SAFETY ASPECTS OF HEBRIDES ARTILLERY RANGE COMPUTER & COMMUNICATIONS SYSTEM UPDATE

BY

COLONEL S. ABATE, MSc, CEng, FIEE, MBIM, REME
MAJOR R. J. WILKINSON, RA
M. RICHARDSON, MSc
(Ordnance Board)

This article is a shortened version of a presentation by the authors at an Electrical Research Association symposium on Hazard Assessment held on 20 November 1991 at the headquarters of the Institution of Electrical Engineers in London.

The project described has now reached the implementation stage with the contract announcement in April 1992. Hazard analysis of the system will continue.

ABSTRACT

The Ordnance Board was tasked to advise on the safety implications of the computer aided control at the Royal Artillery Range on South Uist in the Outer Hebrides. This work has been performed in parallel with the development of both the draft Interim and the Interim versions of Def Stan 00-56.

This presentation is based upon the Ordnance Board's experience during the implementation of 'SR 4017—The Introduction of a Replacement Central Computer and Communications System for Range Safety Purposes at the Royal Artillery Range Hebrides (RARH)'. This is one of the first MOD projects to be subjected to the rigours of Def Stans 00-55 and 00-56[1,2]. At this stage it must be said that the contractors were required to work to the first Draft Interim Standard together with proposed alterations that had been submitted by Adelard (the company that wrote and edited Def Stans 00-55 and 00-56 for MOD). The development of safety advice to this project, as in all cases, was an iterative process, in which ideas were floated, discussed, accepted or rejected and then reviewed at a later stage. It is our intention to give you a flavour of the problems met and the discussions that occurred in order that you may benefit from our experience.

The Ordnance Board

Firstly, a few words on the role of the Ordnance Board within the Ministry of Defence. It traces its history back to the reign of Henry V when one of the King's friends was killed as a result of an accident involving the firing of a cannon. Since then with only one short break, in the late 19th century, a version of the Board has been in existence to monitor the safety of explosives. Its official title, as is the way of these things, has changed though its essential role has not.

Today the Ordnance Board is part of the Procurement Executive, working directly to the Chief of Defence Procurement (CDP), and it is tasked with giving independent impartial safety advice on whether weapon systems and munitions are safe and suitable for service. Over the years its sphere of

influence has expanded from the area of explosives, which continue to be the core of the Board's work, to cover advice on the range safety of ballistic and guided weapons, unmanned aerial vehicles and lasers. As technology has developed the Board has become concerned with the safety implications of the use of computers, micro-processors and their associated software incorporated within weapon and range safety management systems.

The Board has a 'Bench' which consists of the President of two star rank and two Vice-Presidents of one star rank. These posts rotate between the three services. Below them are a number of single service 'Divisions' each of which is headed by a Board Member. Each Division is designated a letter: 'G' Division has responsibility for land service guided weapons; 'B2' Division covers infantry weapons and pyrotechnics. A particular reference must be made to 'S'—Support Division which is staffed with a number of scientists who provide expertise in specialist areas including safety critical software.

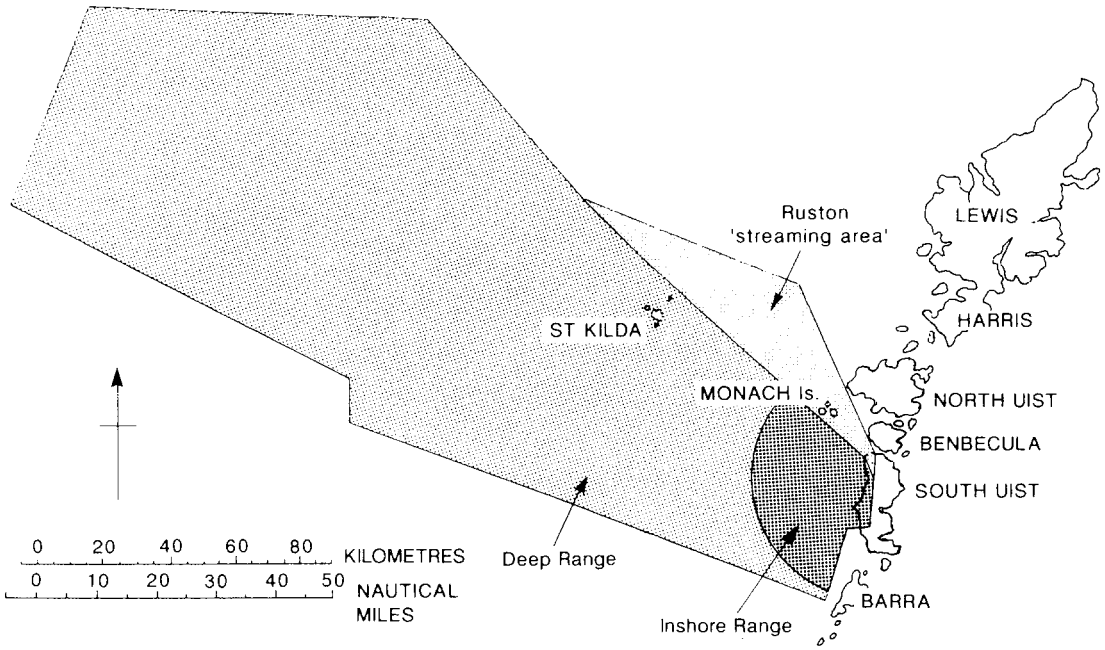

FIG. 1—ROYAL ARTILLERY RANGE, HEBRIDES, RANGE AREAS

The Royal Artillery Range Hebrides

The purpose of this presentation is to discuss the safety experience associated with the early stages of the introduction of a new central computer and communications system at the RARH. The present system was introduced in the early 1970s, with major additions being made in 1980/81. It has a number of operational limitations and is coming to the end of its useful life.

Before becoming involved in detail we will describe the environment in which the new computing system will operate and give an outline of the requirement. The main function of the Range is to provide facilities to conduct live firing safely and to assess the performance of a full range of in-service and trial weapon systems.

The Range is located in the Outer Hebrides with facilities spread over a number of sites. As can be seen from FIG. 1, the range danger area extends into the Atlantic some one hundred and sixty miles; the Island of St. Kilda, which is situated 57 miles down range, is used for the installation of some range surveillance and control equipment. For planning purposes the Range is divided into two:

- The 'Deep Range' into which long, medium and intermediate range surface-launched land-based missiles and targets such as Lance and Sea

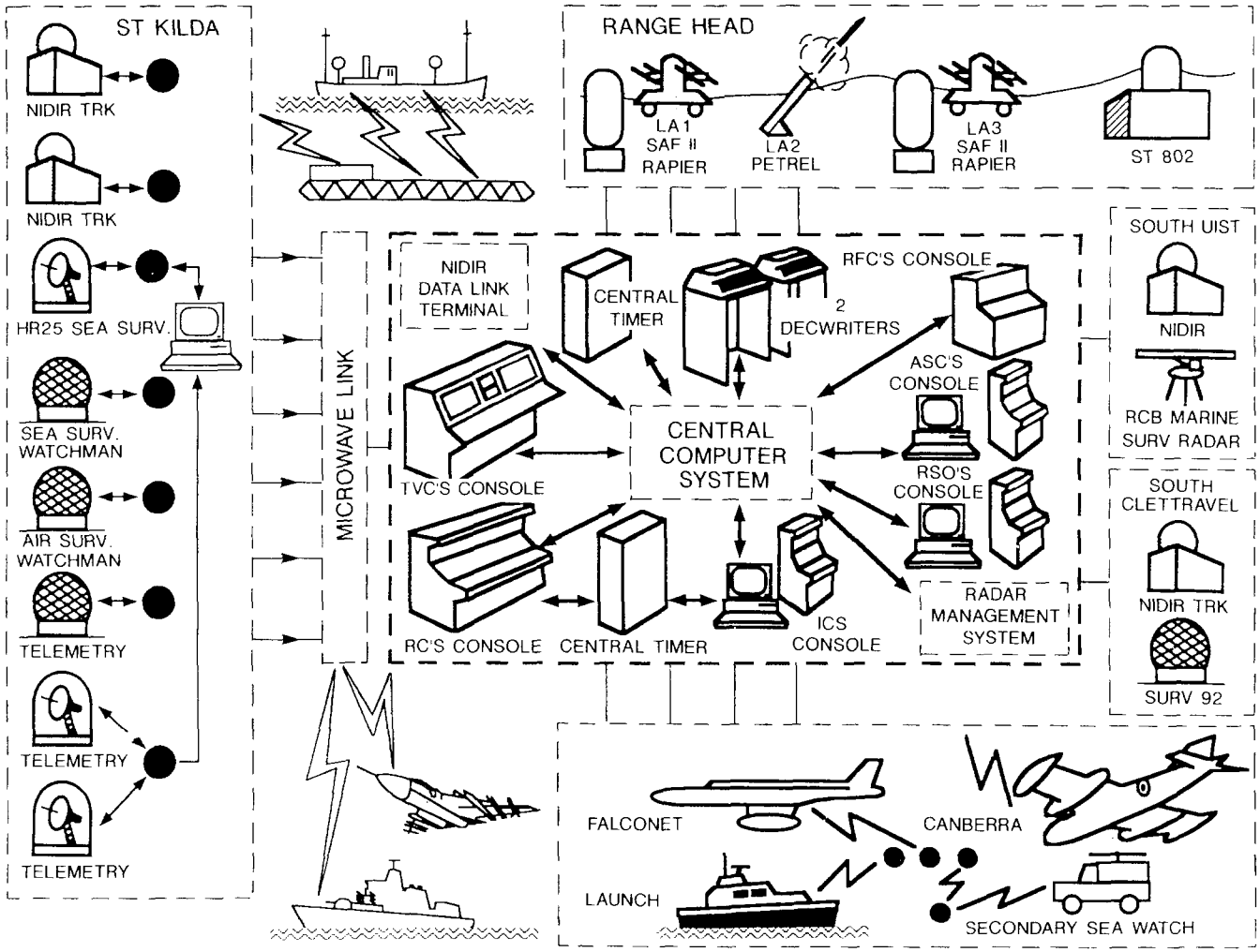

FIG. 2—RANGE CENTRAL COMPUTER AND COMMUNICATION SYSTEM UPDATE BOUNDARY

Petrel and where sea-borne weapons such as Sea Dart and airborne weapons such as Sea Eagle are fired.

- The 'Inshore Range' where short range surface-launched air defence weapons such as Rapier and Javelin and their associated targets (Falconet and Skeet) are exercised.

A major limitation of the present computer system is that it allows only one of the 'Ranges' to be active at a time. A key requirement for the future system is that concurrent activity on both ranges must be possible. This made it necessary to define in clear terms the meaning of concurrent activity with respect to possible activity within the Range as a whole including the land danger areas.

The central computer system is located in the 'Range Control Building (RCB) on South Uist. Its purpose is to:

- Monitor and display the air and sea surveillance picture in and around the Range produced by surveillance radar.
- Present to the appropriate safety officers details of weapon danger areas and zones, which can be superimposed upon the air and sea surveillance returns. This is at present achieved with the use of computer-driven cursive displays.
- Assist in the control of tracking radar, telemetry systems and remotely controlled targets.
- Record data for later analysis.
- Provide training facilities including 'dry exercises' to the range staff.

The complexities of the problem are shown in FIG. 2, where the area shown within the heavy dotted line is that part of the system covered by SR 4017.

The future system will be required to handle information from a variety of sources:

- Static air and sea surveillance radar located at South Cletraval (a mountain on North Uist), St Kilda and South Uist, and mobile radar deployed along the coastline of South Uist. These are supplemented by long-range maritime patrol aircraft such as Nimrod as and when required.
- Telemetry.
- Tracking radar located on St Kilda, South Uist and South Cletraval.
- Information from participants, such as aircraft or ships.

In summary the safety objective of the whole system is to detect the entry of intruders into the range danger area, inhibit launch if the range is not clear or to terminate the flight of missiles or targets if they develop a malfunction which could result in either or both transgressing the pre-planned danger area.

Organization of the Project

In the contractor selection phase of the project, the Board's role was concerned only with advising the project manager on the safety principles to be applied, with a particular emphasis on the use of safety critical software. The project manager is responsible for the implementation of this advice.

Feasibility Stage

The feasibility of introducing a new computer system onto the range was investigated by Theta Analysis and Systems Ltd. Three issues were resolved in 1989 before Theta produced their report:

- The Board would assist in the formulation of the safety policy statement and would refer to Draft Interim Def Stans 00–55 and 00–56.
- The Range Safety Officer (RSO) would retain authority for all range safety decisions. The RSO would intrepret the information presented by the

computing system; hence he or another designated safety officer would remove the firing inhibit or initiate flight termination as required. The integrity of the information presented to the RSO must be assured.

- When modelling range safety, the related factors must be agreed by all relevant parties beforehand.

The Theta report was published in August 1989. The Board contributed to Annex G, 'The Policy Statement for the Provision of Safety Critical Software'. This annex was intended to provide guidance in the provision of software to ensure that the requirements in safety critical applications were appropriate to the operational needs of the Range. It did not address the overall safety problem, which was examined later in the preliminary hazard analysis as part of the system design stage. The policy statement stated clearly that in the event of conflict with Draft Interim Def Stan 00–55 and 00–56 the policy statement would take precedence.

The policy statement covered the following areas:

(*a*) The aims of the policy.
(*b*) Assumptions and constraints.
(*c*) When the policy was applicable.
(*d*) Actions required to show compliance with the policy.
  (*i*) Methods and practices applicable to the design.
  (*ii*) Methods and practices for safety critical elements.
  (*iii*) Design characteristics.
  (*iv*) Monitoring and supervision.
  (*v*) Documentation.
  (*vi*) Acceptance and certification.

System Design Phase

From a short list of five contenders in the contractor selection phase, two consortia were selected to compete in the system design phase.

The MOD Safety Assurance Working Party

The purpose of the working party is to review the working papers and draft deliverables as tasked by the project management committee and to advise on the safety aspects of the system design phase. Particular emphasis is placed upon the preliminary hazard analysis and risk assessment.

The following are represented on the MOD Safety Assurance Working Party:

- The Project Manager, as chairman.
- The head of the Project Management Support Team (PMST).
- The Ordnance Board, which performs the function of the MOD Safety Assurance Advisor (SAA).
- The RSO from RARH representing the user.

The Development of Safety Targets

As it was recognized that the establishment of safety targets would be a difficult task, the inaugural meeting of the MOD Safety Assurance Working Party agreed that the Project Manager and the Officers of the Board would collectively propose a way forward. It was agreed that a computing system failure leading to no information being presented would not result in a long-term hazard, as appropriate inhibition of firing or flight termination would be taken as an immediate action by the RSO. The most hazardous situation was one in which the range safety officer was presented with misleading information on which to make safety decisions.

It was decided that the limitations of the inputs provided to the computing system had to be considered in the definition and specification of the system. There was no point in having a computing system capability vastly in excess of that required to handle the available input data. In the ensuing discussion the following safety targets were agreed:

- *Accuracy of Display*:
  (*a*) Temporal. To 100 msecs. This figure was based on the relationship between the speed of a contact and the display resolution on the largest scale display.
  (*b*) Spatial. Within a sphere of 22 m diameter. This was based upon the likely display resolution of the largest scale display.
- *Corruption of Information by the Computer System*: In order to give the RSO confidence in his display it was agreed that the incidence of a single error occurring in a set of data should not exceed 1 in 100. If this was exceeded the RSO should be alerted automatically within 1 second, allowing a period of time that was considered reasonable for a flight termination or inhibit decision to be made.

It was considered that when assessing the probability of anyone being injured or killed during a trial or live firing (a 'range event') at the Range two discrete probability criteria had to be met. These are:

- A probability of injury or death from any one range event.
- An accumulated injury probability over any one year period at the Range to resident individuals, i.e. range staff.

Ideally the criteria should have a high confidence level associated with them but it was recognized that some of the data to be used in the analysis would be subject to technical judgement in selection.

Discussions Leading to Hazard Analysis

An informal meeting then took place between the Project Manager, officers of the board and each of the competing consortia at which minutes were not taken. The discussions were free-flowing and open-ended. The meetings were considered by the Board as the beginning of an iterative process which would lead to a method of risk classification which would evolve into a balanced and complete preliminary hazard analysis. The following matters were covered:

(*a*) The Board's Philosophy behind the generation of danger area traces was explained. A comparison was made between those danger areas associated with systems fitted with a flight termination system and those that were not; the differences were highlighted.

(*b*) The experience of the RSO must not be underestimated and he must not be left out of the safety loop otherwise the computing system would automatically become safety critical as was stated earlier.

(*c*) It was stressed that as a hazard was identified a probability and mean time at which it could occur were to be assigned to it. It was accepted that it might be difficult to utilize figures at an early stage and a qualitative approach might have to be adopted.

(*d*) It was confirmed that the policy document would take precedence over the two Draft Interim Def Stans but if some of the processes were assessed to be safety critical the spirit of the Def Stans would be followed. The interpretation of the phrase 'in the spirit of' did cause some heartache later in the project. It was stressed however that the Ministry aspired to a system that was not safety critical.

The Development of Risk Criteria

As a result of these meetings it was agreed that the Board would examine the possibility of assigning values to the probability classes given in Def Stan 00-56. This became an iterative process between the project management team and the Board. It was agreed that the figures given had to be project specific, i.e. they could only be applied to the RARH new computer system and those of its peripherals having a lifetime of greater than ten years. The figures used are not to be taken as a precedent for any other projects. The Board's initial proposals are shown in TABLE I.

TABLE I—*Quantifying probability—the Ordnance Board's first proposals for boundaries between categories*

Incredible	*Improbable*	*Remote*	*Occasional*	*Probable*	*Frequent*
Once per 100 system lifetimes or per 10,000 yrs	Once per 10 system lifetimes	Once per system lifetime	Once per year	Once per month	

The most important boundary was considered to be that between 'occasional' and 'remote'. It was considered acceptable that an 'occasional' failure would occur during the life time of the system and that a 'remote' failure should not occur during the system lifetime. Around this a logarithmic scale was drawn up and adjusted using technical judgement.

Subsequently these proposals were expanded into those given in TABLE II, which assumes a 10 year system life.

TABLE II—*Quantifying probability, assuming a 10 year system life*

Frequent	$>10^{-5}$ per event
Probable	10^{-5} to 10^{-6} per event
Occasional	10^{-6} to 10^{-7} per event
Remote	10^{-7} to 10^{-8} per event
Improbable	10^{-8} to 10^{-9} per event
Incredible	$<10^{-9}$ per event

Using the Adelard proposals which have since been incorporated into the Interim Def Stan 00-56, TABLE III was produced in which the frequency of range events and severity classification were used to define risk categories.

TABLE III—*Definition of risk categories A, B, C and D*

	Probability per Range Event	*Catastrophic*	*Critical*	*Marginal*	*Negligible*
Frequent	$>10^{-5}$	A	A	A	B
Probable	10^{-6}	A	A	B	C
Occasional	10^{-7}	A	B	C	C
Remote	10^{-8}	B	C	C	D
Improbable	10^{-9}	C	C	D	D
Incredible	$<10^{-9}$	D	D	D	D

A probability/risk classification matrix (FIG. 3) was constructed to show lines of constant risk relating to the project and the safety target. Its intention is to introduce the project's interpretation of assurance level for protection

against systematic failure. Line 1 on the diagram represents a line of constant risk that is unacceptable and line 2 the desirable maximum risk. The zone between represents the safety critical region. Risk class A is unacceptable. Risk class B will require that software is produced with assurance Level 1 against systematic errors, the production of a formal specification, a formal 'safe sub set of Ada' and the use of static analysis to provide verification that the specification has been implemented correctly. These procedures are in addition to the validation required which will include comprehensive testing of the software both independent of and when incorporated within its host hardware.

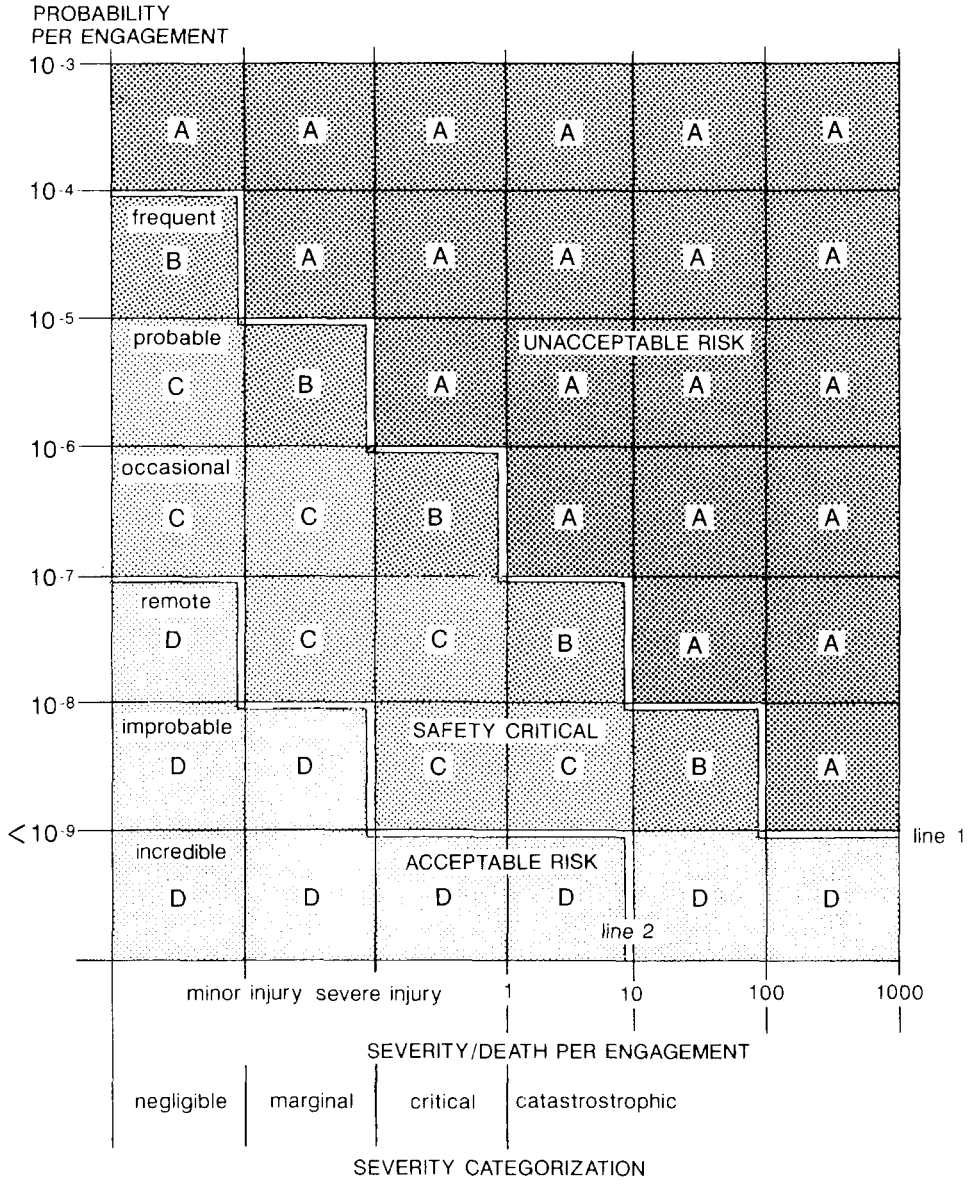

FIG. 3—ACCIDENT PROBABILITY/SEVERITY MATRIX AND HAZARD RISK CLASSIFICATION
(for definition of risk categories A-D, see TABLE III)

Risk class C will require that software is produced with assurance Level II against systematic errors. Code generated should be analysable by static methods; however, it would not be necessary to validate the code against a formal specification. The requirement to test the software comprehensively, both independent of and when incorporated within its host hardware, remains.

Safety Assurance Plans

Concurrently both system design consortia produced their respective safety assurance plans. MOD(PE) defined the roles of the various agencies and individuals involved in the monitoring of the safety standards applied during the project. It is of interest that the Ordnance Board accepted the role of the Ministry of Defence Safety Assurance Authority, which is a departure from the normal policy of the Board. The independent status of the Independent Safety Assessor (now the Independent Safety Auditor) was discussed and it was agreed that he could be a sub-contractor within the consortia but that he must have an independent line of management. Both plans detailed the scope of work required and the tools that were to be used in the conduct of the safety assessment, and they listed a number of safety milestones to be met.

The Preliminary Hazard Analysis

The activities associated with the preparation of the preliminary hazard list and the preliminary hazard analysis were conducted concurrently by both companies. Hazards were identified during visits to the Range during periods when the deep range was in use, by studying the environment and current documentation and by discussions with the range staff and others. A list of safety-related incidents that had occurred over a period of years was produced by the Range.

The project management team considered that the purpose of the preliminary hazard analysis was to assign risk classifications to the identified hazards associated with the range environment, without considering the effect of the computer system on safety. Some problems arose due to the natural inclination to consider the safety implications of the computer system. The Project Management Safety Assurance Working Party believed that the contribution of computer failure to risk assessment belonged in this case to a system hazard analysis since the allocation of failure probability would require design knowledge not yet available. The relationship between preliminary, system and sub-system hazard analysis will generate considerable discussion within future projects. However we are sure that a flexible approach is more sensible and rigid rules will be avoided. After all rules are for the guidance of wise men and the obedience of fools.

The early drafts of the preliminary hazard analysis produced by each company failed to appreciate that the key to range safety at RARH was the ability to detect intruders of all types. If an intruder was detected the Range could take the appropriate firing inhibit action using proven hardware based fail safe systems; thereby reducing considerably the level of risk. There was some difficulty in illustrating accident sequences and after some thought it was suggested that a series of block event trees be used.

A further problem was encountered in the application of the safety targets for risk probabilities per year instead of risk probability per event. It was apparent to the Board that the concept of cumulative risk had not been fully appreciated. A member of the range staff such as the visual flight safety officer who is present at up to 1000 firings a year is at greater cumulative risk than a weapon system operator who is only present at a single firing. A cumulative risk is only appropriate to range staff or local inhabitants living and working on or close to the range.

Both companies have completed preliminary hazard analyses and each assigned a risk class to accident sequences relating to generic events, e.g. those involving guided weapons, ballistic weapons, sea skimmers, unmanned aircraft, etc. Some recommendations were made that could be fed directly into the preliminary design, others were more appropriate to the implementation phase. Def Stan 00–56 makes no reference to a review of risk classes after the

preliminary hazard analysis has been delivered. It is essential that these should be reviewed with the Independent Safety Auditor, the MOD Project Manager and his advisors to avoid nugatory design work.

Before the preliminary hazard analysis was started work on producing a User Requirement Specification (URS) commenced. Drafts of the URS were continually reviewed and as a result it is hoped that all the requirements for the system have been correctly described (FIG. 4). Successive versions of the URS provided the input into high level documents which may be termed the system logical and physical designs.

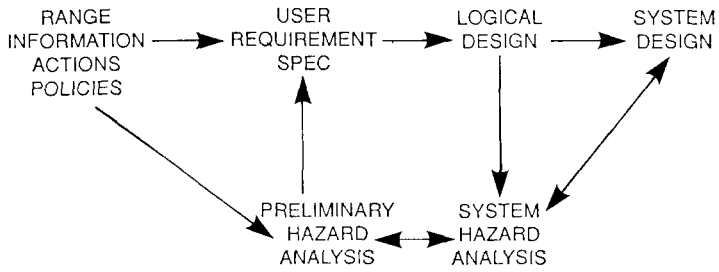

FIG. 4—HAZARD ANALYSIS IN THE DESIGN OF A SYSTEM

System Hazard Analysis

At present the system hazard analysis examines the logical design, cataloguing the ways in which a system failure may relate to the hazards defined in the preliminary hazard analysis if corrupt or partial information is presented to the range safety officer.

It is essential that hazards, functions, processes and components are systematically cross-referenced by a numerical code. This code should apply to both hardware and software elements; for the latter, functional groups of modules and individual modules should be coded just like a hardware sub-system or component. Such a code will enable the migration of hazard to be traced through interacting functions or processes, allowing the direct and indirect effects of failure to be studied.

The system hazard analysis also considers Common Mode Failure (CMF). Protection against CMF is achieved by maintaining independence between different parts of the system. The inhibit and destroy sub-systems are examples. The system hazard analyses investigated the interaction of the functions, such as the power supply and the role of the range staff, at the logical level. In addition both analyses have investigated the top level design for the inhibit and destroy sub-systems and the means by which redundancy and monitoring processes can be used to provide defences against single and common mode failure. The system hazard analysis at this stage cannot provide assurance regarding the accuracy or corruption during overload conditions; information on this area will only become available during the implementation phase. It follows that the system hazard analysis is a process that continues throughout the life of the project and as a design matures the system hazard analysis has to be reviewed.

Independent Safety Audit

Both consortia appointed sub-contractors as Independent Safety Advisors or Auditors (ISA). This was agreed by the Board provided that there was an independent chain of management. It is important that representatives of the ISA are involved in the development of the Design Authorities proposals and criticize drafts of the Preliminary Hazard Analysis and the System Hazard

Analysis; however, both these documents must be deliverables* to the MOD Project Manager.

An Independent Safety Assessment Report should be prepared separately by different individuals. This report may be incorporated as an annex within the PHA and/or the SHA as appropriate or as a separate deliverable. The latter approach is preferred, particularly if the MOD have indicated that individual deliverables will be commented on. This was the case in this project.

Divergence from Def Stan 00-56

The last problem to be mentioned resulted from the immaturity of the Draft DEF STAN 00-56.

It had already been agreed that the policy given in the feasibility study would take precedence. As a result it was agreed that it was the risk level that had to be identified and which would identify the software procedures to be followed rather than the identification of various integrity levels.

Conclusions

The following recommendations are made with regard to the future development of Def Stan 00-56:

(*a*) There is a need to clarify the user requirements and to attempt at an early stage to understand what is required of the system. Requirement capture as a whole should have a Def Stan of its own.

(*b*) The subject of safety integrity needs to be reviewed to make it easier to understand, i.e. 'user friendly'.

(*c*) Mitigating circumstances need to be examined, particularly in cases where the total probability of malfunction comes from several independent failure modes involving hardware and software.

(*d*) The need to relate hazard analysis activities to a project life cycle is confirmed. Since the activities should be reported in deliverables to MOD, timing is important so that comments can be incorporated into early design definitions. Cross-referencing and traceability of functions and components forwards and backwards into the documentation is very important. In this context structured configuration management systems should be used.

(*e*) Some benefit accrues to the MOD in that the use of the method suggested in Def Stan 00-56 has made both consortia more aware of the wider issues relating to the computer replacement. They gained knowledge of the functions which are mission critical in addition to those that are safety critical and can thus focus design and testing effort accordingly.

Final Note

Finally we must stress that the replacement of the RARH Central Computer System is a specific project, with its own particular problems. Thus none of the figures or criteria referred to in this presentation should or can be used as a precedent on any other project.

References

1. Geary, K.: Safety management—the background to Defence Standard 00-56; *Journal of Naval Engineering*, vol. 33, no. 2, Dec. 1991, pp. 251-258.
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.

* A 'deliverable' is a document contractually required to be supplied by the contractor to the Project Manager.