SAFETY MANAGEMENT

THE BACKGROUND TO DEFENCE STANDARD 00-56

BY

K. GEARY, BSc, CENG, FBCS, GIMA
(Sea Systems Controllerate, Bath)

ABSTRACT

This article explains the background and reasoning which led to work on drafting Interim Defence Standard 00-56. The Standard's emergence, coinciding with increasing sociological awareness of safety issues, is discussed in relation to safety management. Project factors are also considered and improvements over the widely promulgated first draft IDS 00-56 (1989) are outlined.

Introduction

The concepts embodied in Interim Defence Standard (IDS) 00-56[1] are described in the article which follows this one[2].

Development of IDS 00-56 began early in 1989, based on the existing procedures of a large defence contractor, to whom we are grateful. The impetus was due to the need to place Interim Defence Standard 00-55 in context. The first draft was promulgated for public comment mid-1989 and was also applied to live projects, with lessons learned contributing to the specification for the second draft. Minor refinements to the second draft resulted in successful publication.

Background

In the past, hazard analysis of relatively simple mechanical systems could be performed subjectively by examination. There was adequate confidence in this process because the detail of functional mechanisms was visible. Such analyses were often based upon lessons learned from experience. Like many design rules, safety considerations have evolved reactively and, as reports of recent civil disaster enquiries have taught us, they are still doing so. Where established design practices are relatively stable, design safety rules have matured to an acceptable level. However, with systems becoming ever more complex due to the increasing pace of technological evolution and the ever increasing demands for sophisticated functionality, often implemented through software, the hazard analysis exercise is no longer straightforward. In such circumstances it is unwise to rely on developing safety rules reactively. Technology in general is no longer sufficiently stable to be able to consolidate experience before newer technological advances are implemented with even greater degrees of sophistication and sensitivity, thereby increasing the scope for root causes of accidents. Furthermore, safety has become 'fashionable' and the sociological climate is nowhere near as forgiving as it used to be. Accidents are becoming more unacceptable and there is widespread recognition that they are usually preventable.

This new awareness has placed the safety assessment and certification process much more in the limelight and, as a result, the need for evidence of design safety has received wider recognition. Safety assessment requires demonstration that safety management has been properly applied. This is accomplished by knowledgeable overseeing and documentary evidence. In Interim Defence Standard 00–56 there is a requirement to record safety criticality status and, where relevant, the safety management activities carried out throughout the lifecycle of the system. Such evidence, recorded in a Hazard Log, is central to the documentary evidence that would be required by a safety assessor.

Acceptable Risk

Deliberations on safety criticality inevitably lead to the question 'What is an acceptable risk?'. Deciding on the acceptability of risk is unfortunately not always a quantitative judgement; it may be biased by emotions. Public opinion, albeit strongly influenced by what constitutes a good news story, and the resulting political opinion will have most influence on what is an acceptable risk. For example, we accept a probability of death by road accident of 1 in 10 000, but a risk of death of 1 in 1 000 000 for an uncontrolled nuclear release from a power station[3] can cause reactions resulting in expensive public enquiries, mass demonstrations, and Parliamentary questions. As an example of public sensitivity, reporting of Tornado losses in the early phase of the Gulf war illustrated how relatively few losses for such military action still raised public concern and political comment.

The issue of human fallibility does not seem to be of great concern[4] to the public at large. Although many notable disasters are directly attributable to human failure, society still seems to be prepared, under many circumstances, to rely on the familiar human operator and show a lack of trust in automated systems, especially those where there is little general understanding and visibility of the operating mechanism. Reversion to manual control is not possible for many modern defence systems because humans are not sufficiently quick or accurate in their reactions to substitute for computerized real-time control.

What constitutes an unacceptable hazard means different things to different people. The term 'accident', used in the general sense, has a wide meaning which can refer to any unintended event that may or may not cause damage or

harm. An unintended event that causes damage could range from a minor scratch on some paintwork to large scale destruction of property and lives. When it comes to the grey area of deciding whether a system is in one category or another, arguments occur between those that have economy and schedules as their prime objective and those concerned with prevention of what the safety assessors consider to be unacceptable accidents.

The problem of deciding what is an acceptable risk is complicated by the need to attribute a 'metric' (some meaningful unit of quantification, e.g., for rail travel, death rate per passenger mile) to risk in the form of probability of accident per some unit of measure. But, what is the unit of measure to be? It could be units of time (such as mission hours), units of activity (such as number of projectiles fired), or units of demand (such as the likelihood of accident per single missile). Random failure distributions, which constitute a measure of physical degradation, are not readily transferable to systematic failures that may or may not manifest themselves in an unsafe way. The severity of consequent system failures is predetermined with respect to specific operational circumstances at the time of incidents[5]. The general lack of a universal metric prevents direct comparisons being made between sectors. Therefore, problem-specific metrics are likely to remain for some time unless there is a breakthrough in perception of accident measurement criteria.

The issue is not just a MOD problem, it needs to be tackled on a national basis. The difference between civil considerations and military ones is that the military makes use of systems that are designed to be hazardous, but only to an enemy and only where and when intended. Current civil and military activities associated with safety critical software are complementary in that current MOD priorities[6] equate to the class of civil safety considerations for systems that are potentially lethal.

Rationale

There are several NATO, Defence, or Naval Engineering standards which lay down design rules for safety for various categories of military equipment. Many of these standards call for a hazard analysis to be conducted. Often, there may be a chicken and egg situation whereby the system or an aspect of the system has to be recognized as potentially hazardous before a safety-related design standard is invoked. With systems incorporating explosives, for example, policy makers have already performed a high level mental hazard analysis because experience over many years has taught us that explosives can be dangerous and a safety policy has duly evolved. An example is AOP-15[7] which is a standard that applies to explosives and calls for a hazard analysis to be performed.

The need to assess the safety of systems with sophisticated control mechanisms has been focused by the increasing use of software-based control and the consequent concern over the integrity of safety critical software and its interaction with computing hardware. This raised the issue of deciding when software was or was not classified as safety critical. In searching for a suitable model standard it became apparent that there was little in the way of existing applicable standards, guidance or *de facto* procedures for hazard analysis of systems or components[8], whether or not they are computer controlled, other than those applied to plant in the traditional heavy construction, nuclear and chemical industries.

Another observed general problem was that hazard analysis was sometimes applied in the latter stages of development or close to acceptance. With no definitive policy or obligatory or advisory standard, hazard analysis may be progressed by subjective judgement exercised by a committee. Although this practice may traditionally have been applied successfully to relatively simple

technology, it is not sufficiently effective when applied to modern complex high functionality systems. Two significant contributory documents containing some guidance on hazard analysis of systems are MIL STD 882B[9], which is a high level document, and the HSE Guide[10] which includes a description of Fault Tree Analysis.

Requirements for consistency, clarity and methodical argument in hazard analysis inevitably lead to the need for a standard. Good engineering management regarding safety needs to be sure that safety critical systems and components are identified at an early stage. Furthermore, in order to avoid non-critical system projects being tasked unnecessarily, such systems should be exempted from safety policy requirements as early as possible in their lifecycle.

Project Factors

The lack of methodical or timely hazard analysis or deficiencies in the auditable documentary safety evidence will introduce a high risk of incurring significant delays and extra costs through a need to carry out expensive re-work at a late stage in the project. The Channel Tunnel project found out, to its cost, that a simple safety aspect, such as shuttle door width apparently overlooked during design, can be very costly to put right after production[11]. If safety assessment is left until final safety certification is required, say for embarkation, certification processes may reveal unacceptable safety risks which had not been previously realized. This will result in a delay or prevention of certification and introduction into service, and project costs and timescales will be significantly extended while safety features are dealt with retrospectively. Project risk assessment (not to be confused with *safety* risk assessment which may use similar methodologies such as FTA) is currently high profile as an essential management aid. This being so, early implementation of hazard analysis and *safety risk* classification will form a significant contribution to the reduction of *project risk* whenever safety is a factor.

The usual means of addressing safety is to set up a project safety committee, although this is not always the case for smaller projects. Design is normally perceived to be the critical path to project success with the work of the project safety committee being an ancillary procedure and occasionally seen as a necessary evil. It is not unusual for early design decisions to be made before the project safety committee has established itself and in those circumstances the hazard analyses may not be finalized before the design is almost complete. The project safety committee therefore may follow design rather than its work becoming an integral contribution to the design process. This approach tends to assume that the design is tolerably safe and the safety committee's role becomes one of producing safety papers and gathering approval from the various safety advisers. If the safety committee operates in a reactive fashion, unaccounted resources of members will inevitably be employed in negotiating compromise, sometimes accompanied by protracted and detailed technical discussion, rather than the more efficient and creative task of contributing to design safety, with approval following almost by implication.

The initiative for Interim Defence Standard 00-55[12] was a proactive measure aimed at reducing the risk to safety from software specification and design flaws. Interim Defence Standard 00-56 is also proactive in its approach to design safety. Its objective is to identify component safety criticality in the context of the system so as to enable the optimum use of resources by focusing on the safety critical elements and apportioning a safety classification to each. Resources can then be optimized by applying the appropriate design rules to the critical components, such as the application of IDS 00-55 to safety critical software. (As yet there is no equivalent of IDS 00-55 for computing hardware). By taking a proactive approach to safety management, IDS 00-56 can be used

to control costs by targeting the critical areas of computer controlled system function. In contrast, the more blunt approach of a reactive safety policy may lead to unnecessary expenditure by making some parts or systems safer but much more expensive than they need be.

On a more general level, the IDS 00-56 approach offers a way towards greater efficiency for safety management tasks. Uniformity of presentation and of requirements for safety case evidence would enable a single definitive interface to be derived between projects and an infrastructure incorporating the various safety assessment and certification bodies. This would greatly ease current project burdens of interfacing individually to several different safety advisers and would facilitate improved efficiency in assessment and certification through a single safety adviser co-ordination facility.

Causal Links

Increased complexity of system design creates increased scope for root causes of accidents. Systems are becoming more sensitive to apparently insignificant or unexpected events and the causal links are no longer readily apparent. The old tale about the lack of a horseshoe nail resulting in the loss of the kingdom is an illustration of a causal link which was not perceived before the event. Under a reactive approach to safety rules, the response would be to analyse such a scenario after the event. The likely resultant policy would be that all farriers would be instructed by law to carry a minimum of 500 horseshoe nails at all times, in those days on pain of death which adds a new dimension to the safety criticality of nails. However the IDS 00-56 philosophy facilitates a proactive approach to safety management so that an assessment can be carried out and an early informed judgement made about the critical components of a system, if applicable including logistics and maintenance.

Sensitivity

Although not safety critical, the problems with the Hubble telescope illustrate the sensitivity of refined technology to a minor physical event compounded by human deviations[13]. An investigation found that a tiny fragment of non-reflective coating flaked off a metering rod cap, resulting in an erroneous reading based on reflected light. Tests showing misalignment of instrumentation were incorrectly blamed on the test device and an aberration detected by an older instrument was dismissed. At the time the contractor's quality assurance department was understaffed and so the relevant quality control procedure was not enforced. It is well known that the telescope, costing $1.6bn, suffers degraded performance.

It might be possible to establish causal links to show that almost everything is safety critical. However, common sense must prevail in the depth and detail of analysis and in the importance of causal links. IDS 00-56 hazard analysis progresses in a hierarchical top down fashion, enabling each level to be examined and decisions made as to which of the lower level elements (e.g. the most critical elements) should be targeted for analysis in greater depth. It should be recognized that nothing is 100% safe; even living eventually results in death. A reasonable and acceptable degree of risk must therefore be assumed, otherwise analysis costs may become disproportionate to benefit and we could end up establishing a causal link between project management and shortened life expectancy.

Software

Examples of causal sensitivity may be seen in software-based systems. Those in the software industry have long been used to the software 'bugs' that have

dogged computing systems for years. Software is discrete, complex and ultra-sensitive to apparently minor deviations in program or data. Until recently we have been able to tolerate software errors as long as they did not cause too much inconvenience or loss of system availability. However, the ACARD report [14], published in 1986, publicly expressed concern over software being used for safety critical applications. Attention was then turned to the significance of software in safety-related systems. Action was started with the objective of reducing safety risk in defence equipment resulting from software flaws and, following much deliberation and consultation, Interim Defence Standard 0-55 has been produced.

Experience

Trial application of the first draft 00-56 on live projects was enlightening. It was interesting to note that experience of live application generated observations which contradicted some of the comments received concerning the style of the Standard. It was therefore possible to form an evaluation based on experience of use as well as theoretical judgement. Other projects have subsequently applied the first draft and, whilst too late to contribute, have confirmed observations from the initial trials. A recent application, based on the first draft plus the subsequent redrafting plan for guidance, was reported as a valuable exercise for the safety assessment concerned.

One observation on the use of the Standard under current procurement policy is that it may be difficult at present for assessment contractors to quote one fixed firm price for the whole job. There are two main reasons for this. Firstly, there is a lack of price estimation experience against the tasks involved. Second, the amount of assessment work is dependent upon the design contractor's procedures and documentation and on the nature of the system being assessed and its operational environment. Typical contractual strategies so far have been either to predefine the hazards to be investigated or to let a running contract and place tasking by means of a series of fixed price work packages. The latter approach seems to be preferred by both projects and contractors.

Evolution

The final draft of IDS 00-56[1] shows a new title which reflects its initial and immediate role related to IDS 00-55[12]. There has been a reform of document style and structure and, hopefully, the clarity of requirements associated with this complex topic has been improved. The first draft of IDS 00-56 attempted to simplify safety classification too much, however both comment and experience of use indicated that safety classification is not simplifiable to an elementary level. Initial impressions of complexity often fade when implementors learn to apply IDS 00-56. With a change of the current title to increase its scope, the Standard should be capable of being used to address most or all safety risks associated with systematic and random failure, where software is one aspect of system design. Significant changes from the 1989 draft include:

(*a*) refinement of the safety criticality classification and inheritance schemes;

(*b*) accommodation of mature technical safety cultures by allowing substitution of deep analysis by the application of established safety design rules;

(*c*) consideration of the contribution to safety by the human operator as part of the system[15];

(*d*) consideration of the possible need to balance system initiated hazards with defence against greater hazards from hostile acts.

This final feature is an important pragmatic concept for safety assessment of Defence equipment. Civil systems are designed to be 'fail safe', which normally involves the system ceasing to function or switching automated control over to manual control. Most if not all safety standards take this approach. Many Defence systems, however, may have a role where the success of their mission could be regarded as safety critical. For example the mission of a CIWS is to protect a vessel from deliberate hostile acts. If it fails, human lives and the vessel are likely to be lost. Under such circumstances, it must be recognized that, although an individual life could be put at risk from the system, a far greater risk will be incurred if the system fails to perform its mission to defend.

Although safety policies usually only address peacetime, detailed press reporting of war activities and losses and the resultant social and political concern may mean that such policies will need to be reviewed. Despite the Allies' success, the 1991 Gulf war provided abundant material for media analysis, albeit mostly speculative, on the availability, reliability and performance of complex weapon systems. Whatever the military perspective, it is the kind of coverage that some politicians cannot ignore forever.

Conclusion

Software is a component of a system and it is the system that may be dangerous, not the software on its own. Any viable hazard analysis must therefore consider the system in its operational environment in order to arrive at a classification for software criticality. It is inefficient to carry out individual component-oriented system hazard analyses and therefore there is a potential broader context for IDS 00-56. The Standard is required initially in order to identify when IDS 00-55 should be applied; however the principles in IDS 00-56 are generic and capable of accommodating a wider scope.

When carrying out a hazard analysis of a system or component, it is necessary to include the operational scenario in which the system will be used. Hazard analysis for the identification of safety critical components cannot be performed by analysing the components in isolation; it must include relationships with the real world.

Experience has shown that hazard analyses can be variable in the depth, completeness and timeliness of application and, when problems related to safety and assessment are discovered at a late project stage, resolution of deficiencies can pose considerable risk to project criteria. Interim Defence Standard 00-56 represents a significant step forward in procedures to introduce definitive engineering disciplines to the area of safety management.

It is widely recognized that discovery of design flaws late in development means delays and added expense, with post-production changes typically costing 100 times more to correct than if found during the specification and design phase. The value of the Standard to projects is to provide a safety management framework, including milestones progressing with the specification and design activity and to enable safety contributions to be made to these success-critical stages. To view the Standard as merely a documentary procedure, adding to costs, is to overlook its greater strategic advantage as an enabler of project risk reduction by significantly reducing the probability of unexpected objections at the safety certification and acceptance stage.

If the principles of the Standard were adopted for a wider scope, project management efficiency could be improved. The Standard's documentation and and consultation scheme could provide a single project interface to the many system safety advisory and certification bodies that inevitably become involved with certification of a Defence system.

Predictive methods will never replace experience but, if used in conjunction with experience, they should enhance designers' ability to exploit advancing

technology whilst maintaining safety at acceptable levels and at optimum cost. This new Standard does not in itself provide all the answers, but it has already served to focus minds on the issues of acceptable risk and on the infrastructure necessary for the application of engineering thoroughness to safety management.

References

1. Ministry of Defence: Hazard analysis and safety classification of computer and programmable electronic system elements of defence equipment. *Interim Defence Standard 00-56;* Directorate of Standardization, Glasgow, 1991.
2. Geary, K.: Defence Standard 00-56 for hazard analysis and safety risk assessment; *Journal of Naval Engineering*, vol. 33, no. 2, Dec. 1991, pp. 259-267.
3. Health and Safety Executive: *The tolerability of risk from nuclear power stations;* HMSO, London, 1987.
4. Tuler, S., Kasperson, R. E., Ratick, S.: Human reliability and risk management in the transportation of spent nuclear fuel. Pp. 169-194 in *Reliability on the move: safety and reliability in transportation;* ed. G. B. Guy, Elsevier Applied Science, London, 1989.
5. Harbison, S. A.: Safety objectives in nuclear power technology; *Reliability Engineering and System Safety,* vol. 31, No. 3, Elsevier Applied Science, London, 1991, pp. 297-307.
6. Ministry of Defence: Draft MOD policy statement for the procurement and use of software for safety critical applications; *D/CSSE/4/22*, 14 Dec. 1987.
7. NATO: Guidance on the assessment of the safety and suitability for service of munitions for NATO armed forces, *Allied Ordnance Publication 15 (Stanag 4297);* NATO Military Agency for Standardization, March 1985.
8. Stoddard, R.: Are there bugs in the program?, *Defence Computing,* Feb. 1990, p. 10.
9. US Department of Defense: System safety program requirements, *Military Standard 882B;* Dept. of Defense, Washington DC, 1984.
10. Health and Safety Executive: *Programmable electronics systems in safety related applications;* HMSO, London, 1987.
11. BBC News: News report on Channel Tunnel delay of 6 months and £100M lost revenue for safety modifications to shuttle exit doors; BBC1 6 o'clock News, 8 April 1991.
12. Ministry of Defence: The procurement of safety critical software in defence equipment, *Interim Defence Standard 00-55;* Directorate of Standardization, Glasgow, 1991.
13. Joyce, C.: A flake of film foiled Hubble; *New Scientist*, 1 Dec. 1990, p. 21.
14. ACARD: *Software—a vital key to UK competitiveness;* HMSO, London, 1986.
15. Lucas, D.: Looking facts in the face; *Professional Engineering,* July/Aug. 1990, pp. 28-29.