Ensuring supplier safety analysis is not performed in isolation! The gulf between the Project Safety Engineer and the Front Line User

N.B.DURSTON

HP Enterprise Services Defence and Security Ltd, UK, Nicholas.Durston@hp.com

Keywords: Software, Safety, Committee, Hazard, Analysis

Abstract

This paper will explore, through use of a case study, the organisational difficulties experienced by Project Safety Engineers in determining whether software faults analysed in isolation could result in credible hazards or flight safety risks to users on the front line. The author has experience of defence projects where associated hazard identification and management activities have been complicated by ineffective or inexperienced Project Safety Committees. The aim of this paper is to identify where potential risks exist in Project Safety Committee management and to offer recommendations for improvement in order to increase the efficiency and effectiveness of the committee in determining credible platform-level hazards and consequent accidents. HP is the largest supplier of software intensive programmes to the UK MoD and as such, is represented at Project Safety Committees across a range of prime, sub-contactor and partnership capacities. The author is the Project Safety Engineer for HP's AMPA Programme and has been tasked with production of the AMPA Safety Case.

1 Introduction

When defence equipment is in service, the Duty Holder[1] role will normally reside with the respective Front Line Command. A MoD Project Team will take on the role of support to the Front Line Command Duty Holder. The MoD Project Team within their duty of care remit will ensure that the Front Line Commands are:

- supported and supplied with equipment and capabilities where risks have been assessed to be broadly acceptable or tolerable and As Low As Reasonably Practicable (ALARP);
- provided with suitable and sufficient information to enable the equipment and capabilities provided to be used appropriately.

The Acquisition Safety and Environmental Management System (ASEMS) describes MoD policy requirements for the management of Acquisition Safety and Environmental Protection. Compliance with these requirements aims to ensure compliance with safety and environmental legislation and MoD policy and through effective and efficient safety and environmental management; all appropriate precautions are taken to prevent harm to personnel and damage to equipment or the environment, consistent with providing the operational capability and cost-effective solutions required by the respective Front Line Commands.

The component of the ASEMS concerned with safety, the Project Oriented Safety Management System (POSMS) [4], describes the Safety Management processes and procedures to be employed during a project's life cycle by MoD Project Teams. These processes and procedures are designed to provide guidance for the identification and management of the safety risks of equipment and capabilities throughout the acquisition process.

In following the guidance of POSMS [4], projects are provided with assistance in identifying the safety risks through the application of hazard identification and assessment methodologies. Also provided is assistance in identifying and applying appropriate mitigation measures to eliminate or reduce safety risks to levels which are tolerable and ALARP. Furthermore POSMS [4] provides assistance in the identification and management of residual safety risk.

In order to support and supply equipment and capabilities where risks have been assessed to be broadly acceptable or tolerable and ALARP, the MoD Project Team requires a Safety Case for the equipment and capabilities which they procure.

Def Stan 00-56 [2] defines a Safety Case as a structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment.

An integral component of the Safety Case is the Hazard Log, a continually updated record of the hazards, accident

---

1 DES SE SEP [3] defines the term 'Duty Holder' within MoD as those personnel who occupy key positions which are responsible and accountable for the control of activities that are so hazardous that they could give rise to a risk to life.

The Duty Holder is responsible for the safe operation of systems and facilities in their area of responsibility and for ensuring that Risks to Life are reduced to at least tolerable and ALARP.

sequences and accidents associated with a system. It includes information documenting the management of each hazard and accident. The hazard log is utilised and maintained as the principal means of establishing progress on resolving risks associated with identified Hazards. It provides traceability of the Hazard management process to show how Safety issues are actioned, tracked and resolved.

By the very nature of a MoD Project Team following the POSMS [4] guidance of Preliminary Hazard Identification and Analysis, Hazard Identification and Analysis, Risk Estimation and Risk and ALARP Evaluation activities, it is clear that these activities cannot be performed in isolation in order to document information pertaining to the management of each hazard and accident in the Hazard Log.

2 The Concept of the Project Safety Committee

POSMS [4] states that the key elements for the effective management and delivery of safety are co-ordination, agreement and proper response by those authorities with responsibilities for the equipment.

Def Stan 00-56 [2] defines a Safety Committee as "A group of stakeholders that exercises, oversees, reviews and endorses safety management and safety engineering activities."

Essentially the Project Safety Committee (PSC) must define Terms of Reference to provide a forum through which all stakeholders with safety responsibilities can ensure effective co-ordination on safety issues, and make decisions after consultation with those having relevant specific knowledge or subject matter expertise. The MoD Project Team Leader with Safety delegation is required to seek and consider relevant advice through the PSC, but ultimately remains the decision maker as they are the risk holder.

The objectives of the PSC are to:

- Facilitate effective co-ordination on safety issues by all stakeholders with safety responsibilities;
- Facilitate access for decision makers to all those with relevant knowledge;
- Afford competent oversight of the Safety Case during production and maintenance;
- Present an audit trail showing that appropriate advice has been sought and that Safety Management decisions were well founded and endorsed.

The key principles of the PSC are to ensure that all relevant authorities are consulted, actions are agreed and properly allocated, and a record is kept of proceedings.

PSC tasks should include:

- Definition and review of the project's safety policy and strategy;
- Definition and review of the project's safety targets and objectives;
- Definition of the System boundaries to determine Safety responsibilities;
- Provision of advice to the Chairperson of the Safety Committee on the safety responsibilities for each authority associated with the project;
- Provision of advice to the Chairperson of the Safety Committee on the standards, statutory regulations and any restrictions with which the projects must comply;
- Review, monitoring, classification and allocation of new equipment hazards as they are identified;
- Review of the project's Safety Case and progress on achieving safety targets, to a predetermined schedule, issuing the results to the Delegated Authority;
- Seek assurance of the implementation of any control measures that are deemed necessary to reduce identified risks to Tolerable and ALARP;
- Guarantee of appropriate and timely availability of training and issue of documentation;
- Perform audits of the project's Safety Case to ensure that it is comprehensive, the audit findings should be then reported to the Delegated Authority;
- Review and monitoring of safety performance and maintenance of the Safety Case.

The PSC should be established during project conception by the MoD Project Team Leader in conjunction with the Front Line Command, to set out the safety requirements for the equipment.

The PSC may meet regularly as a body, or its work may be included as a permanent item in another forum. Particular care should be taken to ensure that all relevant parties are included in this instance. The PSC can either be established for a single capability, or a family of variants of a capability.

The frequency of PSC meetings is dependant on many factors including the stage of the project, the complexity of the system and whether the PSC is supported by Working Groups or has complete responsibility. The PSC will be required to convene at greater frequency towards Project milestones where periods of considerable review and decision making are expected.

The PSC may occur less frequently during periods of stability, for example, the in-service phase. However, the committee must provide oversight of the Safety Case to ensure that it remains valid through maintenance and the monitoring of safety performance. This should be considered when the system or its use changes, or when counter-evidence demonstrates the predicted level of safety performance is not being achieved in practice.

The PSC should be chaired by the MoD Project Team Leader, who holds a Letter of Delegation through the chain of command from ministerial level.

Membership of the PSC should include stakeholders representatives, as appropriate and when required, from:

- MoD Project Team including the Project Safety Manager, and other technical officers, responsible for the procurement aspects of the project;
- MoD Project Team responsible for the support aspects of the project;
- Front Line Command;
- Prime contractor;
- Sub-contractor;
- Design Authority;
- Trials, test and evaluation team;
- Release To Service Authority (RTSA);
- User representatives (Capability User);
- Training Authority;
- Maintainer;
- Maintenance Authority;
- Specialist advisors (eg from MoD, certification authority or industry safety consultants);
- Independent Safety Auditor (ISA);
- Interfacing MoD Project Teams;
- Representatives from the relevant MoD assurance organisation;
- Technical Specialists.

A function of the PSC includes the review of safety documentation, such as, the Safety Management Plan, Hazard Log and Safety Case Report and advising the MoD Project Team leader on their suitability. Agreement and endorsement that the document is suitable is generally recorded through a recommendation in the meeting minutes.

Def Stan 00-56 [2] states that records of key decisions made by the PSC shall be detailed in the Safety Case. PSC recorded minutes should detail:

- Stakeholder representatives present;
- Discussions held;
- Advice given;
- Decisions made;
- Recommendations to those with delegated authority for Safety management;
- Recommendations that the safety documentation is satisfactory and can be Authorised for release by the agreed signatory;
- Actions agreed.

Where relevant, the outputs from the PSC should generate updates to the following:

- Safety Management Plan;
- Hazard Log;
- Safety Case Report;
- Any specific Safety Requirements held within the System Requirements Document.

3 The Potential for an Ineffective Committee and associated Project Risks

A number of project risks exist where organisational management conditions may result in an ineffective PSC. The POSMS [4] provides an indication of such risks:

- **Risk 1**: Potential stakeholders may not be identified and therefore their needs and planned system use may not be addressed adequately in the derivation and development of safety requirements or reflected during the production of the Safety Management Plan. This risk is likely to occur if the PSC is not established as early as possible in the project life cycle. This risk may also occur if the PSC is established with an incomplete membership.
- **Risk 2**: Safety activities detailed in the plan to be performed may be inappropriate and insufficient in delivering the required levels of safety performance and assurance. This risk is likely to occur if the PSC fails to review, approve and endorse the safety activities and Safety Management System described in the Safety Management Plan. This risk may propagate areas of disagreement concerning safety responsibilities which are ultimately not identified.
- **Risk 3**: Problems concerning the safety programme are not identified in a sufficient timeframe. This risk is likely to occur if the PSC fails to convene with sufficient frequency. This risk will ultimately impacts project time and cost.
- **Risk 4**: The MoD Project Team taking responsibility from the designer. This risk is likely to occur in the event the PSC attempts to control the detailed design solutions, rather than relying on the Contractor's Safety Working Group and design function. To mitigate this risk MoD Project Team personnel should exercise influence through representation at the Contractor's Safety Working Group and through the setting of appropriate safety requirements.

4 The Advanced Mission Planning Aid

Air Forces across the world are increasingly reliant on technology to enhance tactical communication, collaboration and precision to increase Pilot situational awareness. One

such technology is HP's Advanced Mission Planning Aid (AMPA).

Today, HP's AMPA family of mission planning products caters for a wide range of users and is established as the air mission planning system of choice for the UK MoD and a growing number of export customers.

AMPA has been used extensively on recent operations by a number of platforms including fast jet (in both air-to-air and air-to-ground roles), strategic and tactical air transport, and support helicopters. HP's response in providing early upgrades and heightened service levels to support UK operations was recently acknowledged by the UK Secretary of State for Defence [1].

AMPA enables communications and information-sharing across all RAF bases and deployed units, enabling the accurate execution of sortie profiles. Digital maps and intelligence information are compiled into a single easy-to-use interface, enabling pilots to visualise critical elements of each flight before takeoff.

AMPA is a common mission-planning software solution, which has evolved to be an essential mission enabler for some platforms, upon which users are becoming increasingly reliant. There is a risk that the incorrect design, integration and operation of an AMPA system could contribute to an aircraft incident or accident.

AMPA has been in-service since 1995 and is a legacy system. In performing the retrospective safety appraisal of AMPA, the author expects to face the challenges commonly encountered with legacy systems, regarding the difficulties in demonstrating the traceability between system requirements, which are often omitted or in poor condition and the original design information, which often difficult to locate.

Like many legacy systems, no safety requirements have been placed upon AMPA by the customer. There are also areas of functionality for which no formal requirements exist. Therefore, performing a functional failure analysis of the requirements is likely to result in an incomplete analysis of the system and a risk that safety involved failure modes, and associated hazards, and their contribution to consequent accidents may remain unidentified.

The author has suggested an approach where all AMPA outputs are analysed. This approach ensures that preliminary hazard identification is not performed in isolation. Through a well established and effective committee, the author expects that credible platform-level hazards will be identified through presentation and discussion of the potential failure modes of the outputs at the PSC. In order for this approach to be successful the author has made the following recommendations regarding the provision of advice to the MoD Project Team Leader on membership and frequency of the committee.

Recommendation 1: It is recommended that the prime contractor's Project Safety Engineer (PSE) advises the MoD Project Team leader on membership of the PSC, to ensure that AMPA stakeholders are adequately represented to an appropriate level at the PSC.

By following this recommendation, the MoD Project Team leader will mitigate the risk of an incomplete membership of the committee.

Recommendation 2: It is recommended that the prime contractor's PSE advises the MoD Project Team leader to ensure that AMPA stakeholders adequately review the safety activities and Safety Management System described in the Safety Management Plan.

By following this recommendation, the MoD Project Team leader will mitigate the risk of an inappropriate and insufficient plan to deliver the required levels of safety performance and assurance and that all members recognise their safety responsibilities.

Recommendation 3: It is recommended that the prime contractor's PSE advises the MoD Project Team leader to ensure that members of the PSC represent the actual AMPA users in order to understand how the system is used.

By following this recommendation, the MoD Project Team leader will mitigate the risk of an insufficient understanding of the use of AMPA.

The Front Line Command has a key role at the PSC since they possess detailed knowledge of the environments which AMPA is used and relevant operational experience. Additionally their personnel will usually be those who are most exposed to the risk of harm.

By ensuring AMPA users are adequately represented to an appropriate level at the PSC, the risk of promoting conditions which could propagate an insufficient understanding of the use of AMPA is greatly reduced. An insufficient understanding of the use of AMPA can result in safety risks not being identified or managed.

Safety risks not identified through an insufficient understanding of the use of AMPA will not be addressed adequately in the derivation and development of safety requirements. Alternatively the Prime Contractor may spend excessive design effort with a focus on areas of AMPA functionality which are incorrectly identified as having greater safety significance than the actual use.

User representatives on the PSC may also be able to detail the ways in which the use of AMPA may have changed since the original design, or be able to justify development decisions which may no longer be known.

Real operational experience evidence which can be used to substantiate safety claims and to provide assurance of compliance with assumptions may be detailed by User representatives.

Recommendation 4: It is recommended that the prime contractor's PSE advises the MoD Project Team leader on the frequency of PSC meetings, to ensure that the committee meets appropriately to discuss, advise and craft decisions following the completion of Hazard Identification and

Analysis and Risk Estimation activities in determining credible platform-level hazards and consequent accidents.

By following this recommendation, the MoD Project Team leader will mitigate the risk of problems concerning the safety programme not being identified in a sufficient timeframe and ensures that actions and decisions can be made appropriately with regard to Risk and ALARP Evaluation activities.

The author believes by following these four recommendations the MoD Project Team leader will not only be complying with POSMS guidance, that some people may consider satisfying a box ticking exercise, but generally adding value to the provision of safety assurance for the capability and to the MoD as an organisation.

5 Conclusion

In conclusion, the author has introduced the Front Line Command Duty Holder who is responsible for the safe operation of capabilities in their areas of responsibility. The Front Line Command Duty Holder is supported by a MoD Project Team who will supply equipment and capabilities where risks have been assessed to be broadly acceptable or tolerable and ALARP. The MoD Project Team will follow POSMS [4] guidance to comply with MoD Safety Policy and in doing so the MoD Project Team Leader will establish a PSC.

The author introduces the concept of the PSC and identifies four project risks which are likely to result from an ineffective committee. The author introduces HP's AMPA as a case study and makes four recommendations to the MoD Project Team Leader responsible for AMPA. By following these recommendations the author believes that an effective PSC will be established and chaired by the MoD Project Team Leader, reducing the likelihood of experiencing those four risks identified earlier in the paper.

In establishing the PSC in such a way, the author believes that the committee will possess the correct knowledge and expertise to facilitate the determination of credible platform-level hazards or flight safety risks, and consequent accidents which may result from software faults with AMPA, ensuring that HP's safety analysis is not performed in isolation and is in consultation with the Front Line Commands who operate the many variants of the legacy system to support their air platforms.

6 Recommendations

Recommendation 1: It is recommended that the prime contractor's PSE advises the MoD Project Team leader on membership of the committee, to ensure that AMPA stakeholders are adequately represented to an appropriate level at the PSC.

Recommendation 2: It is recommended that the prime contractor's PSE advises the MoD Project Team leader to ensure that AMPA stakeholders adequately review the safety activities and Safety Management System described in the Safety Management Plan.

Recommendation 3: It is recommended that the prime contractor's PSE advises the MoD Project Team leader to ensure that members of the PSC represent the actual AMPA users in order to understand how the system is used.

Recommendation 4: It is recommended that the prime contractor's PSE advises the MoD Project Team leader on the frequency of PSC meetings, to ensure that the committee meets appropriately to discuss, advise and craft decisions following the completion of Hazard Identification and Analysis and Risk Estimation activities in determining credible platform-level hazards and consequent accidents.

7 Acknowledgements

The Author would like to acknowledge HP Enterprise Services Defence and Security Ltd and the UK MoD Defence Equipment & Support Air Platform Systems Project Team for their assistance during the production of this paper.

8 References

[1] P. Luff MP. Letter addressed to Chris Abbott, Vice President & Managing Director HP Defence UK, from Peter Luff MP, Minister for Defence, Support and Technology. Ref: MSU4/5/4/11cc. Dated 22nd November 2011.

[2] UK MoD. "Safety Management Requirements for Defence Systems Part 1 Requirements", Ministry of Defence, Defence Standard 00-56 Issue 4. (2007).

[3] UK MoD DES SE SEP. "Duty Holders Within DE&S – Principles" DE&S Safety And Environmental Protection Leaflet Issue 1.0. (2012).

[4] UK MoD DES SE SEP. "Project Oriented Safety Management Systems", Version 2.3s. DE&S Safety And Environmental Protection Group. (2011)