Improved Acquisition Processes for Safety-Critical Systems in the Australian Department of Defence

Peter A. Lindsay
Software Verification Research Centre,
The University of Queensland, Queensland 4072
Peter.Lindsay@svrc.uq.edu.au

Abstract

This paper describes recently developed policy and procedures for safety management during system acquisition within the Australian government's Defence Materiel Organisation (DMO). The thrust of the safety policy is that: all systems are considered safety-critical until shown otherwise; and any project acquiring or upgrading a system involving safety-critical elements is required to establish a System Safety Program during acquisition, and to deliver a Safety Case prior to acceptance into service. The policy is spelled out in detail, and recommended acquisition procedures are described.

Keywords: safety-critical systems, acquisition processes, software safety, defence.

1 Introduction

1.1 Motivation

The Australian government's Defence Materiel Organisation (DMO) is responsible for procuring new defence systems, and for overseeing major upgrades of existing systems, for the Australian Defence Force (ADF).[1]

Under Australian civil law, any organisation owes a duty of care to its employees and to members of the public who may be inadvertently harmed by the organisation's activities. The potential safety risks of many defence systems, even in peacetime operations, place a high level of responsibility on the DMO to deliver into service only systems that have been demonstrated to be safe. Although much of the responsibility for functional system safety rests with the system developer (here called simply the Contractor), the DMO has responsibility for many aspects of safety management throughout the acquisition lifecycle.

[1] The DMO is also responsible for in-service support of ADF defence systems, but the current paper is concerned only with the acquisition phase of a system's lifecycle, including major upgrades.

Due to the joint service nature of many acquisition projects, and the trend towards increasing integration of different systems into single facilities, it is important that there be a single uniform system-safety policy within the DMO.

1.2 Target of the Policy and Procedures

This document outlines new policy and procedures for safety management during system acquisition within the DMO. The policy is intended to apply to procurement of any system with functional safety implications, but particularly computer-based and software-intensive systems. The policy is aimed primarily at Project Offices in the DMO, and is part of the reform of acquisition practices currently underway in the DMO.

The policy and procedures provide a framework within which Project Offices can develop specialised safety requirements based on specific systems or standards, in a manner consistent with that used elsewhere in the DMO. The aim of the framework is to provide a traceable source for all safety management requirements for Project Offices, which can be easily updated to reflect newly developed principles, or lessons learnt from practical experience. It is not however intended to supercede ADF certification or regulatory requirements, such as those mandated by the various Technical Regulatory Agencies, and it stops well short of detailed technical requirements. Similarly, it does not mandate particular standards, although the procedures do provide pointers to useful sections of commonly used defence safety standards, by way of guidance.

The framework is structured along acquisition lifecycle lines, in phases as follows: early in project planning and requirement development; during Request for Tender preparation, Contractor selection and contract negotiation; throughout system design and development; and at system acceptance and transition to in-service support.

The policy and procedures were originally developed for the DMO's Directorate of Software Acquisition Reform[2] as part of the DefSafe project, as explained below. They were compiled from a number of sources, including existing policy and guidance from ADF Technical Regulatory Agencies (e.g. RAAF 7001.054), SVRC

[2] Now the Directorate of System Engineering and Software Acquisition Management (DSE&SAM).

Safety Critical System	Any system which contains, controls or influences the design or operation of physical devices which may cause injury or death.
Safety Critical Software	Software, including embedded machine code or instructions written to programmable devices, which is contained within or influences a Safety Critical System.
Safety Case	A collection of documentation, including high level arguments and the results of assurance activities, which demonstrates the safety of a system.
Project Office (PO)	DMO entity responsible for acquisition of a particular platform, facility or system until acceptance into service by the ADF.
Contractor	A company or companies, including subcontractors, responsible for providing a platform, facility or system to the Australian Defence Force.
Preliminary Safety Assessment	A study to determine whether a particular acquisition project contains safety critical elements (see Section 4.1).
Customer Safety Program	A set of processes to be followed by the Project Office to ensure acquisition of a safe system (see Section 5.1). The Customer in this case is the ADF.
Project Safety Officer	A person within the Project Office responsible for the Customer Safety Program.
Stakeholder	Any person or organisation with a legitimate financial, legal, professional or personal interest in the safety of a system.
Program Risk Reduction Strategy	A co-operative strategy to be followed by the Project Office and the Contractor to minimise safety program risk.
Mutual Risk Reduction Phase	Co-operative activities conducted by the Project Office and the Preferred Tenderer, to determine the size and cost of the safety program before commencement of the main contract.

Table 1. Terminology

experience supporting various DMO projects (Atchison et al, 1999), and existing Australian and International standards (DOD Def(Aust) 5679; Wabenhorst and Atchison, 1999; RTCA/DO-178B; MIL-STD-882C). They have since been incorporated into the DMO Knowledge System (DMOKS) and are being trialled in a number of acquisition projects.

1.3 Outline of this paper

The main terminology used here is outlined in Table 1. Section 2 describes the background to development of the policy and procedures, and outlines the DefSafe project and its achievements to date.

The safety management framework consists of an Overarching Safety Policy (Section 3) and 11 supporting policy statements covering different stages of the acquisition lifecycle: preliminary assessment of whether the system is safety critical (Section 4); pre-contract activities (Section 5); in-development activities (Section 6); and transition into service (Section 7). Each of the policy statements is given in full here, together with the recommended procedure for carrying out the policy. The DMOKS version includes more detailed guidance.

While the policy and procedures are aimed primarily at DMO acquisition practices, they are expected to be relevant to any organisation procuring complex safety-related systems.

2 Background: the DefSafe project

The DefSafe project (more formally titled *Specifying and Acquiring Safety Critical Systems*) commenced in January 1999 and is being carried out by staff of the Software Verification Research Centre (SVRC) under contract to the DMO.

A major focus of the DefSafe task has been interaction with safety-related DMO projects to gain firsthand experience of the issues they face. More than twenty projects have been provided with safety advice ranging from training and facilitation of safety analysis workshops, through to review of Requests For Tender (RFTs), contracts and contract deliverables. Projects have originated from each of the ADF services (army, navy and air force) and represent a spectrum of engineering stages, from concept development through to in-service support. Additional Project Offices were surveyed to determine the use of safety and software standards within the DMO. (A number of different standards are being applied, in different combinations.) A “lessons learnt” paper was presented at the 1999 Australian Safety Critical Systems and Software Workshop (Atchison et al, 1999).

A survey of international system safety standards was conducted (Wabenhorst & Atchison, 1999) and a number of technical studies have been undertaken, in part to assist in the further development of Australian Defence Standard Def(Aust) 5679 (DOD 1998). These include:

- operator-error issues in safety-critical systems, and how they are handled in standards (Hussey & Atchison, 2000a)
- a review of architectural design principles for safety (Hussey & Atchison, 2000b)
- a review of safety issues in acquisition of commercial off-the-shelf (COTS) systems (Lindsay & Smith, 2000)
- comparison of the treatment of Safety Integrity Levels in international safety standards

A model is being developed to use as the basis of CMMI-like assessments of suppliers' capability maturity in safety management and safety engineering (Robinson et al, 2001): see Section 5.2 below.

Another DefSafe activity has involved delivery of education and training within the DMO, including a module on safety-critical systems in the DMO's regular Software Acquisition Management course.

3 Overarching Safety Policy

The Overarching Safety Policy is as follows:

> *All systems shall be considered potentially safety-critical, and shall undergo a Preliminary Safety Assessment to determine if they contain safety critical elements. Any project acquiring or upgrading a system involving safety-critical elements shall establish a System Safety Program to minimise and mitigate safety risks associated with the project, and shall deliver a system Safety Case prior to system acceptance.*

(Further details of requirements for the Preliminary Safety Assessment and the System Safety Program are given below.)

The policy is refined into 11 supporting policy statements below, grouped into lifecycle stages. Each policy statement is accompanied by a recommended procedure for carrying out the policy. Project Directors can modify these procedures at their discretion, but would be expected to justify why their approach improves on the recommended approach, and would be expected to ensure that equivalent deliverables are generated.

The policy is intended to apply to all DMO acquisition- and major upgrade projects, to the extent that each project must undertake a Preliminary Safety Assessment. Once it has been established that a project does not contain safety-critical elements, no further requirements in this document are applicable.

Where substantial changes are made to any system, the policy should be re-applied in full.

4 Is the System Safety Critical?

4.1 Preliminary Safety Assessment

Policy Statement 1: *Every new system acquisition or upgrade project shall undertake a Preliminary Safety Assessment (PSA) to determine if the new system will contain safety-critical elements.*

Whilst all DMO-procured systems are to be considered potentially safety critical, the size and nature of the safety program will depend on the nature and complexity of the system and on the potential for accidents. For systems with no potential to cause death or injury, no safety activities are required beyond a Preliminary Safety Assessment.

The recommended procedure for carrying out a PSA is as follows:

1. Identify the major components of the system to be acquired or modified.
2. Determine the operational environment and operational modes of the system.
3. Determine whether the system, in any of its operational modes or environments, controls or includes physical devices which may cause serious injury or death.
4. Construct a list of possible accidents associated with the system. Include estimates of the severity of each accident.
5. If the system is assessed as including no safety-critical elements, record this decision and its justification, and seek endorsement of this decision by the appropriate Branch Head; no further action shall be required with respect to this Policy.
6. Assess the impact of the required safety program on the overall program, particularly on software development. If possible, modify the system concept to eliminate or reduce safety risk.

It is important to conduct the PSA as early as possible in the acquisition lifecycle, so that adequate resources can be allocated for managing safety risk.

An indicative list of systems that should be assessed as safety-critical (adapted from Def(Aust) 5679) is provided in Table 2.[3] Where a system is not covered by one of these categories, and cannot be shown to be clearly non-safety critical, a preliminary hazard analysis should be conducted.

Systems considered potentially safety critical are those controlling or influencing physical devices that may cause serious injury or death. Such systems include, but are not restricted to:

- Any munition-related system that controls or directly influences the prearming, arming, enabling, release, launch , firing, flight path or detonation of a munition system, including target identification, selection and designation;
- Any system that controls or directly influences the movement of gun mounts, launchers and other equipment;

[3] "Injuries or death" is usually taken to include possible long-term health problems and damage to the environment. In some cases it is extended to include loss of platform or major capital equipment.

- Any computer-based combat system;
- Any system that controls or directly influences the movement of munitions and/or hazardous materials;
- Any system that monitors the state of another system for safety purposes;
- Any system that controls, regulates or contains potentially dangerous energy sources;
- Any system used to compute safety critical data (including applications software that may not be connected to or directly control a safety critical hardware system, such as stress analysis programs);
- Any system that collects, stores, manipulates, and reports or displays data that may be safety critical in nature;
- Any system that controls or partially controls the movement of a vehicle (e.g. ship, aircraft, land-based craft, radar-guided objects). This includes traffic-control systems;
- Any system that controls or partially controls potentially dangerous moving parts of equipment to which personnel or members of the public may come in close proximity.

Table 2. Non-inclusive list of systems that should be considered safety critical.

5 Pre-Contract Activities

Having determined that a system may contain safety-critical elements, the Project Office needs to carry out a number of safety management activities prior to finalising a contract with the system developer.

5.1 Establish Customer Safety Program

Policy Statement 2: *A Customer Safety Program shall be established for all projects containing systems that have been assessed as potentially safety-critical.*

Responsibility for safety management does not rest solely with the Contractor. Whilst the Contractor is required to deliver a safe system, the Project Office is also required to ensure that a safe system is specified and delivered. The term Customer Safety Program is used for that part of the overall System Safety Program concerning the ADF. The DMO acts as the ADF's agent during acquisition and is thus responsible for establishing and developing the Customer Safety Program.

The recommended procedure for developing the Customer Safety Program is as follows:

1. Appoint a Project Safety Officer. This is the person in the Project Office responsible for managing the Customer Safety Program. Typically they would work closely with the project engineering manager, but report directly to the Project Director.
2. Identify safety stakeholders. These may include: the Project Office; the ADF project sponsor; relevant defence Technical Regulatory Agencies; the prime contractor (when selected) and sub-contractors; proposed end-users; the system's proposed in-service support facility; domain experts; and representatives of other systems or members of other organisations that will interact with the system during its operation.[4]
3. Determine the appropriate certification authority or authorities.
4. Determine certification, regulatory and legal safety requirements.
5. Prepare a Customer Safety Management Plan.

The Customer Safety Management Plan may be a separate document, or may be part of the project Engineering Management Plan. It should include details of:

- The various stakeholders, and their responsibilities;
- The certification process, and the requirements to be met for certification;
- The preferred standards to be used for safety management;
- The hazards identified in the preliminary safety assessment; and
- The scope of the safety program, and the relationship of the program with other systems, and with support requirements.

To ensure that the Project Office has the necessary contractual tools to properly monitor and ensure compliance of the contractor's safety program, the Customer Safety Program should be established as early as possible in the project lifecycle. At the very latest, the safety program should be established in time for safety planning outputs to be included in the Request For Tender (RFT) or Request For Proposal (RFP).

5.2 Requesting and Evaluating Tenders

Policy Statement 3: *The Request for Tender (RFT) or Request for Proposal (RFP) for system projects and upgrades shall communicate safety program requirements and seek a proposed solution for safety management.*

In order for the DMO to ensure that the Contractor has the intention and the capability to conduct an effective safety management process, it is important during the tendering process to solicit the Contractor's proposed solution for safety management, together with evidence that they are capable of implementing this solution. This information should not just be used to assist selection of the preferred tenderer, but should also be a basis for negotiations before contract signature to agree on a program that meets the certification requirements.

Since integrity assurance requirements can be a major cost driver in acquisition, it may be necessary to conduct a Preliminary Hazard Analysis on the system concept prior to RFT and tender evaluation, to ensure that safety program costs are taken into account.

The recommended procedure for carrying out the policy is as follows:

[4] Operation should here be taken to also include maintenance and decommissioning.

1. Define safety program requirements, including the use of standards and regulations. The relevant Technical Regulatory Agencies should be contacted for advice.
2. Define all safety program deliverables and their format.
3. Require that a single contractor (preferably the prime system contractor) have primary responsibility for execution of the safety program.
4. Request a draft Safety Management Plan, including organisational structure, roles, responsibilities and technical processes.
5. Request evidence of the contractor's ability to execute the Safety Management Plan.
6. Define special software program requirements for safety-critical software. Include any constraints or assumptions about the software safety integrity.

To support (in part) the tender-evaluation procedure the DefSafe project is developing a reference model, based on the Software Engineering Institute's "Capability Maturity Model – Integration" (CMMI)[5] approach (CMMI 2000). This model can be used as a reference point to assess a supplier's process capability as applicable to safety management and safety engineering practices (Robinson et al, 2001). The model is intended to reveal areas of project risk where extra Project Office vigilance may be required, but is not intended to replace the need for safety standards, or supercede any of the policy statements below.

5.3 Finalising the Contract

Policy Statement 4: *The overall Safety Management approach shall be agreed between the Commonwealth and the Preferred Tenderer before commencement of the main development contract.*

The best opportunity for cooperative resolution of safety program risks is following the selection of the preferred tenderer(s) and before contract signature. During this period, a joint Client/Tenderer team should competently identify and assess project risks.

Since safety management is a cooperative activity, the pre-contract phase is also an excellent opportunity to establish working relationships and instill a cooperative safety culture in the project.

There is considerable risk and uncertainty associated with safety programs, particularly with relation to cost. Sometimes safety risks associated with a new design can be difficult to estimate before design is substantially complete; as a result there may be considerable cost involved in either changing the design or conducting appropriate design and implementation assurance.

These risks mean that the actual cost of a safety program cannot always be determined in advance, and under fixed-price contracts can lead to disputes and an incomplete safety program.

In order to reduce the cost uncertainty associated with safety programs, it is useful if agreement can be reached on what constitutes acceptable risk in the context of the project and to agree assurance criteria in advance. For projects involving software, for example, this may include determining what activities are required for each Safety Integrity Level (SIL), and what SIL each particular software component should be developed to.

It is desirable to co-operate with the preferred tenderer to manage the risk as effectively as possible. One of the ways of doing this is by undertaking mutual risk reduction activities. These provide funding separate to the main contract to allow the project and the preferred tenderer to analyse project risks and ensure that sound risk management processes will be in place once the main contract commences.

In all cases, it is necessary to determine and agree an appropriate management structure, and to implement this structure as part of the development contract. Such a structure will include descriptions of the roles of each party, including the role of the certification authority and any independent evaluator.

The recommended procedure for carrying out this policy is as follows:

1. Arrange workshops with the preferred tenderer and appropriate stakeholders, to discuss and agree:
    - Risk assessment criteria, including levels of tolerable risk (upper limits that the customer will accept).
    - Roles and responsibilities within the safety organisation.
    - Procedures for risk assessment and cooperative risk mitigation.
    - The Preliminary Hazard List, including a discussion of hazardous operational scenarios.
    - The Safety Management Plan, and the use of safety standards.
    - The role of the Evaluator or certification authority.
    - The use of IV&V or other independent safety assessment
2. Identify program risks and cost uncertainties, and determine a risk reduction strategy
3. Form a System Safety Management Group (SSMG) including representatives from each of the major stakeholders
4. Define and agree contract safety program requirements.

The active SSMG participants may change over the course of the project, to ensure appropriate knowledge and skills are present, but should at very least include representatives of the main contractor and the Project Safety Officer.

[5] CMMI is a registered Service Mark of Carnegie Mellon University and the Software Engineering Institute.

6 System Development

Once the contract is in place, the main onus of safety management passes to the Contractor. The Project Office's role switches to one of monitoring Contractor activities throughout development.

6.1 Contractor Safety Management Program

Policy Statement 5: *The Contractor(s) shall be required to undertake a Safety Management Program for all systems assessed as containing safety-critical elements.*

The recommended procedure for carrying out this policy is to impose the following requirements on the Contractor:

1. Document the approach to safety, and all planned safety activities in the System Safety Management Plan (SSMP).
2. In co-operation with the Project Office determine a safety process that meets the requirements for certification, and revise the SSMP to reflect this before commencement of the main development contract.
3. Convene regular meetings of the System Safety Management Group (SSMG).

The Contractor Safety Management Program and Customer Safety Management Program together comprise the System Safety Program referenced in the Overarching Safety Policy above (Section 3).

6.2 Hazard Identification and Risk Analysis

Policy Statement 6: *The Contractor shall be required to undertake a hazard identification program and to determine the required risk reduction.*

The recommended procedure for carrying out this policy is to impose the following requirements on the Contractor:

1. Provide or reference a system description and function definition
2. Produce a list of possible accidents, with associated severities
3. Produce a list of accident sequences, with estimates of probabilities where applicable
4. Produce a list of system hazards which could contribute to the possible accidents
5. Assign a target probability for each system hazard necessary to reduce accident risk to tolerable levels
6. Produce a list of system safety requirements required to mitigate the hazards
7. Document the procedure and results of the hazard and risk analysis for inclusion in the system Safety Case. (See Section 6.6 for details of the Safety Case).

Different system safety standards use different approaches to conducting risk analysis and assessment: the above list attempts to capture what they share in common. The preferred approach is simply to mandate an appropriate standard be applied.

6.3 Hazard Treatment

Policy Statement 7: *The Contractor shall be required to reduce, eliminate or mitigate the effects of identified hazards in accordance with the safety requirements and risk assessment criteria.*

The recommended procedure for carrying out this policy is to impose the following requirements on the Contractor:

1. Identify alternative concepts for system operation and/or design
2. Assess risk mitigation options, including feasibility and program impact
3. Select one or more mitigation options, and document the justification for this selection.
4. Implement the selected mitigation option or options
5. Identify specific design standards, guidelines or practices to be applied
6. Apply system hazard analysis to identify potential hazard causes and design safety requirements.
7. Where the risk is to be mitigated through improved reliability of either software or hardware, determine the target level of reliability or integrity necessary to achieve satisfactory risk reduction.
8. Define verification criteria to meet the design integrity requirements

6.4 Safety Verification

Policy Statement 8: *The Contractor shall be required to demonstrate that the final system design satisfies the previously identified safety requirements, and that no new hazards have been introduced during system design or modification.*

The recommended procedure for carrying out this policy is to impose the following requirements on the Contractor:

1. Produce or reference a description of the design of each component design
2. Produce or reference a list of safety-related design decisions related to each component
3. Demonstrate that each component satisfies any related safety requirements, and that all selected mitigations have been properly applied
4. Where applicable, conduct verification activities to provide assurance that the component satisfies reliability targets or software safety requirements
5. Demonstrate that any new hazards introduced during the design process have been adequately treated

6.5 Hazard Tracking and Management

Policy Statement 9: *The Contractor shall be required to implement and manage an auditable hazard management system.*

The recommended procedure for carrying out this policy is to impose the following requirements on the Contractor:

1. Record all identified hazards in a hazard log. This includes hazards identified by any of stakeholders.
2. Have the hazard log periodically reviewed by the System Safety Management Group
3. Have the hazard log contents and their classification approved by the Project Safety Authority
4. Implement mechanisms to communicate hazards between sub-contractors and the Prime Contractor, and between the Prime Contractor and the Project Safety Authority.

6.6 Document Safety Case

Policy Statement 10: *A documented Safety Case shall be provided by the Contractor presenting an argument and supporting evidence that system hazards have been identified and their risk reduced to acceptable levels.*

The recommended procedure for carrying out this policy is to require the Contractor to produce and maintain a Safety Case in stages throughout system development. At a minimum the Safety Case should contain:

- Preliminary Safety Case for delivery at Preliminary Design Review
- Interim Safety Case for delivery at Critical Design Review and Test Readiness Review
- Operational Safety Case for delivery prior to system acceptance

7 Transition to In-Service Management

Safety is an ongoing process, and must be continued after acquisition. From the Project Office's point of view, this means that the in-service support agency must be provided with sufficient resources and information to continue maintenance of the Safety Case, and to continue monitoring hazards associated with the system.

Policy Statement 11: *The Safety Case shall be included as part of the in-service documentation for the system, and shall be maintained and updated as the system is modified or as new hazards are identified. Where substantial changes are made to the system this policy shall be re-applied in full.*

The recommended procedure for carrying out this policy is as follows:

1. Include the Safety Case as part of the configuration baseline transferred to the in-service support agency.
2. Ensure that in-service support procedures are in accordance with the operational and support assumptions made by the Safety Case.
3. Ensure that in-service support procedures include recording and analysing system failures and operational incidents for safety impact, and updating the hazard log where appropriate.
4. Determine the impact of all system changes or updates on the Safety Case, and undertake additional hazard analysis where required.
5. Include the results of any further hazard analyses as part of the Safety Case.
6. Prepare new Safety Cases for substantial changes to the system, including for decommissioning of the system.

8 Summary and Conclusions

This paper has outlined a policy framework for managing safety during system acquisition. The aim of the framework is to improve practices in the Defence Material Organisation and to make them uniform and consistent across the organisation.

The framework consists of an overarching safety policy plus supporting policy statements and procedures. The overarching safety policy could be paraphrased as saying that a system shall be considered safety critical unless proven otherwise, and that a safety program shall be established early in acquisition and a Safety Case delivered prior to system acceptance.

The framework was originally developed as part of the software acquisition reform program of the Defence Acquisition Organisation (DAO). Since work began, the DAO has become the DMO and the organisation's scope has broadened to include in-service support of ADF systems. In 2001 it is planned to extend the framework's scope similarly, as part of the DefSafe project.

Detailed guidance material and worked examples are also being developed, to aid in implementation of the procedures.

9 Acknowledgements

A number of people contributed to the work reported here. The SVRC's Brenton Atchison, Andrew Rae and Peter Lindsay were the main developers of the policy and procedures, with significant input from DSE&SAM's Adrian Pitman. Many of the concepts and much of the wording was drawn from Department of Defence publications, including Def(Aust) 5679. Useful review comments were received from Tony Cant (DSTO), Chris Edwards and David Marshall (DSE&SAM), Tony Mitchell (DSMA) and others, including the anonymous reviewers.

10 References

ATCHISON, B., LINDSAY, P. and CANT, A. (1999): Improving safety management in defence acquisition. *Proceedings 4th Australian Workshop on Safety Critical Systems and Software*, Canberra. 1-8. McNICOL, M. (ed). Australian Computer Society. http://svrc.it.uq.edu.au/Bibliography/svrc-tr.html?99-42.

CMMI Product Development Team (2000): CMMI-SE/SW: Capability Maturity Model – Integrated for Systems Engineering/Software Engineering, version 1.0 continuous representation. Technical Report 2000-TR-019, Software Engineering Institute, Carnegie Mellon University, USA.

DEPARTMENT OF DEFENCE (1998): *The Procurement of Computer-based Safety Critical Systems*. Australian Defence Standard Def(Aust) 5679. http://www.dsto.defence.gov.au/esrl/itd/safety.

HUSSEY, A. and ATCHISON, B. (2000a): Hazard analysis of interactive systems. Technical report 00-18, Software Verification Research Centre, The University of Queensland, Brisbane. http://svrc.it.uq.edu.au/Bibliography/svrc-tr.html?00-18.

HUSSEY, A. and ATCHISON, B. (2000b): Safe architectural design principles. Technical report 00-19, Software Verification Research Centre, The University of Queensland, Brisbane. http://svrc.it.uq.edu.au/Bibliography/svrc-tr.html?00-19.

LINDSAY, P. and SMITH, G. (2000): Safety Assurance of commercial-off-the-shelf software. 43-51. In *Proceedings 5th Australian Workshop on Safety Critical Systems and Software*, Melbourne. GRIFFITHS, A. (ed). Australian Computer Society. http://svrc.it.uq.edu.au/Bibliography/svrc-tr.html?00-17.

MIL-STD-882C (1993): *System Safety Program Requirements.* US Department of Defense Military Standard.

ROBINSON, N., LINDSAY, P. and PITMAN, P. (2001): Extending the Integrated Capability Maturity Model (CMMI) for safety-related applications. To appear: *Proc 8th Internat. Syposium of the Internat Council on Systems Eng (INCOSE)*, Melbourne, Australia. http://svrc.it.uq.edu.au/Bibliography/svrc-tr.html?00-40.

ROYAL AUSTRALIAN AIR FORCE (1999): *Airworthiness Design Requirements Manual*, Australian Air Publication 7001.054, November 1999.

RTCA/DO-178B (1992): *Software Considerations in Airborne Systems and Equipment Certification*. Requirements and Technical Concepts for Aviation.

WABENHORST, A. and ATCHISON, B. (1999): A survey of international safety standards. Technical report 99-30, Software Verification Research Centre, The University of Queensland, Brisbane. http://svrc.it.uq.edu.au/Bibliography/svrc-tr.html?99-30.