DEFENCE STANDARD 00-56

A COUPLE OF DATABASES TO ASSIST THE PROJECT SAFETY CASE

BY

NICHOLAS HALES MSc BENG(HONS) AMIEE
(Sea Systems Controllerate, Bath)

ABSTRACT

This article describes the concept and implementation of two database systems for projects developing safety cases. The databases are designed to assist by, in one case, providing information on how previous projects approached (Hazard Analysis), and by automating the process of recording and using the Hazard Log (database for the Hazard Log).

Introduction to the databases

The use of Interim Defence Standard (IDS) 00-56,[1] is widespread but as yet some activities necessary to fulfil it's requirements remain unsupported. Much that is needed as policy is given under the auspices of the new Ship Safety Management Office, primarily in the form of the requirement for a safety case for each project.

As the previous article in the *Journal*[2] states with regard to the record of safety management performance:

> 'The value of this process is . . . the positive shift up the safety management learning curve . . . '.

IDS 00-56 recognizes this continuous learning from experience and in the performance of Preliminary Hazard Analysis (PHA) using previous data and in the records the hazard log provides, this objective is substantially fulfilled. The following appears in the standard:

> 'Previous actual in-service incident and accident data relating to similar or other applicable systems shall be reviewed to identify hazards and accident scenarios that may be associated with the new system. Should a hazard analysis or safety risk assessment of a similar system be available, it may be used as a source of data; . . . '

The latter is of course with caveats. In addition the maintenance of a hazard log has been recognized as central to the process of assuring safety to certification requirements. It provides a record of what causes hazards, how the likelihood develops and the expected consequences.

In view of his then imminent retirement and the problems he foresaw in passing on experience, the previous Head of SS646 (Norman ELLIS), requested the weapon safety committee approve the development of a database. This to be done in order to provide a means by which the sometimes rapid turnover in staff in MoD positions, and the consequent loss of expertise, may be ameliorated. It has also been the desire of the Head of SM836 (Kevin GEARY), to be able to provide projects with a computerized hazard log, among other safety tools. A contractor has developed an ORACLE based system, but this is heavy on computing requirements.

This article outlines:

- The major features of the developed databases.
- How the designs assist the objectives of IDS 00-56 and the Ship Safety Management System (SSMS).

- The tool used in the developments and the minimal requirements of the run-time system.
- The demands on users for a significant pay-off in the case of the PHA database.
- The availability of the systems.

System features of the PHA Database

The system is built on the principle of a suite of databases, three in all, two of which are linked by pre-programmed query bases of which there are four. In addition there is a menu from which a system type may be selected, for example detonator or torpedo. Choosing an item from this menu sorts all records relating to that subject into a file, which may subsequently be printed out. Thus a project starting the safety analysis phase of a new Close in Weapon System (CIWS) for instance, may make reference to the facts and opinions of those involved in the development, procurement and safety certification of previous CIWSs. All this is done using a user-friendly interface (FIG. 1), so that most users need only input data to add to their own received database, when they find themselves in possession of safety related papers, and select from menus for all other requirements. The system runs in Windows or from DOS and provided the Windows version is 3.0 or above, an icon to assist selection from Windows can be added. No expensive application need be purchased for those only adding or deleting data, making queries, and obtaining print-outs, although anybody wishing to tailor the generic to their own requirements will need a copy of Dbase IV.

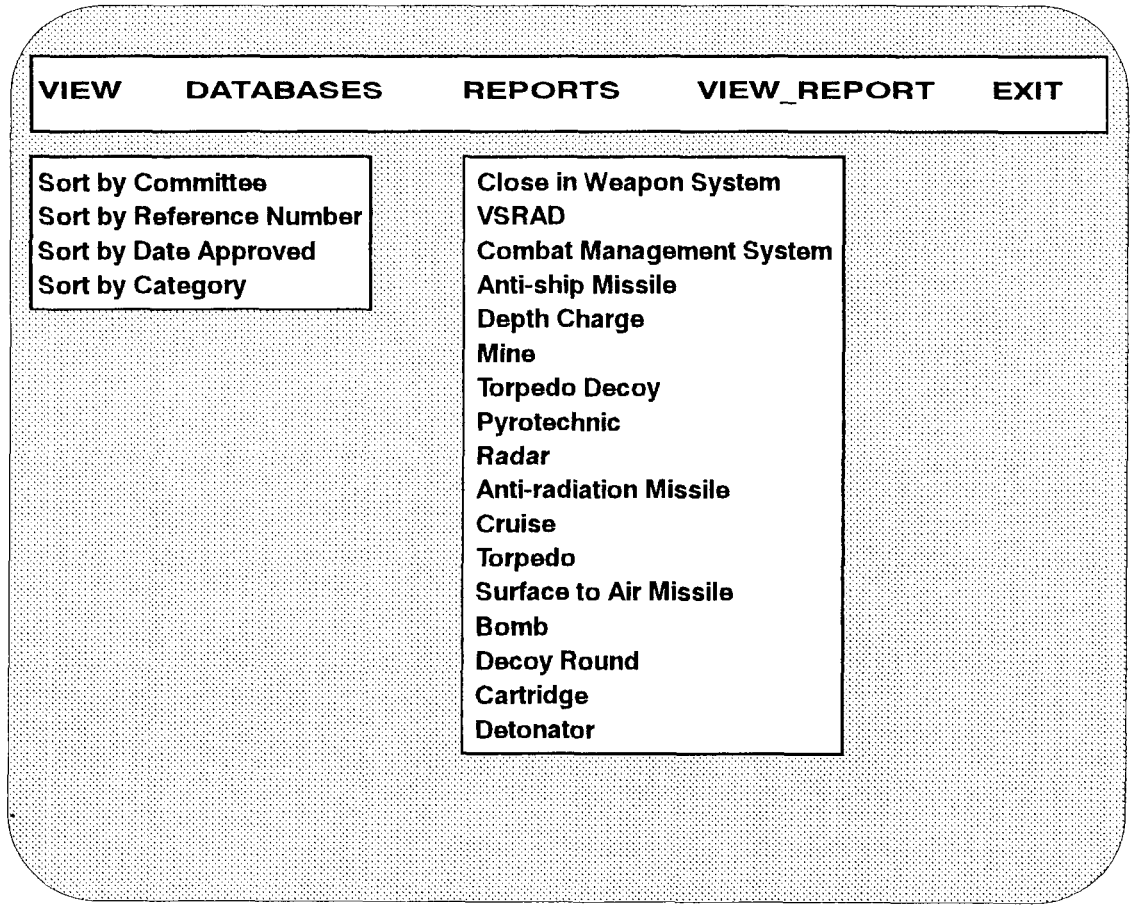


FIG. 1—FACSIMILE OF THE MAIN MENU SCREEN OF THE PHA DATABASE
TWO DROP-DOWN MENUS SHOWN, BUT IN REALITY ONLY ONE WOULD APPEAR AT A TIME

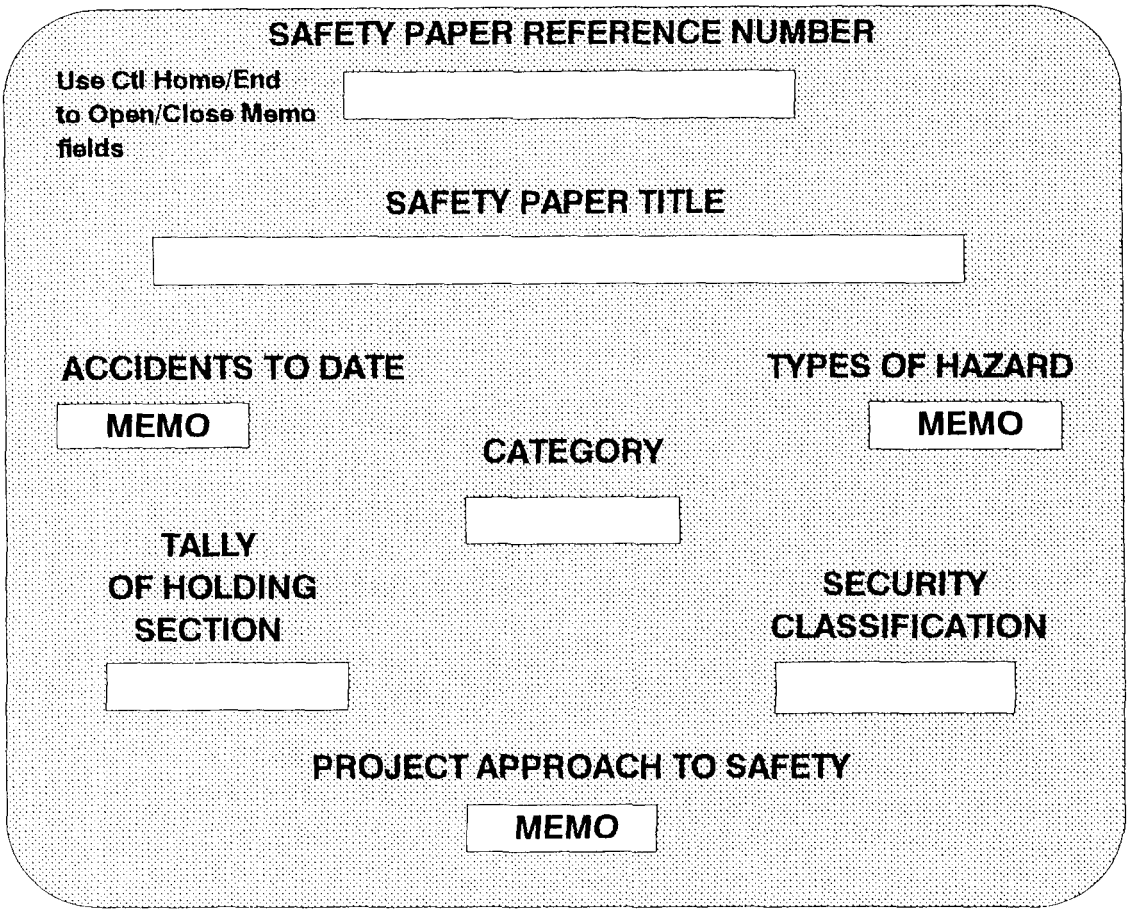


FIG. 2—FACSIMILE OF THE INPUT SCREEN OF THE SAFETY PAPER DATABASE

A typical project query may start by examining the standards database, which is not linked to query files, for typical standards in the project specific safety area. The next task may be the selection of the query menu item which sorts the two linked databases, dealing with safety papers and committees, into type order. Doing so will permit the user to identify those committees and safety papers which dealt with that type of system. Having identified them, the user may then view the actual records in their screen format (FIG. 2). When viewing in this way the memo fields may be examined. These are normally hidden and much of the detail of what was done, what accidents have occurred etc can be recorded in them without cluttering screens. Finally, either the section holding the papers of interest may be contacted, in order to recover a copy, or a print-out of the information relating to the system type may be obtained, including the memo fields (FIG. 3).

How the PHA Database serves the objectives of IDS 00-56 and the SSMs

This system offers a number of direct benefits to the SSMS, as described in the ship safety handbook which it is anticipated will be on circulation by the publishing date of this article, and assists in fulfilling the requirements of IDS 00-56.

There is, unfortunately, a dearth of easily available data from previously procured systems, despite the fact that somebody must hold the data somewhere. This system goes a long way towards addressing that crimp. The major advantage for projects using Defence Standard 00-56, is that a pool of data from previous work is either immediately accessible or a simple phone call away. This alone could save the MoD (PE), in terms of consultancy fees, tens of thousands of

This report shows the records selected by category and their memo contents.

CATEGORY	TORP
DESCRIBE	SPEARFISH FIRING INTERLOCKS ON VANGUARD CLASS SUBS
MSP_REF	C305040
ACCIDENTS	None known as at 6/12/93.
UNIQ_HAZ	Significant omissions in the areas of explicit management responsibility and quantitative attributes for safety. Best that can be said is "No grounds for concern". Functional failure analysis revealed two potential malfunctions: 1. The interlock may permit firing to proceed when the system is in the correct state. 2. The interlock prevents the firing when the system is in the correct state. The latter causes most concern and the principle of a 'Battleshort' needs to be addressed in future.
WHO_HOLDS	SM836B
SEC_CLASS	RESTRICTED
APPROACH	Done retrospectively as 00-56 not in force during development. Done to best possible principles of 00-56 bearing in mind the lateness of the attempt to satisfy safety concerns.

FIG. 3—TYPICAL PRINT OUT FROM THE PHA DATABASE
(EXAMPLE SHOWS WHEN ONLY ONE RECORD ON TORPEDOES IS IN THE DATABASE)

pounds every year. It also provides the foundations on which the safety case required by the SSMS may be built. A guide for project teams involved in procuring safety critical software[3], also mentions that it is expected that for the most part, PHA will be done in-house by the MoD rather than by consultants. So it is essential that a large pool of experience is available, and this can be recorded for posterity with this system.

Equally when personnel thoroughly versed in safety issues move on to fresh pastures, typical problems can be addressed with a much reduced risk of oversight by new, less experienced staff through reference to the database.

Having the development in house means that the data which individuals collect can be collated. Each user may use the Export facility and send a disk of the data thus output to SM836. All such disks can be imported to the master system and then returned to users with an upgraded database, which they may then add to their own system using the Import facility. This enables the cross-fertilization of ideas, essential in the early stages of safety assessment.

As a spin-off, a standards database has been added which has 60+ standards at the time of writing. This may be useful in deciding which standards to apply to systems related to safety, as part of the contract. The user may add to this his own set related to any subject at all, and may track those already on the system as their status and issue numbers change, as they so frequently do.

Demands on users of the PHA Database

In order to maintain a comprehensive and up to date database for new projects to use, users will be asked to supply updates at about six months to one year intervals. Of course there will be no pressure on individual users to supply data but hopefully most people will input safety papers they examine from time to time.

Hazard log system features

The system is the more significant of the two and is built on the principle of a suite of databases, three or four in all depending on the version. These are for the hazards themselves, the accident sequences leading to them, the main components involved in initiating the accident sequence and lastly in two versions the sub-components. In addition there is a menu for quick queries, a special query linking particular fields from all databases for an overall view and a menu to identify and obtain print-outs of the remaining big risks. All this is achieved using a user-friendly interface, (FIG. 4). The system runs in Windows or from DOS and provided the Windows version is 3.0 or above, an icon to assist selection from windows can be added. No expensive application need be purchased to use the system as already compiled.

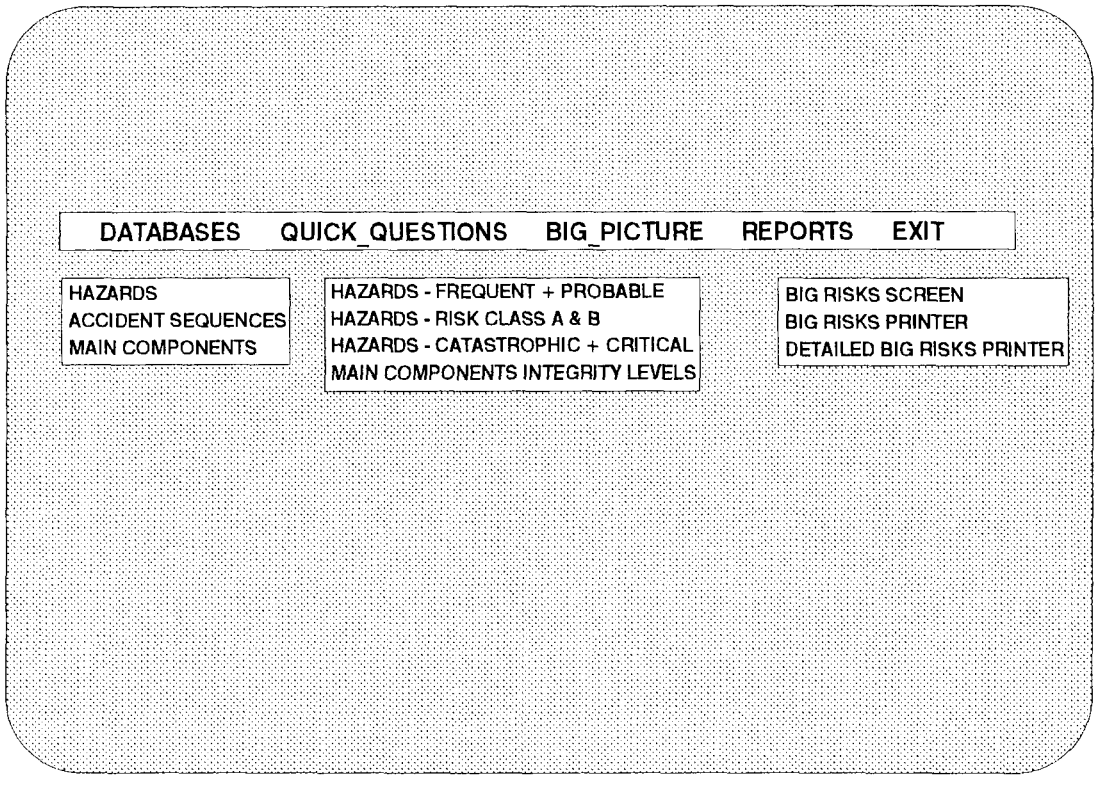


FIG. 4—FACSIMILE OF THE MAIN MENU SCREEN OF THE HAZARD LOG
THREE DROP DOWN MENUS 'DATABASE'; 'QUICK QUESTIONS'; 'REPORTS' IN REALITY ONLY ONE WOULD APPEAR AT A TIME

A typical 'Quick Question' may be examination of the database for high risks, hazards with a high probability of occurring, hazards causing the severest accidents or components and their safety integrity level. A set of fields is presented enabling identification of for example in the latter case, all components of safety integrity levels S4 and S3, showing:

- The safety target.
- The actual achieved level of safety.
- The integrity level.

- The accident sequence involved.
- The component reference number.

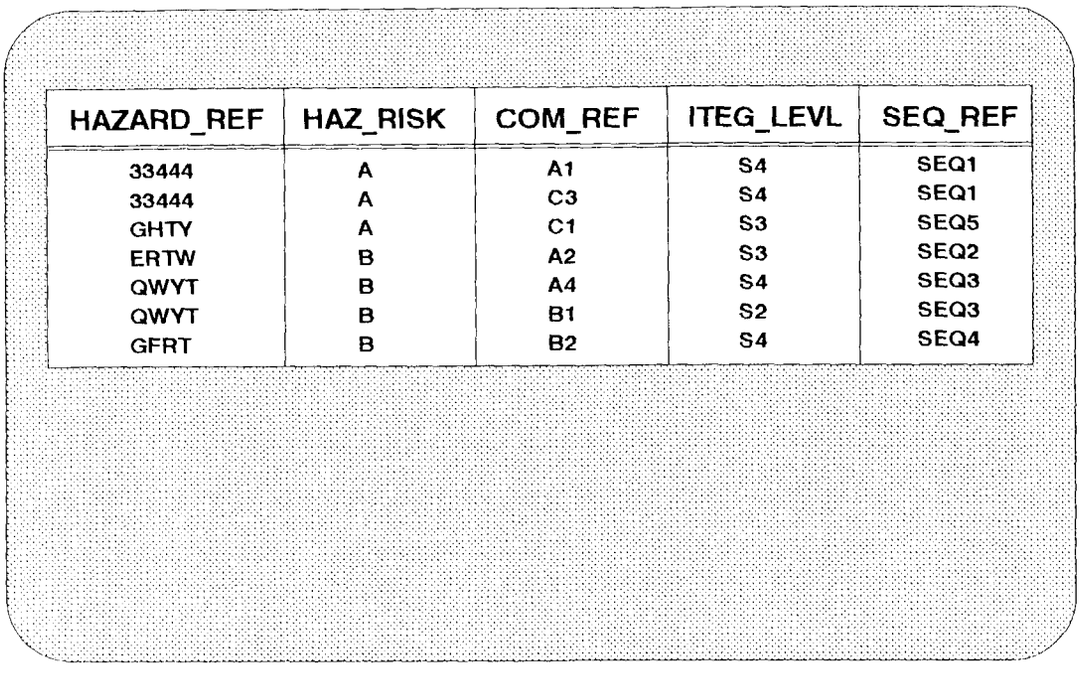
The BIG_PICTURE links the databases to provide a view of the risk classes A and B with the components involved and the accident sequences that lead to the hazards which are also given. The reports menu allows the user to print-out the big risks shown on the previous menu and also enables the user to obtain the print-out of the big risks either with or without the data in all the memo fields in addition. A typical print-out using test data is given at (FIG. 5), that includes the memo fields. These are normally hidden and much of the detail of what was done, what still needs to be done etc. can be recorded in them without cluttering screens. (FIG. 6) shows a facsimile of the screen view of the BIG_PICTURE, the choice of index can be selected by users experienced with Dbase IV, this one shows the selected fields sorted on Risk Class (HAZ_RISK column).

HAZARD REFERENCE NUMBER	12345
HAZARD DESCRIPTION	The cam may malfunction leading to the weapon firing at indiscriminate targets.
ACCIDENT SEQUENCE NUMBER	as123
RISK CLASS	a
MAIN COMPONENT	mcl
SAFETY INTEGRITY LEVEL	s4
COMPONENT DESCRIPTION	hardware cam
NOTES ON COMPONENTS	This cam is made of titanium steel but in trials to destruction held at Lancaster University has had a figure attached to the probability of failure which is below the safety target. It would be too expensive to procure a new cam based on a superior metal mix and the timescales for implementation would be excessive.
SUB-COMPONENT REFERENCE	sc1
SUB-COMPONENT INTEGRITY	s3
SUB-COMPONENT DESCRIPTION	cam pivot
NOTES ON SUB-COMPONENT	This particular component has shown itself to be capable of meeting the safety target in all trials so far conducted.

FIG. 5—TYPICAL PRINT-OUT FROM THE HAZARD LOG

The objectives of the IDS 00-56 hazard log

This system offers advantages over other systems known to SM836. It is very light on computer space and as such can be used by the smallest projects without problems. It also costs the project nothing, so should reduce the charges to which the contractor feels the MoD is liable. The system will provide the MoD with a standard format for hazard logs which will greatly reduce certification timescales and the data can be extracted and analysed, if this becomes a useful and necessary requirement, into LOTUS 123 for instance.



HAZARD_REF	HAZ_RISK	COM_REF	ITEG_LEVL	SEQ_REF
33444	A	A1	S4	SEQ1
33444	A	C3	S4	SEQ1
GHTY	A	C1	S3	SEQ5
ERTW	B	A2	S3	SEQ2
QWYT	B	A4	S4	SEQ3
QWYT	B	B1	S2	SEQ3
GFRT	B	B2	S4	SEQ4

FIG. 6—FACSIMILE OF THE SCREEN VIEW OF THE BIG PICTURE

It is flexible, there being four versions of the system. These enable the project to choose whether to have a hazard log which is strictly according to IDS 00-56 Annex E requirements, or to choose one which provides an extra database for sub-components, (the standard version only provides for main components). These two versions are both then sub-divided into two more versions which cater for different project approaches to recording hazards:

(1) Lets the user identify a hazard with a number of reference numbers for each accident sequence leading to it.

(2) Permits the user to identify the hazard using the same reference regardless of how many accident sequences lead to it.

Some projects may find one approach easier than the other.

As reports of usage are made, adjustments can be made to the system without great expense as it is in-house and takes very little time to tailor. Additional Dbase IV features could be added at a later stage including Password control, should these prove necessary.

Demands on users

None

Development and run-time requirements of both systems

The systems were developed using Borland Dbase IV (previously owned by Ashton Tate). The great advantage of the delivered systems is that they have been compiled using the fairly recent Borland Dbase IV compiler. In effect, the only thing a potential user requires is an IBM compatible PC running MS.DOS. Each system is supplied on two disks which when loaded using the methodology described in the documentation accompanying the development, create a run-time environment of about 2.5 Mbytes on a hard disk.

The systems may be used by MoD staff only at the moment. However, it is hoped that in the near future contractors too will be able to use the hazard log in order to standardize the received format and to reduce costs incurred by contractors in preparing safety cases, charges which of course get passed on to the

project. It is intended that a record be kept of all sections holding data so that upgrades can be despatched.

Availability

The data and run time files are now available for both systems along with brief notes for the user. Readers are invited to request copies should they have need to perform PHA as part of a project or should they deal with safety matters on a regular basis in the instance of the PHA database and should they be in need of a user-friendly automated method of recording data for the project safety case in the instance of the hazard log database.

References:

1. Ministry of Defence : Hazard Analysis and Safety Classification of the Computer and Programmable Electronic System Elements of Defence Equipment. Defence Standard 00-56 (Interim); Directorate of Standardization, Glasgow, 1991.
2. Billett L. K.: The Ship Safety Management System (SSMS); *Journal of Naval Engineering*, vol. 34, No. 2, June 1993, pp. 280–294.
3. Ministry of Defence (Sea Systems Controllerate) : Guide for project managers on development involving safety critical software. [LN Length: RM, String:'_']