

**SOFTWARE VERIFICATION RESEARCH CENTRE
SCHOOL OF INFORMATION TECHNOLOGY
THE UNIVERSITY OF QUEENSLAND**

**Queensland 4072
Australia**

TECHNICAL REPORT

No. 00-13

**A Comparison of MIL-STD 882C and MIL-STD 882D for
Australian Defence Acquisition**

Brenton Atchison, Peter Lindsay

April, 2000

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

Produced under contract CA38809 with the Australian Defence Acquisition Organisation, Directorate of Software Acquisition Reform.

Note: Most SVRC technical reports are available via anonymous FTP, from svrc.it.uq.edu.au in the directory /pub/SVRC/techreports. Abstracts and compressed postscript files are available via <http://svrc.it.uq.edu.au>.

A Comparison of MIL-STD 882C and MIL-STD 882D for Australian Defence Acquisition

Brenton Atchison, Peter A. Lindsay

Software Verification Research Centre, School of Computer Science and Electrical Engineering, University of Queensland, Australia

email: {brenton, pal}@svrc.uq.edu.au

Abstract

This report compares the use of the system safety standard MIL-STD 882C with MIL-STD 882D for the use of Australian Defence Acquisition. It summarises the differences between the standards and examines the implications of the transition from MIL-STD 882C to MIL-STD 882D in the Australian Defence Acquisition environment. The conclusion drawn is that the approach taken by MIL-STD-882D relies on an acquisition environment that may not transfer to Australian conditions and that additional controls are required to apply MIL-STD 882D effectively.

Keywords: system safety engineering, defence acquisition

1 Introduction

US military standard MIL-STD-882C [2] is currently the most commonly used safety standard in Australian Defence acquisition. A revised standard, MIL-STD-882D [3], has recently been released. The purpose of this report is to describe the differences between the two standards, and to discuss the implications should MIL-STD-882D be used in Australian Defence acquisition.

An overview of the content of MIL-STD-882D is provided in Section 2 and a summary of the main differences between the two standards is provided in Section 3. Section 4 considers the likely use of MIL-STD-882D in the United States and issues of acquisition of Non-Development Systems are discussed in Section 5. Based on these considerations, recommendations are made in Section 6 on the use of MIL-STD-882D in Australian Defence acquisition.

This report was prepared under contract CA33809 [1] with the Australian Defence Acquisition Organisation.

2 Content of MIL-STD-882D

The stated purpose of MIL-STD-882D is to “ensure the identification and understanding of all known hazards and their associated risks, and that mishap risk is eliminated or reduced to accepted levels.” To achieve this goal, a minimal set of requirements are defined as follows:

1. Documentation of the system safety approach. Such documentation will describe the

implementation of MIL-STD-882D requirements, including how system safety is integrated into the overall program and how hazards and risks are communicated to and accepted by the appropriate authority. Guidance on issues to consider is provided in Appendix A of the standard.

2. Systematic identification of hazards, encompassing all hazard sources and system phases. Hazard identification is a responsibility of all program members.
3. Assessment of mishap risk to determine the potential impact of hazards on personnel, facilities, equipment, operations, the public, and the environment. A risk assessment model is suggested in Appendix A, including mishap severity and probability levels and risk acceptance levels. However, the project is free to define acceptable risk levels and acceptance authorities.
4. Identification of mishap risk mitigation measures. The order of precedence is to eliminate through design, incorporate safety devices, provide warning devices then develop procedures and training.
5. Reduction of mishap risk to an acceptable level. The risk mitigation approach is to be mutually agreed to by both the developer and the program manager.
6. Verification of mishap risk reduction through appropriate analysis, testing, or inspection.
7. Review of hazards and acceptance of residual mishap risk by an appropriate authority. The authority for risk acceptance should include the system user.
8. Tracking of hazards and residual mishap risk. A tracking system for hazards, their closure, and residual mishap risk must be maintained throughout the system life cycle. The program manager must keep the system user apprised of the hazards and residual mishap risk

Appendix A contains additional guidance on safety activities. The guidance is indicative only and needs to be included in contracts explicitly.

3 Differences between MIL-STD-882C and MIL-STD-882D

The revision of MIL-STD-882C to MIL-STD-882D was largely driven by the tenets of U.S. Defence Acquisition Reform and requirements of new Defence Standards. In particular, the aim was to eliminate strict guidance, providing greater flexibility in the acquisition process.

The major differences between MIL-STD-882D and MIL-STD-882C are as follows:

1. No formal system safety plan is required. Instead, the system safety approach is agreed between Contractor and Project.
2. All detailed tasks from MIL-STD-882C have been removed, including detailed requirements on safety management processes, hazard analyses and verification activities. As a result, the standard is no longer tailorable and the minimal requirements provided are mandatory.
3. No formal safety program deliverables are mandated. Each project is free to determine the data that is required.
4. There is an increased recognition of the system user's role in safety management. In particular, the risk acceptance authority must include the system user in the mishap risk review.
5. The focus of risk assessment is on mishap risk, rather than hazard risk. This provides a

means for reducing risk by controlling mishaps after engineered system failure.

The impact of these changes is that there is much greater freedom to implement a suitable safety program. As a result, greater responsibility is placed on Contractors to define appropriate system safety programs and on the Project Office to assess and monitor adequacy of the programs. This increased responsibility may lead to greater thought being applied to safety program definition. However, successful application clearly relies on suitable expertise and motivation of all parties.

The MIL-STD-882D changes also place greater emphasis on managing safety through cooperative decision-making. Ideally, this will focus the safety program on active risk reduction tasks. However, a danger is introduced that inadequate evidence of risk reduction is produced, leading to difficulties in system certification, maintenance and modification, and possibly unsafe operational systems.

4 U.S. use of MIL-STD-882D

The transition in the U.S. from MIL-STD-882C to MIL-STD-882D is part of an overall acquisition reform program and must be seen in the context of the U.S. Defence acquisition environment. Some of the factors to consider include the following:

- MIL-STD-882D makes use of U.S. Civil Law, requiring that mishap risk must be identified, evaluated, and mitigated to a level acceptable (as defined by the system user or customer) to the appropriate authority and compliant with federal laws. This requirement is supported by mandatory procedures for acquisition programs, in DoD Regulation 5000.2-R [4]. It is assumed that the threat of legal liability will ensure that Projects and Contractors follow best practice.

The law is particularly applicable in Total System Responsibility contracts, where developers assume total responsibility for the system, receiving limited engineering direction. In some cases, the developer may choose to limit liability by closely involving the U.S. Government in the procurement process.

- The system safety process developed around previous revisions of MIL-STD-882 are expected to be well known and accepted through industry, particularly Defence contractors. Project Offices are also expected to be familiar with safety programs. In fact, detailed tasks of MIL-STD-882C not included in MIL-STD 882D can now be found in modified form in the US Defense Acquisition Deskbook [5].
- The U.S. Department of Defence has an extensive safety regulatory process and technical review boards, and provides a valuable source of guidance for determining suitable system safety programs.

Due to these factors, the short-term use of MIL-STD-882D is not expected to change the US Defence acquisition process significantly. However, changes in the long term are expected when safety programs begin to vary from accepted practice.

5 Acquisition of Non-Development Systems

The introduction of MIL-STD-882D also has implications for Australian acquisition of Non-Development systems, particularly U.S. systems. In this instance, the close level of interaction with Contractors expected by MIL-STD-882D cannot be relied upon, particularly for acquisition of existing systems. Given the greater freedom in the safety approach, DAO also cannot assume that use of the standard has produced a suitably rigorous safety program. Instead, assurance of safety will need to be assessed through documentation. Significant effort may be required to review such

documentation or produce it in instances where it is not available.

In some cases, it may be possible to liaise with other certification agents where pre-certified systems are acquired with limited modifications. However, care should be taken to ensure that any assumptions on the operational use and environment are not violated.

6 Conclusions and Recommendations

The revision of MIL-STD-882C to MIL-STD-882D applies the principles of U.S. Defence acquisition reform to system safety programs by reducing standard requirements to a minimal number. This presents much greater freedom to the Contractor and Project Office to implement the safety program in accordance with project needs.

However, the freedom offered by MIL-STD-882D is accompanied by a greater responsibility for each project to define and execute a suitable safety program. It is not sufficient to invoke the standard and assume that an adequate safety program will be followed. Instead, the Project and Contractor must take an active role to define an approach to safety engineering and ensure it is implemented. Defining a suitable safety program is a significant challenge since recommended practice for safety programs varies substantially, particularly for software-intensive systems. To be successful, access to specialist skills and knowledge is vital.

The approach taken by MIL-STD-882D relies on an associated Defence acquisition environment that may not transfer to Australian conditions. In particular, it assumes that acquisition is carried out with threat of litigation under U.S. Civil Law and that best practice will be maintained through industry and government culture and regulatory oversight. Without such a suitable acquisition environment, the use of MIL-STD-882D increases the risk that a deficient or over-protective safety program will be implemented. Furthermore, the lack of detailed guidance may lead to increased costs when implementing the program, disputes with Commonwealth or certification delays.

Accordingly, we do not recommend the use of MIL-STD-882D unless adequate controls are put in place. Such controls would include at least the following::

1. For development systems the approach should be documented and agreed in a System Safety Management Plan (SSMP) prior to contract. Comparison with other approaches recommended by other international standards may be useful in determining the adequacy of defined processes. Where development of SSMP is a significant undertaking, pre-contract funding to preferred tenderer(s) may be required.
2. For development systems, the Commonwealth should take an active role in the safety management process, as recommended by MIL-STD-882D. Where necessary, training and support services should be sought to obtain suitable expertise.
3. For development systems, the results of the system safety program should be documented. Program results should be assessed by a Third Party suitably qualified to determine the adequacy of the safety program and validity of results. If possible, the assessor should be engaged throughout the project to provide feedback in a timely manner.

For non-development systems, documentation justifying acceptable risk should also be made available and assessed prior to system acquisition. The assessment should validate that any assumptions made in the operational use or environment of the system are maintained in the target conditions.

7 Acknowledgements

The authors gratefully acknowledge the Australian Department of Defence, Directorate of Software Acquisition Reform for sponsorship of this report and Axel Wabenhorst, Chris Edwards and Tony Cant for comments on previous revisions of this report.

8 References

- 1 Australian Department of Defence Contract CA38809, Specifying and Acquiring Safety-Critical Software Systems, January 1999.
- 2 U.S. Department of Defense. MIL-STD-882C, System Safety Program Requirements, January 1996.
- 3 U.S. Department of Defense. Draft MIL-STD-882D, System Safety, April 1999.
- 4 U.S. Department of Defense. DoD 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs and Major Automated Information Systems.
- 5 U.S. Department of Defense. Defense Acquisition Deskbook.