

DEVELOPMENT OF AN ELECTRONIC SAFETY CASE FOR A MILITARY COMMUNICATION, COMMAND AND CONTROL SYSTEM

Richard Maguire

&

Alan Garside

SE Validation Limited, Salisbury, UK
rlm@sevalidation.com

Cobham Defence Communications, Exeter, UK
agarside@whiskyalpha.com

Keywords: Electronic safety case; Military command and control; Resources

Abstract

The modern infantry soldier is expected to operate across a wide spectrum of operational scenarios from war fighting to humanitarian aid. Deployments can be National, International Single/Joint Services or as part of a coalition with other international services.

Key to success in any military operation is the ability for personnel at the combat level to manage and control their environment and to directly influence their situation. This needs to be done in real-time, through decisive actions based on sound and safe situational awareness information.

An integrated digital soldier system has recently been designed and developed, which allows combat units to monitor and react to the 'chaos of battle'. This digital mapping, navigation and communication capability has a recognised relationship to the safe operation of combat capability and as such requires an explicit safety argument with associated evidence to demonstrate that residual risk is as low as reasonably practicable.

This paper presents the real example of how the risk evaluation and preliminary safety case development was actually done for this new equipment. It was an expression of wish that the safety case would be in electronic format using graphical notations. In this way, the case for safety could be demonstrated remotely and used as programme submission evidence as part of key gateways early in the military procurement cycle.

This paper will present the key stages that the programme team went through in developing the preliminary safety case, from hazard identification through to graphical argument construction and on to publication. During this relatively short project it has also been possible to record the resource effort used through this component of the programme, so this is also presented as rich evidence for future programmes.

1 Introduction

The integrated digital soldier system (IDSS) has been designed to provide a fully integrated C4I operational capability. It consists of a bespoke personal data terminal and soldier interface unit comprising high sensitivity GPS, a digital magnetic compass, audio mixer, short & long range radio, and USB & RS232 input/output terminals.

The system offers a bottom-up process to enable fighting units to accurately populate a local operational picture. The system can be configured for several different roles, addressing the needs of Special Forces, Observers, Infantry Support Teams and other dismounted user groups. These roles and capabilities mean that the system will be used in safety related areas and so requires risk and safety assessment.

The remainder of this paper is organised as follows; section 2 will review recent historical incidents associated with dismounted operations. Section 3 will describe the derivation of the high level safety claim and strategy, along with the construction of a risk tolerability matrix. Section 4 presents the results of the preliminary HAZID process. Section 5 gives details of the construction of the electronic safety argument and safety evidence. Section 6 discusses and records the resource profile used in this exercise.

2. Review of recent historical incidents

A literature review was undertaken to identify specific accidents and incidents that have occurred that have involved a significant aspect of loss of situational awareness. It was not the intent of this paper to produce an exhaustive record and discussion on historical incidents, rather to give some grounding to the scope and nature of the safety relationship that the IDSS would be expected to contribute to. The following brief incident descriptions serve well to describe the domain of interest.

"The soldier suffered a fatal gunshot wound from a friendly element. The Soldier was in an M1115 HMMWV in an unfamiliar area after dark when his element mistook the friendly element for hostile forces. The two elements opened

fire, at which time the deceased Soldier was struck in his left lung and shoulder. Three other Soldiers suffered unspecified injuries. The Soldiers reportedly were wearing their required PPE. The accident occurred during the mid-evening.” [5]

“Two groups of Army Rangers emptied their weapons against each other without first identifying where they were shooting. In the fading light, some troops resorted to firing at muzzle flashes. Others just followed the aim of their team leader. "Some soldiers lost situational awareness to the point where they had no idea where they were." [1]

“The coroner concluded the pilots had deliberately fired on the convoy, in spite of being responsible for providing air support for coalition forces in the area. The act was a "criminal one, since the pilots broke the combat rules of engagement in failing to properly identify the vehicles and seek clearance before opening fire". He said: "The pilots chose not to take steps to confirm the identity of the vehicles in the convoy. The pilot who opened fire did so with disregard for the rules of engagement and was acting outside the protection of the law of armed conflict."” [2]

With the potential to influence accident events such as these, it was considered essential that a programme of safety and risk assessment was necessary for the IDSS.

3. Derivation of basis for safety and risk assessment

Within any safety argument a key tool is the risk tolerability criteria. This explains the relationship between accident severity, accident frequency and risk class. The tolerability of risk for this programme can then be clearly described along with proposed actions and tasks for any particular hazards with any particular level of accident risk.

With the programme status being relatively early in a procurement process, it was judged that only a basic indication of the safety framework was required. This could be used as a basis for future development of the safety analysis that could be made more focussed when a specific acquisition programme is being considered.

Consistent with any usual risk assessment, the accident risk position can only be judged against a combination of severity and likelihood – each of which must be defined at the outset.

3.1 Key Accidents

Key accidents are generic expressions of the main groupings of accident types that could be credible through the failings of the system of interest. These are usually defined in just a few groups:- Personnel, Environmental and Equipment. The UK defence standards [3] recommend that accidents are defined for each of the appropriate groups in explicit ways to allow and assist further safety and risk analysis.

Personnel: Impact

This can range from fatalities and capture to cuts, grazes and bruising

Environmental Impact

This can range from habitat destruction to very localised contamination

Equipment Impact

This can range from total equipment destruction to surface damage

3.2 Consideration of Severities

The UK defence standards [3] encourage four categories of severity:- Catastrophic, Critical, Major and Minor. The standards also recommend that each of the categories is defined in specific terms appropriate to the project or system of interest. The range of severity should be defined for all key accident descriptions. The table below proposes severity definitions across the accident types.

Severity Category	Personnel Impact	Environmental	Equipment
Catastrophic	One or more fatalities, and/or capture of one or more service personnel	Large scale damage with national significance e.g. release of hazardous gases, or permanent damage to habitats or endangered species.	Loss or destruction of project equipment AND loss or destruction of wider or neighbouring equipment
Critical	Multiple severe injuries as defined in the UK Reporting of Injuries Diseases and Dangerous Occurrences Regulations (RIDDOR)	Damage limited to a small area, or wider spread damage with minimal lasting effects on habitat or species.	Loss or destruction of project equipment
Major	A single severe injury as described in RIDDOR and/or multiple minor injuries.	Temporary local damage to a habitat or species	Damage to project equipment that leads to the equipment being taken out of service for repair.

Severity Category	Personnel Impact	Environmental	Equipment
Minor	At most a single minor injury requiring professional medical attention (may include an MO or an Army Combat Medical Technician)	Contamination of personal environment with little or no damage to habitat or species	At most cosmetic damage that does not reduce the operating capability of the project equipment

Table 1:- Severity Categories

3.3 Consideration of Frequencies

The defence standards [3] encourage the description of categories of frequency to describe a range of time periods that have relevance to the project or system under analysis. The representation of time is usually done using a logarithmic scale with the longest time span being anything beyond the expected system life. At the current stage of this project, four frequency categories are identified; these are described in the table below.

Frequency Category	Qualitative Description	Quantitative Description
Probable	Occurring on a monthly basis	Greater than $1 \times 10^+1$ per year
Occasional	Occurring on an annual basis	Between $1 \times 10^+1$ and 1×10^0
Remote	Occurring on a decade basis	Between 1×10^0 and 1×10^-1
Improbable	Occurring on less than a decade basis	Less than 1×10^-1 per year

Table 2:- Frequency Categories

3.4 Risk Tolerability

Risk is generally accepted as representing a combination of severity and likelihood and for this relatively simple exercise, there is no reason to over-complicate the practice. During the construction of this matrix the defined severity and frequency categories are set on the axes of the matrix and each intersect specifies a risk position. These risk positions can then be judged for tolerability and risk grading.

Keeping in mind the definitions for severity and frequency a matrix is constructed using a decreasing scale of risk for the reducing categories of the two properties. The resulting table

is shown below, with the familiar "A" to "D" risk classes completed

	CAT	CRIT	MAJ	MIN
PROBABLE	A	A	B	C
OCCASIONAL	A	B	C	D
REMOTE	B	C	D	D
IMPROBABLE	C	D	D	D

Table 3:- Risk Tolerability Matrix

The defence standards [3] encourage proactive determination of actions for hazards in each risk class. Preliminary proposals for these are made below and will be agreed with the customer.

Risk Class A: Intolerable except in exceptional situations, hazards with these risks shall be referred to the customer's safety panel.

Risk Class B: Undesirable but tolerable with the endorsement of the project safety committee, and only when the risk is strongly demonstrated to be ALARP.

Risk Class C: Tolerable with the endorsement of the project safety committee. A brief ALARP argument should also be recorded.

Risk Class D: Broadly Acceptable, no further action is required.

4. HAZID process and results

The objective of the preliminary hazard identification is to identify, as early as possible, the main credible hazards and accidents that may arise during the life of the system. It provides input to the Safety Case Report, initiates the Hazard Log and provides the starting point for subsequent Risk Analysis. The technique adopted is one of Hazard and Operability Study (HAZOPS) technique conducted by a group of individuals with experience and knowledge of the equipment under analysis.

The HAZID process was undertaken in two parts – physical hazards and consequential functional hazards. Both used a guideword prompt sheet; the physical hazard identification used the existing prompt sheet from older versions of the defence standard [4] and the functional hazard identification a smaller list of guide prompts. These guide-words were as follows;

- Loss – capability or data loss
- Corruption – information or data corruption
- Incorrect – information or data that is false or untrue
- Intermittent – capability or operation that is erratic
- Delayed – capability, information or data that is provided to or from IDSS late

Example results from the HAZID process are shown below

2	Hazardous Comp'n's, eg	Actions and Notes	Sev.	Prob.	Risk Class
a	Flammable substances; e.g. solid liquid or gaseous	Magnesium content (SIU). 2. Xenoy CL (GE plastics) with metal loaded-static discharge.	Major	Improbable	D
b	Lasers	No Hazard			
c	Explosives	No Hazard			
d	Asphyxiates, toxic or corrosive substances	Existing Hazard Log Item 18 - Failure of LCD Encapsulation - If the LCD breaks, don't put internal liquid crystal into the mouth. When the liquid crystal sticks to the hands, feet and clothes, wash it out immediately. TFT display not LCD. 2mm of poly-carbonate screen.	Minor	Improbable	D
		Existing Hazard Log Item 22 - Precautions for safe handling and use of battery. Refer to Material Safety Data Sheet No 1218.0072 for sealed Lithium Ion Battery Type BT-70838 - there are more than one battery type in use on this system - safety data sheets are available	Major	Improbable	D

Table 4:- Physical Hazard ID Extract

	System Function	Guide word prompt	Yes / No Hazard	Actions and Notes
2a	NAVIGATION	Loss	No	IDSS not to be used as primary navigation instrument.
2b	E.g. Mapping, terrain analysis, own positional information, navigation planning	Corrupted	N/A	
2c		Incorrect	Yes	Cross checking with other cues; wider military system as mitigation. No specific hazard with this equipment, inherent in all communication systems.
2d		Intermittent	No	IDSS not to be used as primary navigation instrument.
2e		Delayed	No	IDSS not to be used as primary navigation instrument.

Table 5:- Functional Hazard ID Extract

5. Construction of Electronic Safety Case

The electronic case for safety was constructed using Adelard's ASCE tool, although other GSN tools are available.

The first part of any GSN is to construct the top claim and top argument; this is shown in Figure 1 below.

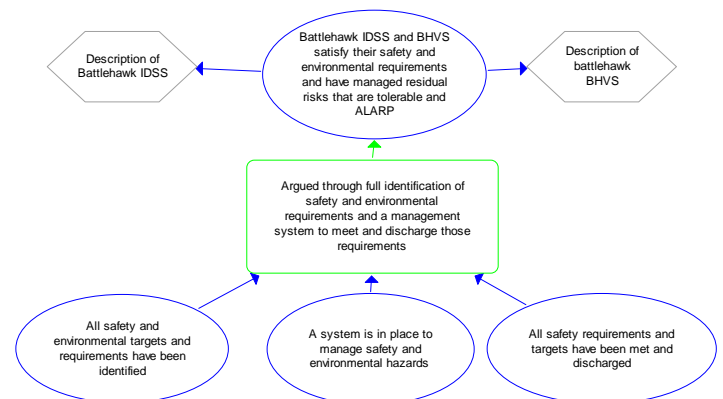


Figure 1:- Top Safety Claim and Argument

The second part of the construction was to expand out each of the three first-level sub claims. These are shown in the Figures below.

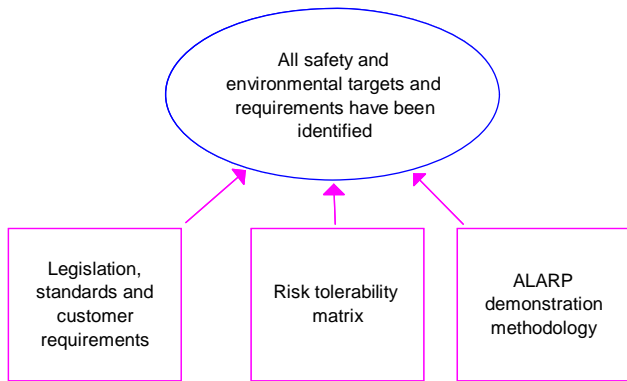


Figure 2 :- First sub-claim argument



Figure 3 :- Second sub-claim argument

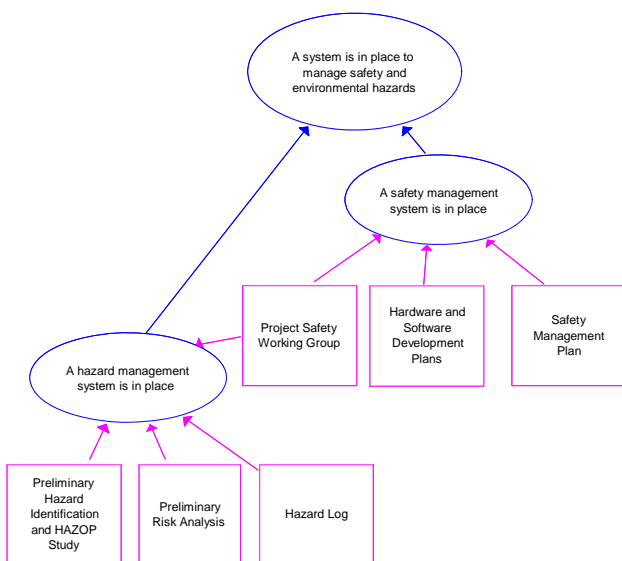


Figure 4 :- Third sub-claim argument

These structures led quickly to evidence items and it was a fairly simple exercise to create the basic text to complete the nodes and to provide the hyperlinks to existing and developed document sets including a safety management plan, risk tolerability matrix, hazard log and HAZID minutes.

The construction of the GSN was undertaken at the equipment holder's site, this gave ample opportunity to identify existing company references and to check exact text content.

In common with the capability of the ASCE toolset and the requirements of higher management, a simple MSWord export of the whole case for safety was produced. However, as the equipment was the subject of contemporary international bids and internal discussions, the safety case was left in electronic format using the free GSN viewer along with the structure and reference documents all burned to a CD. The data took up some 22.7MB of space, this easily fitted on a CD disc that could be shared around internally and used to form a readily available component to project bid support.

6. Resource Recording

As this piece of work was undertaken using the format of a sub-contract, it has been easy to extract the resource records of the task. These were necessarily captured as part of the financial recording requirements of the contract, and whilst it is not appropriate to publish the economic data, the time data is considered most useful.

The invoices from the safety consultants can be split into three distinct areas; pre-the HAZID, the HAZID and post-the HAZID. The captured data reveals the following;

- 1 day Preliminary meeting and contract discussion
- 2 days Document review, critique and familiarisation
- 1 days HAZID information pack preparation
- 3 days HAZID meeting and write up
- 3 days Developing GSN outline and node text
- 1 day Presentation and publication

A similar analysis of data from the equipment designers revealed the following time overview;

- 1 day Preliminary meeting and contract discussions
- 1 day Document provision and monitoring
- 4 days (8 x 0.5) HAZID meeting
- 1 day (4 x 0.25) GSN and text review
- 2 days (4 x 0.5) Presentation

Essentially the same time in man-days was spent by both parties to the contract – 11 days, making the total resource effort for this simple exercise a total of 22 days. It is left to the reader to judge whether this reflects well or poorly on the parties to the contract!

References

- [1] Guardian Newspaper Group “Friendly Fire Death was a Criminal Act, Coroner Rules”, 17/03/08
- [2] Guardian Newspaper Group “Military Hid the Truth of Friendly Fire That Killed US Hero”, 05/04/05
- [3] Ministry of Defence, “Safety Management requirements for defence systems”, Defence Standard 00-56 Issue 4, June 2007.
- [4] Ministry of Defence, “Safety Management requirements for defence systems”, Defence Standard 00-56 Issue 2, August 1997.
- [5] US Army Combat Readiness Center “Accident Briefs” Countermeasures, February 2006