SOFTWARE VERIFICATION RESEARCH CENTRE

SCHOOL OF INFORMATION TECHNOLOGY

THE UNIVERSITY OF QUEENSLAND

Queensland 4072
Australia

TECHNICAL REPORT

No. 99-42

Improving Safety Management in Defence Acquisition

Brenton Atchison, Peter Lindsay, Tony Cant

December 1999

Phone: +61 7 3365 1003
Fax: +61 7 3365 1533

To appear in *Proceedings, 4th Australian Workshop on Safety Critical Systems and Software*, ed. M. McNichol, Australian Computer Society, 1999, pages 1-8.

Improving Safety Management in Defence Acquisition

Brenton Atchison[1], Tony Cant[2] and Peter Lindsay[1]

[1] Software Verification Research Centre
School of Information Technology
The University of Queensland
Queensland 4072, Australia

[2] Defence Science Technology Organisation

brenton@svrc.uq.edu.au, pal@svrc.uq.edu.au, Tony.Cant@dsto.defence.gov.au

Abstract

Improved management of safety during procurement of computer-based safety-critical systems is one of the key concerns of the Australian Government's Department of Defence Software Acquisition Reform program. This paper reports some lessons learnt from a task currently being undertaken by the Defence Acquisition Organisation, Defence Science Technology Organisation (DSTO) and the Software Verification Research Centre (SVRC) to study management of safety and implementation of software safety standards in a range of defence projects. Effective safety management requires the identification of potential issues, and planning for their resolution, early in the procurement process. The lessons learnt are general and may be of benefit to other organisations involved in specification and acquisition of safety-critical software systems.

1. Introduction

1.1 Defence acquisition reform and safety

As part of the Department of Defence's Software Acquisition Reform program, the SVRC and DSTO are undertaking a number of tasks in support of the acquisition of computer-based Safety-Critical Systems. The project (known as 'DefSafe') aims to improve Defence acquisition processes through a mix of research, project-based consultancy and policy guidance.

Advice to defence projects is an important part of DefSafe. Projects with which we have been involved include: a ship-launched missile-decoy system, a digital display system for fighter training aircraft, an air-combat training system and a ship command-and-control system. (This paper will not address details of specific projects). Many projects are at an early stage of procurement, while others have already undergone substantial development but a detailed safety case has not yet been formulated. Advice to projects covers the use of safety standards, the safety management process, preliminary hazard analysis and so on.

Policy advice is centred on an extensive survey of the relative strengths and weaknesses of international safety standards and a companion study of how Defence currently invokes standards in its existing contracts. The DefSafe team is also providing advice to Defence on the general approach to procurement and on certification and regulation issues.

The research aspects of the DefSafe Project are focused on further development of the Australian Standard DEF (AUST) 5679 [1], written by DSTO and recently published by the Army Engineering Agency. This Standard provides requirements and guidance for the development and assessment of safety-critical computer-based systems, focusing on requirements for the system safety case. Under DefSafe, research will be carried out into a number of technical issues, including the impact of human factors on safety and the integration of Commercial Off-The-Shelf (COTS) items and other non-development items into safety-critical systems.

1.2 Lessons learnt

The work presented in this paper draws on DefSafe experiences and observation of overseas (primarily US and UK) defence practices. It reinforces our previous experiences with the implementation of safety programs across a range of different industries.

Many different technical and management issues can affect the success of a project's safety program. Perhaps the most important issue is the timely recognition of possible safety implications of the system under procurement – be they possible hazards for operators, other defence staff, allies, or even civilians. These safety implications are not always immediately obvious. All too often, safety is considered only late in the procurement lifecycle, by which time it may be too late, or too expensive, to implement effective risk mitigations. This often results in sacrifice of system functionality or imposition of undesirable operational constraints.

This paper presents some of the issues that we have observed in the implementation of safety programs across a broad range of defence projects, at different stages of the development lifecycle. Some of the issues have well-known solutions while others are symptoms of the inherent difficulty of analysing, designing, implementing and assuring safe computer-based systems. In any case, it is hoped that other projects – in defence and other application domains – can benefit from the mistakes of the past by taking timely and appropriate management action.

The paper is organised as follows. Section 2 discusses issues that arise in the choice of safety standards to be applied to a project. Section 3 describes issues for the safety management process, and discusses the regulatory and certification context. Section 4 discusses safety management issues, including procurement processes and capabilities. Section 5 describes technical factors that are known to cause difficulties in safety management. Section 6 presents a checklist of issues for consideration in early phases of the procurement lifecycle. Finally, Section 7 presents a summary and conclusions.

2. Choice of safety standards

In a sense, existing Safety standards embody ‘best practice’ in safety management, yet the range of available safety standards is potentially very confusing, and choosing the best standard for a particular project can be difficult. Here we present some relevant background, then some observations about the choice of safety standards for safety-critical computer-based Defence systems.

2.1 International trends

The SVRC has carried out an extensive survey of international safety standards [2], drawing on existing surveys [3], [4], covering the following standards:

- DEF (AUST) 5679 [1]
- MIL-STD-882C [5]
- NATO StanAgs 4404 [6]and 4452 [7]
- UK Defence Standards 00-54 [8], 00-55 [9] and 00-56 [10]
- ARP Standards 4754 [11] and 4761 [12]
- RTCA/DO-178B [13]
- IEC 61508 [14]

There are some clear trends emerging in these standards.

The *system* nature of safety is clearly recognised. Moreover, standards are now addressing the whole system lifecycle, from concept through to decommissioning. In many cases (such as MIL-STD-882C), there is a broadening of definition of safety so that it covers not simply “life and limb” but includes also equipment damage and threats to the environment.

The concept of a *Safety Case* is central in many safety standards. A Safety Case documents the evidence providing assurance that the system will be safe to operate, and assumptions on which the assurance is based [15], [16].

Emphasis in the past has often been on documenting the quality of the engineering process, but certifiers increasingly require also “product” assurance – details of safety features of the design and evidence of their effectiveness. For example, the UK Ministry of Defence’s flight certification authorities focus entirely on product evidence. At the very least, the safety case needs to contain sufficient details of design and identification of safety mechanisms for an independent safety assessment to be made (“transferable assurance”).

Standards are increasingly recognising the inherent difficulty of assuring the safety of software-based systems, and encourage system engineers to consider other (simpler or more reliable) means of implementing safety-critical functionality. Standards that address software safety are now deliberately moving away from the use of quantitative (probabilistic) risk assessment in favour of qualitative analysis and evidence of good design practices.

2.2 Defence use of standards

A number of safety standards are used in Defence projects: projects that we are aware of have invoked one or more of the following standards: MIL STDs 882B and 882C, UK Defence Standards 00-55 and 00-56, RTCA DO-178B, DEF (AUST) 5679, and StanAgs 4404 and 4452. Publication of the use of standards is limited [17]. In some cases, standards have been invoked that do not provide sufficient coverage of safety aspects, while in other projects no specific safety standards are used.

Clearly, the approach to procurement of Defence systems within Australia is not a uniform one as far as safety standards are concerned. Special problems can arise where multiple standards are invoked, because of the difficulty in reconciling what can be vastly different approaches to safety management.