus, the standard needs to be understood not only at the strategic level (see the previous section) but also at the planning and application levels of a business. The large size, the breadth of scope, and the unfamiliarity of the standard suggest that acquiring this knowledge and understanding is likely to require more than mere reading. In most cases courses are essential. But a course does not make someone an expert, and there will be a continuing need for the resolution of queries, the discussion of anomalies, and the reassurance of staff who may lack confidence. Provision should be made for

support of the staff who will be expected to use the standard.

Further, to speak of 'users' of the standard may suggest staff who work from the document, clause after clause. But any one clause may require an extensive process, such as risk assessment, to be executed. This implies that the process must be defined and put in place, the staff trained and managed, and appropriate quality assurance procedures instituted. Thus, using the standard will involve numerous people, carrying out various related tasks that must be coordinated, with many of the tasks requiring professional judgement that depends on knowledge and experience. The planning of this requires a thorough understanding of the standard's requirements.

3.3. Knowing How to Apply the Standard

Even when there is a good knowledge of its purpose and why it should be applied, IEC 61508 poses a daunting prospect to both the staff who must apply it and the managers who must instruct them how to do so. Not only will some of its seven parts be irrelevant to a given project or product, or even to the operations of a particular company, but also some clauses within relevant parts will not be relevant. Further, many users are unsure both of how to interpret much of the informative advice (particularly in Parts 5 and 6) and to what extent it should be followed.

Before calling on staff to use the standard, management needs to understand its structure and the relevance of each of its clauses to the company and to the project in hand. They need to provide clear guidance on how and when to use the standard and which parts of it to use in each case.

The standard is 'generic' and is intended as the basis for the development of more specific standards. It is therefore, by definition, broad in its application and open to interpretation, depending on the industry sector in which it is being applied and on the particular project or product in hand. For any particular application it requires a clear definition of which clauses are relevant and how the relevant clauses are to be interpreted and met.

Ideally, in the first instance, sector-specific standards should be produced. If these are prepared by a small team of experts on IEC 61508 and experts on the sector, the resulting document can be an appropriate interpretation, written in appropriate language, with sector-specific details added. Indeed, it is recommended that if the principles of IEC 61508 are to be employed widely, well developed sector-specific standards should be produced urgently.

Even when a sector-specific standard is available, it is still preferable for the management of a company to tailor it to their needs and to provide guidance to staff on its use. When a sector-specific standard is not available, and IEC 61508 is to be applied directly, it preferably should be tailored. But proper tailoring is a considerable task, and if it is too big for a company to carry out, then management certainly must provide detailed guidance to staff on how to use the generic standard.

This necessity is not merely for the sake of efficient usage. It is also a demonstration of management itself. Staff are likely to be demotivated if simply told to comply with a standard that is obviously too broad in its application for the task in hand, particularly if management is seen (or perceived) not to have taken the trouble to understand the implications of their instruction.

A frequent problem is that IEC 61508 is perceived as a standard for system development. But in fact it not only covers the complete system life cycle (from conception to decommissioning) rather than merely the development life cycle, but it also addresses the larger subject of safety management rather than merely technical matters. The misconception is understandable in junior engineers, but it is inexcusable in management. They must understand the standard's assumptions in this respect (see below) and help the standard's users to meet its less well defined requirements, such as those for documentation and proof of decisions and actions taken. Without definitive guidance from their seniors, junior engineers are unlikely to employ the standard either effectively or efficiently.

3.4. Understanding the Principles Embedded in the Standard

IEC 61508 embodies a number of principles that are new to many of its users, the main ones being:

- Identifying and defining safety requirements;

- Using an overall life cycle model as a framework for the safety activities to be carried out during the life of a system;
- Carrying out risk analysis and using this as the basis for defining safety requirements;
- The concept of safety integrity levels.

Ability to meet the standard's requirements depends on having a thorough understanding of all of these, and any user must be fully conversant with them. Yet, many users of IEC 61508 have not previously had experience in safety engineering, and to them all these principles are likely to be unfamiliar. Even those with a background in safety have had problems in understanding some of them. Moreover, applying the principles requires more than a theoretical understanding of the concepts; in all but the simplest cases, a great deal of expertise and practice is called for, and this is not to be found in most individual users or even in many of their companies.

If the standard is to be used effectively, a significant educational programme is needed. If the standard's principles are to be recognised as the basis of safety engineering, both industrial training courses and appropriate undergraduate and Masters-level university modules need urgently to be developed. Indeed, even if the standard's principles were not to be so recognised, there is still a need for education in whatever principles are deemed to be relevant. Safety is now implicit in the objectives of so many industry sectors and in the functionality of so many systems, that safety engineering needs to be a part of the training of all engineers, including so-called software engineers - in fact, particularly of software engineers.

If at the core of a new standard there is one unfamiliar principle, learning how to use it can be a stimulating process. But if four principles key to the new standard are all novel, getting to grips with them can be daunting. Further, when the interpretation of one of them (SILs) is the subject of debate and there seems to be no one with the certain authority to teach it, the prospect of using the standard is all the more disconcerting. Thus, whereas it is not the purpose of this paper to explain the details of the standard, it is appropriate here briefly to address some of the difficulties thrown up by the four technical principles that have been mentioned.

3.4.1. Identifying and Defining Safety Requirements

Companies in some industry sectors have employed safety engineering in the development and management of their plant, processes and products, but most companies that are now using or studying IEC 61508 have not previously specified safety requirements independently of functional requirements. The concept is not complex and so can easily be understood, but in practice its effectiveness depends on the process of hazard identification - which can be time-consuming, tedious and costly. If it is carried out inadequately, there may be no immediate way of knowing this, for hazards not identified are not mitigated, and may be assumed not to exist. For management who do not know that safety analysis depends on a foundation of well managed, meticulous investigation, and who may not be enthusiastic about introducing such practices anyway, the identification of safety requirements may seem to imply a quick and simple process.

If techniques are to be applied effectively, management at all levels in a company, as well as technical staff, need to be educated in the principles of safety engineering.

3.4.2. The Overall Safety Lifecycle

Not only does the standard recommend this model for use by practitioners, but also it uses it to define its own structure. For anyone familiar with life-cycle models, this one is not difficult to comprehend. However, there is one unusual aspect of it that is worth remarking on. Whereas project and system life-cycle models normally portray the development or life of a single system, this one may be concerned with more than one system. And the fact that this is implicit to the model and not explicitly stated means that it is not apparent to many users.

To clarify the point, consider Figure 1. Here, the system being created is the 'equipment under control' (EUC) along with its control system, and its purpose it to achieve some defined utility. A risk analysis of the EUC and its control system is carried out, and certain risks are identified. Then,

according to the standard, if it is deemed necessary to reduce these risks, 'safety requirements' for doing so are defined, and these become the specifications for 'safety functions' - which should, preferably, be implemented separate from the control system (e.g. in a 'protection system', as in Figure 1), but may also be incorporated with it. Once the safety requirements for protecting the world from the risks posed by the EUC have been derived from the risk analysis, the overall safety lifecycle becomes devoted to the safety functions and the (perhaps many) systems on which they will be implemented.

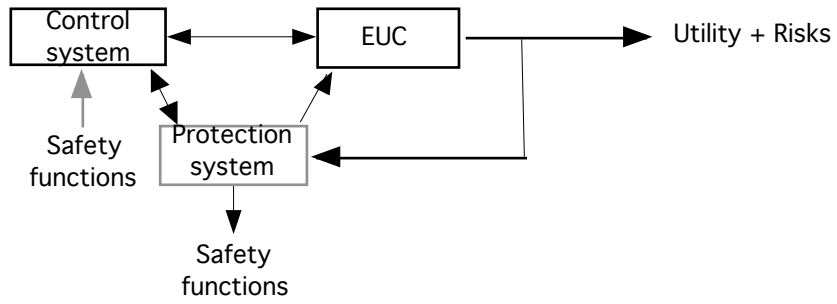

Figure 1: The functional model on which the standard is based

This switch of emphasis from one system to another has confused users of the standard without their realising the source of their confusion. Supporters of the standard's use need to be aware of the problem. Of course it may be argued that the entire plant (EUC and control and protection systems) can be perceived as a single system and there is really no switch of attention, but developers of a protection system are unlikely to find this perspective helpful.

3.4.3. Risk Analysis

The standard requires risk analysis to be carried out and used as the basis for defining the safety requirements. In some safety-related industry sectors, such as petrochemical and nuclear, this has been the norm for some time. But in many sectors, and in most companies, risk analysis has not been applied either at all or in the detail called for in the standard.

Though, in concept, risk analysis is easily understandable, in practice it consists of a number of stages and can be extremely complex. The requirement of the standard to derive risk values is not easily met, either quantitatively or qualitatively, and the use of software, in which failures are systematic rather than random, increases the difficulty. Determining how much risk reduction is required for each identified hazard depends on having determined not only the risk posed by the hazard but also the level of risk that is tolerable in the circumstances. In principle, the tolerable level differs from hazard to hazard, depending on the trade-offs between risks and benefits, so there is, potentially, a considerable task of great complexity implicit in risk analysis.

There is also a sociological side to risk-tolerability decisions. Is it sufficient for a company to make them in isolation? Should those at risk, for example the company's employees and the public, be involved? If not, why not? And, if yes, how can this be facilitated without making the process impossible or too costly and time-consuming?

Many of these difficulties are not touched on in the standard. Yet they exist. The requirement for risk analysis cannot be avoided, for risk-based decision making is now accepted as an essential aspect of safety engineering. So there is an urgent need for more and better guidance on the analysis and management of risk. We need an authoritative handbook that both provides context-setting overviews and explains the small essentials of the technical processes of risk analysis. It should also address the issues involved in risk-tolerability decisions.

But in the absence of such detailed guidance, managers are still obliged to identify, analyse, and manage the risks posed by their plants, processes, and products. It is their responsibility to acquire

sufficient understanding to direct the risk analyses, to ensure that those carrying them out are competent, to put checking processes in place, and to satisfy themselves that what should be done is done and that it is done as well as it could be done.

3.4.4. The Concept of Safety Integrity Levels

The SIL concept is an integral part of the standard's requirements. Yet the different derivations of SILs in different standards, the different ways in which the term 'SIL' is used, and the difficulty in deriving SILs in many cases, have led to considerable confusion [3]. A further problem is that many practitioners go through the motions of deriving SILs unsure of what they are doing, unaware of their assumptions, and unable to check their results.

SIL is a system concept, but is often inappropriately and misleadingly applied to components. As already suggested [3], there is a need for a convention on what is meant when achievement of SILs is claimed.

Given the need to derive SILs in order to comply with IEC 61508, and given the confusion that surrounds them and the lack of certainty even among 'experts', there is a need for research into the theory on which they are based [3] and education in their use. Companies introducing and using the standard cannot ignore them. Judgements need to be made in their derivation and, later, further judgements must be based on what was derived. Management and engineers need to go to whatever lengths are necessary to get a clear understanding of the SIL concept. Not to do so will almost certainly lead to inefficiency as well as error.

3.5. Recognizing the Standard's Assumptions

IEC 61508 does not describe the implementation of a quality system or a documentation system. Yet it assumes both of these things. If the standard is to be taken in isolation as the sole guide to the achievement of safety, safety is unlikely to be achieved and it may not be demonstrated to have been achieved. The standard's assumptions must be understood. Its intended use is circumscribed by its defined scope, so what is outside the scope includes both those things that are irrelevant and the assumptions on which the standard is founded.

Any company intending to use the standard should study its scope and understand its assumptions. Only then can it be ensured that what is assumed is put in place. But undertaking such enterprises as the development of a quality management system is not usually within the jurisdiction of system developers. Doing so requires the planning, the commitment, and the authority of senior management. So senior management have the responsibilities for identifying the assumptions implicit in the standard, understanding their implications on its use within the company, and making sure that the effectiveness of the standard is not compromised by their neglect.

It is not the purpose of this paper to analyse all the assumptions of the standard, but two will briefly be discussed.

3.5.1. Options for System Safety

The standard's requirements are based on the use of safety functions and safety-related systems to reduce risk. This assumes that we already have (at least in design) a functional system, that we have already taken safety into consideration in its design, and that we can determine the residual risk that it poses. The safety functions are then intended to reduce the residual risk still further to some level that is deemed tolerable. These assumptions are not clear to all users of the standard.

Something else that is not clear to many is that specifying and creating safety functions is not the only option for reducing the risk posed by the functional system. Another option is to eliminate or mitigate system hazards by re-addressing the system's design - at the architectural or detailed-design level. Having done this, one must again analyse the system's hazards and determine their risks and, if any is deemed to be intolerable, again face the choice of how to tackle them - whether by further redesign or by introducing safety functions.

The reason why this choice is not recognised is that the standard carries the implicit assumption that the question has been faced, the functional design finalised, and the choice made to add safety functions. This assumption has caused problems, not only for users of the standard who may find themselves having to create safety functions to protect against risks that would better have been reduced by redesign of the functional system, but also because it has led to opposition to the standard. Some have argued that the standard ignores the need to make the functional system safe in the first place and that this deficiency makes the standard unacceptable as the basis of safety engineering.

Such criticism should be heeded when the next draft of the standard is produced. However, having made the functional system as safe as we can, what then? Do we proclaim it to pose zero risk? To do so would be unprofessional. So what do we do about the risk that we acknowledge? We cannot avoid attempting to determine its value (quantitatively or qualitatively), for that is now accepted good practice everywhere. And once we have done that, we are back within the scope of the standard - assessing the risks and creating safety functions to reduce them to tolerable levels.

Thus, while it is unfortunate that the standard does not explicitly attend to reducing the functional system's risks in the first place, this does not invalidate it as a useful standard and it does not alter the fact that its requirements call for currently recognised good practice.

3.5.2. Safety Management System

A cursory reading of IEC 61508 may suggest that its clauses simply mandate a number of technical requirements. But it addresses the broad issue of safety management and not merely the narrow one of technical processes. Although the explicit requirements on management (Clause 6 in Part 1 of the standard) are brief, often vague, and occupy less than two pages, they touch on every aspect of safety management and amount to the need for a 'safety management system'. This in turn depends on an effective quality management system being in place. Indeed, meeting the standard's requirements effectively and fully depends on a safety culture, and the first step towards this is to have a safety management system in place. Companies that fail to recognise these fundamental assumptions do so at their peril.

3.6. Appreciating What the Standard does not Cover

There are also aspects of safety engineering that the standard does not touch on explicitly. Yet, modern thinking calls for them, and it is important for the management in companies using the standard to be aware of them.

The standard is 'goal-based'. Its requirements lead its users to points at which decisions must be made, but decision-making remains the responsibility of the users. Thus, compliance does not consist of following a set of rules, but of carrying out processes, each involving judgement. It requires that evidence is compiled, both to demonstrate why a particular level of safety was deemed appropriate and to support a claim that it has been met.

However, the standard has many reluctant users, and many with no experience of safety engineering. Consequently there is a considerable risk that it will be used prescriptively - that is, as a rule book on what to do rather than as a guide to how to set safety goals and manage their achievement.

If the standard is taken to be a prescriptive and exhaustive recipe for achieving safety, it will not be possible to demonstrate what (if anything) has been achieved. It is important to understand not only the assumptions on which the standard rests (see above) but also what the standard does not cover. Only then will the safety engineering not covered by the standard be carried out. And, again, it is the responsibility of senior management to get to grips with these matters. Three such issues will briefly be touched on here.

3.6.1. Safety Assessment and the Safety Case

Safety engineering requires not only that we achieve a desired level of safety but also that we

demonstrate its achievement. But users of the standard are not all safety engineers. Many are developers, of hardware or software, perhaps engineers and perhaps not, who may hitherto have ignored the fact that their product is safety-related. They and their companies typically think in terms of functionality, and the concept of identifying and assessing risks, and defining and implementing independent safety requirements, is not within their experience. Similarly, the notion of constructing a case to demonstrate that the safety requirements have been met is also unfamiliar.

It may be added, however, that the notion of having to demonstrate that the processes employed in development are appropriate to a given level of quality should be familiar to software engineers. It has long been accepted that, as product quality cannot be measured in acceptable time, evidence must be adduced from the development processes. The same principle applies to having to demonstrate the adequacy of development process to the required level of safety.

But, although the standard offers some advice on safety assessment, it does not give detailed guidance on the collection of the necessary evidence or on the development of a safety case. Thus, blind followers of the standard would be unable to demonstrate the achievement of the targeted risk reduction, even if it were achieved. It is important for a company to identify those things important to safety that are not covered by the standard, to determine their relevance to the system in hand, and to decide if and how they should be covered.

3.6.2. Human Factors

The standard mentions the need to consider human factors in carrying out risk analyses, but it says no more than that, and users need to recognise the omission. Newcomers to risk analysis need to appreciate not only the difficulties of assessing the risks posed by humans but also the extent to which human factors should be taken into account both in the system development and management processes, and also in dealing with risk issues. Humans are integral parts of most systems, and their omission from safety and reliability analyses can have considerable influence on the results. Not only are operators implicated, but so too, as many accident enquiries have found, are senior management, because their policies, leadership or lack of it, and the culture that they engender, can create predispositions to accidents.

Parts two and three of the standard address hardware and software issues respectively, but there is no equivalent section to provide guidance on assessing the risks posed by humans or on mitigating them in system design. Similarly, although 'hardware safety integrity' and 'software safety integrity' are defined, 'human safety integrity' is not. Yet, in many systems, the most likely causes of failure, and perhaps dangerous failure, are due to humans.

If management are to ensure that the risks posed by their plants, processes, and products are tolerable, they need to take advice, not only on risk analysis in general, but on how to take human factors into consideration in carrying it out. If senior management does not take the initiative in this, those using the standard are unlikely to take human factors into account, and many dangerous failure modes may be ignored.

3.6.3. COTS

The assessment of commercial off-the-shelf (COTS) products, particularly software, for use in safety-related systems is a subject that is currently generating considerable interest. Under what circumstances might COTS be used? Given that their suppliers are unlikely to provide sufficient details to allow full safety assessment, what evidence would be adequate?

The standard mentions COTS but does not directly address the question, except that in the final draft of Part 2 it offers brief guidance on using a 'proven-in-use' argument to justify the use of a subsystem for which full documentary evidence is lacking. But the rules on 'proven-in-use' are restrictive: the subsystem needs to be of limited functionality and the conditions of the previous use for which proof of safety is claimed need to have been the same as or 'sufficiently close' to those which will be experienced.

Part 2 relates to hardware, and, because all software failures are systematic rather than random, it is difficult to see how these rules could apply to software subsystems. In the absence of specific

guidance, it is implicit in the standard that if the relevant information is absent then no safety case can be made, and use of the system in question cannot be justified.

The standard is aimed at safety and not commercialism. But it cannot be denied that system development and operation proceed within a commercial reality, so the question remains open and demands research. Meanwhile, users should be aware of both the lack of specific guidance and the implicit message of the standard.

3.7. Possessing the Expertise to Apply the Standard

It is not enough simply to provide staff with a copy of the standard and tell them to use it. From the paragraphs above it should be clear that a great deal of knowledge and understanding is necessary if it is to be put to effective use. There must be appropriate expertise in management, software engineering, safety assessment, human factors, and other disciplines; appropriate analyses must be carried out, professional judgements made, life-cycle tasks performed in conformity with the standard's requirements, and appropriate techniques and tools selected and used. It seems almost superfluous to say it, but awareness of and knowledge about the standard are insufficient - the possession of appropriate competence and experience is a necessity for using it. Developing and acquiring that expertise, nurturing and retaining it, and employing it effectively and efficiently, are the responsibilities of senior management.

3.8. Providing Support to the Users of the Standard

Even if all that is suggested above is put in place, users of the standard - like users of any tool or technique - require continuous support [4]. As the standard is applied to each new project or product, queries arise about the relevance or interpretation of this or that clause or requirement. Education and training needs recur as new staff become involved. Throughout the use of the standard, difficult decisions must be made on such issues as the tolerability of risk and the appropriateness of techniques to SILs. Valuable time can be wasted if staff do not know where to turn for advice or if those to whom they should turn are unprepared.

A company's management should continuously seek to review and improve the way in which the standard is used. If the standard has been tailored for use in the company, the tailored version is on trial. The chances are that it will require further tailoring for each new project; or, at least, new guidance will need to be provided on which clauses are inappropriate in the new context. Sometimes it may turn out that clauses from IEC 61508 previously omitted from the tailored version are now relevant and should be included. And if the standard has not been tailored, there will certainly be a requirement for specific guidance in each new application. There will also be times when the initial guidance is found to be inappropriate, and the staff involved will need to report this and receive up-dated advice - and they will need this quickly if time on a project is not to be lost.

Only over time, and with editing based on feedback from users, will tailored versions of the standard become stable. For this to be achieved, there must be a defined point in the company to which users can communicate their feedback. Moreover, when feedback is received from users, responses must be given to them. When communication is one-way confidence is lost.

What is being said here is that the installation and use of a new standard, particularly one as large and complex as IEC 61508, requires management. And 'management' here does not imply casual supervision but a principal responsibility. A company needs to provide continuing support, in both the management and the technical aspects of the standard's use, and this may require a new or redefined organisational structure.

4. The Ninth Necessity: Infrastructure

The eight necessities explained above are for knowledge, understanding, and action, by various persons of several disciplines and levels within a company -much of it by senior management. It is unlikely that they will all be available when required unless their provision has been systematically coordinated.

It is not sufficient for them to be available at one point in time and then to diminish or disappear, for the complexity and breadth of scope of IEC 61508 mean that the process of installing and coming to terms with it is likely to continue for a considerable time. The requirement for the necessities will continue commensurably. They should therefore be made to comprise an infrastructure which is put in place and maintained.

This may be a large and costly recommendation. But consider how much it costs to have staff struggling with an immense, new, complex standard which is based on several unfamiliar principles. How much time is wasted? If there is no guidance within the company, how many wrong turns are taken, and how many of these have lasting impacts on safety or other aspects of a project? For example, if at the end of a project it is realised that no provision has been made for assessment, how much more does it cost to build up a safety case retrospectively? A well considered, well planned, and well instituted infrastructure for the provision of the first eight necessities is a ninth necessity. And only senior management is placed to plan, create, and monitor the effectiveness of such an infrastructure.

5. Discussion

IEC 61508 is often perceived as a technical standard. But it goes far beyond merely placing technical requirements on system developers. Its theme is the management of safety. As such, its users are not simply the engineers who apply it in their project work but the entire organisation which forms the context for a project or product. The requirements for its effective application fall not only on the engineers but also, and more importantly, on all levels of management. Middle managers must be involved in all aspects of its use, and senior management should first have defined its strategic context and planned its introduction, use and support.

Any new standard poses problems to its users. The temptation to senior management, particularly if the issues are perceived as being purely technical, is to leave them to the engineers. But the engineers will almost certainly not possess the contextual knowledge necessary for planning its application, and they may not even possess the technical knowledge to apply it correctly. The eight necessities of Section 3 are therefore intended to guide management. In brief, the necessities form a checklist, with the accompanying text offering explanations of what is required and why. The ninth necessity of Section 4 provides the means of ensuring that the primary eight are indeed provided.

The necessities are not chronological stages in a process. Rather, they are levels of knowledge, understanding, and action that form a structure essential to the effective introduction and use of the standard. They do not need to be acquired in any particular order. For example, if junior engineers attend an awareness seminar and learn about the principles embedded in the standard (Section 3.4), they may report on the standard's apparent merits to their seniors - who may then take the trouble to learn about the standard's more detailed requirements (Section 3.2). But it is not until senior management have understood the purpose of the standard (Section 3.1) that its need in their business can sensibly be debated. Moreover, it is not until management understand the assumptions that underlie the standard (Section 3.5), and ensure that they are met, that the standard can effectively be employed within the business. Further, it is not until the full scope of safety engineering is appreciated (Section 3.6), and those things omitted by the standard put in place, that a company will be positioned to achieve and demonstrate the achievement of safety rather than merely compliance with the standard.

Evidence suggests that most companies have not put the nine necessities in place, and are therefore inadequately equipped to use the standard effectively and fully. Should such organisations decide to employ the standard, they are advised to commence from the perspective of the ninth necessity. This would induce them to consider not only the other eight necessities individually, but also how to coordinate their introduction and operation so that together they provide the required infrastructure for

the introduction of the standard and the support of its users. Doing this should be regarded as a major project [4], with proper planing, from the strategic level to the smallest technical details, being carried out. Good results always require attention to detail.

Finally, it may usefully be pointed out that when the details concerning IEC 61508 are stripped from Sections 3 and 4, the nine necessities can be seed to apply to the installation of any new standard or other tool. They therefore comprise general guidance on this subject.

Acknowledgments

The valuable comments of Bruce Elliott and Martyn Thomas during the preparation of this paper are acknowledged with gratitude.

References

[1] International Electrotechnical Commission. *International Standard IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems*. IEC, Geneva, 2000

[2] Redmill F. "IEC 61508: Principles and Use in the Management of Safety". *Computing & Control Engineering Journal*, 9, 5, 1998. IEE, London

3] Redmill F. "Safety Integrity Levels - Theory and Problems". In Redmill F and Anderson T (eds.): *Lessons in System Safety - Proceedings of the Eighth Safety-critical Systems Symposium, Southampton, UK*. Springer-Verlag, London, 2000

[4] Redmill F. "The Introduction, Use and Improvement of Guidelines". In Ehrenberger W (ed.): *Safety of Computer Control Systems 1988 (SAFECOMP '88) - Proceedings of the IFAC Symposium, Fulda, FRG, 9-11 November 1988*. IFAC Proceedings Series, Pergamon Press, 1988