Experience with Extending CMMI[SM] for Safety Related Applications

Mark Bofinger, Neil Robinson, Peter Lindsay[1]
Software Verification Research Centre, University of Queensland, Australia

Mick Spiers, Matt Ashford, Adrian Pitman
Directorate of Software Engineering,
Defence Materiel Organisation

Abstract. +SAFE, a safety extension to the Capability Maturity Model - Integrated (CMMI) has been developed and trialed in Australia, for use in assessing suppliers of safety-related systems. This paper describes the latest version of the safety extension and also reports on the results of seven trials.

INTRODUCTION

CMMI (CMMI, 2000) offers a Capability Maturity Model integrated for software and systems engineering. The Australian Department of Defence is using CMMI to assess suppliers of software-intensive systems. The objectives are to identify the strengths and weaknesses of system and software suppliers, and to address identified weaknesses early in the acquisition process. However, CMMI is a generically structured framework, which requires amplification for specialised areas of software and systems engineering, such as safety engineering. Developing safety-critical systems is a high-risk activity and requires specialised skills and experience within an organisation. Although CMMI provides a framework within which safety activities can take place, the *required* and *expected* parts of the model do not mention safety. The only mentions are in the *informative* parts of the model and these mentions are slight. There is, therefore, a risk that an organisation that has been assessed as adequately capable, using the CMMI framework, may turn out to have inadequate processes for dealing with safety.

In 1999, the Defence Materiel Organisation (DMO), part of the Australian Department of Defence, initiated a technical study on Safety Capability Assessment, aimed at producing a safety extension to CMMI. The technical study was part of the DefSafe project being undertaken with the Software Verification Research Centre at the University of Queensland. This project was established to improve safety-critical system acquisition practices in the DMO.

A safety extension to CMMI, +SAFE was developed (Robinson, 2001), and has now been through seven trials. As a result of the trials, the safety extension has been restructured and updated. Here we describe the new +SAFE process model, and report on the results of the first seven trials.

OVERVIEW OF +SAFE

Key Requirements. The key requirement of +SAFE is that it should help the Australian Department of Defence assess an organisation's capability for developing safety-related systems. +SAFE is designed to be used either as part of a larger CMMI based appraisal, or on a stand-alone basis.

+SAFE is intended primarily as a risk management tool. Measures can be taken to address those weaknesses identified in an appraisal. Examples of measures include seeking additional expertise in certain areas or the development and implementation of a process improvement program. It is important to note that +SAFE was never intended to form the basis of any certification and there is no guarantee that systems developed in accordance with +SAFE practices will be adequately safe.

+SAFE is intended to be consistent with the Australian Defence standard Def(Aust) 5679 (Def(Aust)5679, 1998), and not inconsistent with other modern safety standards, such as IEC 61508 (IEC 61508, 1998). These requirements are necessary, as the Australian Defence Force operates and maintains a diverse range of safety-critical and safety-related systems. A number of different system and software safety standards are used in defence acquisition projects, depending on the nature

---

[SM] CMMI is a service mark of Carnegie Mellon University

[1] Appeared in Proceedings Twelfth Annual International Symposium of the International Council On Systems Engineering (INCOSE 2002), Las Vegas, Nevada, 28 July – 1 August 2002

of the system and the acquisition, and the experience of the developer (Robinson, 2001).

Overall Structure. The safety extension has been developed in the style of CMMI, so that users are familiar with the structure and style. There are two process areas, *safety management*, and *safety engineering*, with associated goals as shown in Table 1. The generic goals and practices of the CMMI are used to cover activities that are common to all process areas. Since the model is intended for use as part of larger CMMI appraisal and stand-alone, the model aims to achieve a level of detail that avoids repetition with the CMMI, but is still sufficient to be adequately understood without reference to the CMMI process model. The following sections describe the contents of the two process areas.

CMMI[SM] Categories	**Safety Process Areas**	**Specific Goals**
Project Management	Safety Management	Develop Safety Plans
		Monitor Safety Incidents
		Manage Safety-related Suppliers
Engineering	Safety Engineering	Identify Hazards, Accidents and Sources of Hazards
		Analyze Hazards and Perform Risk Assessment
		Develop Safety Requirements
		Apply Safety Principles and Requirements
		Support Safety Acceptance

Table 1 Structure of Safety Extension

Safety Management Process Area. This process area covers the establishment and maintenance of a safety plan, as well as monitoring, and if necessary correcting performance against the plan. Safety Management also includes managing the approach to safety of any suppliers. Although the Project Management category of CMMI includes Risk Management, technical aspects of safety risk management are covered in the Safety Engineering process area.

The *Develop Safety Plans* goal includes the following specific practices:

- *Determine Regulatory Requirements, Legal Requirements and Standards*

  This covers the capture of requirements, as implied by the title. Where such requirements are directly applicable to the domain, this also involves integrating the requirements with the results of any hazard and risk analysis. This practice also covers selection of standards. For many defence systems, multiple safety standards may apply.

- *Determine Safety Criteria*

  This covers the development of risk targets, which specify, either qualitatively or quantitatively, the acceptable level of safety.

- *Establish a safety organisation structure for the project*

  This covers the special issues that need to be considered when establishing a safety organisation structure. Such organisations need to consider independence, both from a technical and a management perspective. They also need to consider how disputes involving safety will be resolved.

- *Establish a Safety Plan*

  This practice covers the establishment and maintenance of a safety plan. Such planning also covers safety engineering and support processes for safety verification, validation and independent safety assessment activities, such as audits and evaluations.

The *Monitor Safety Incidents* goal (containing the one specific practice) covers the monitoring of systems in order to maintain the relevance of safety analyses. Incidents are reported, and then reviewed against existing hazard and risk analysis. This can result in updates to the analysis and updates to the project safety plan.

The *Manage Safety-related Suppliers* goal includes the following specific practices.

- *Establish supplier agreements that include safety requirements*

  This practice covers the analysis of the project's needs to acquire safety-related products and services, the selection of suppliers, and the establishment of supplier agreements that include safety requirements

- *Satisfy supplier agreements that include safety requirements*

  This practice covers the execution of supplier agreements that include safety requirements, and ensuring that safety assurance is delivered with the product or service. It also covers the

issues that arise when acquiring COTS products that are intended to implement safety-related functions.

Safety Engineering Process Area. This process area covers the activites that deal with safety issues at all stages in the engineering process.

The *Identify Hazards, Accidents and Sources of Hazards* goal includes the following specific practices:

- *Identify possible accidents and sources of hazards*

  This covers the unstructured identification of possible accidents and source of hazards when a system is mostly still in the concept phase.

- *Identify possible hazards*

  This covers the systematic identification of hazards using an appropriate model of the system as a basis for the analysis.

The *Analyze Hazards and Perform Risk Assessment* goal (containing the one specific practice) covers analysis of possible causes and consequences, severity and likelihood of each hazard, and the assessment of the risk presented by that hazard. For hazards that can be attributed to a software failure, a safety target (safety integrity level, level of trust) is assigned instead of a likelihood.

The *Develop Safety Requirements* goal includes the following specific practices:

- *Determine safety requirements*

  This covers the derivation of safety requirements which specify some means of avoiding, mitigating, detecting or reducing the exposure time of a hazard.

- *Determine a safety target for each safety requirement*

  This covers the derivation of quantitative or qualitative targets for each safety requirement, based upon the safety analysis and the safety criteria.

- *Allocate safety requirements to components*

  This covers the allocation of safety requirements to the components of a system in a manner consistent with the properties of those components.

The *Apply Safety Principles and Requirements* goal includes the following specific practices:

- *Apply safety principles*

  This covers the application of general principles (including As Low As Reasonably Practicable and the order of precedence in which mitigations are to be applied).

- *Ensure the application of appropriate rigour*

  This covers the presence of adequate management, engineering and support practices throughout the development of a system to ensure that the system is developed according to the safety requirements.

- *Perform safety impact analysis on changes*

  This covers the analysis of changes for their impact on safety.

The *Support Safety Acceptance* goal includes the following specific practices:

- *Establish and maintain a hazard log*

  This covers the presence and use of a record of the current status of each hazard and the means by which the status has been determined.

- *Develop safety case argument*

  This covers the development of a high level argument that shows why the system is acceptably safe and references to supporting evidence that justifies the claim.

- *Validate system safety for intended operating role*

  This covers the validation of the safety case and the assumptions underlying it, both during development and during the lifetime of the system

- *Perform independent evaluations*

  This covers the adequate independent evaluation of a system and the processes used to develop that system.

Tailoring of the Process Model. When a project is not safety-related, the +SAFE model is not relevant for appraisal. However, safety criticality is not binary, and there are cases between the non-safety related projects and safety-related ones, in which only a part of the model is relevant. In these cases, the +SAFE model is tailored as shown in Table 2. Clearly it is undesirable that safety-related projects claim that their project is *not* safety-related, and thus avoid appraisal against the model. However, since the +SAFE model is being used in an appraisal context, where it is in the interest of the organisation being assessed to demonstrate their capability in safety-related systems, this is unlikely to be an issue.

Project	Safety Manage-ment			Safety Engineering				
Specific Goal:	**1**	**2**	**3**	**1**	**2**	**3**	**4**	**5**
Project is not safety-related								
Project may be safety-related but hazard identification indicates that it is not	√	√	√	√				√
Project is safety-related but all hazards are acceptable	√	√	√	√	√			√
Project is safety-related and some hazards are not initially acceptable	√	√	√	√	√	√	√	√

Table 2 Tailoring the +SAFE model for different projects

The Design of the Process Model. The structure and content of the +SAFE model has been through a number of changes since it was first developed. Initially a study was carried out which considered whether to attempt to integrate a safety process model with CMMI, or to create a stand-alone model. The choice of the stand-alone approach resulted partly from the DMO's desire to use the safety extension as soon as possible. The other key consideration was a concern with the distributed approach that safety might get lost in the larger CMMI appraisal. Appraisers may not be familiar with safety engineering principles, so safety considerations may not receive the attention they deserve. Although the clear intention in CMMI is for additional disciplines to be accommodated through Discipline Amplifications, this does not seem scaleable. Adding the Safety Process Model onto the CMMI would add many detailed amplifications. Adding more disciplines would eventually result in a lack of structure and clarity (Robinson, 2001).

For the first trials, the +SAFE process model included an additional *Safety Support* process area which included, for example, independent safety assessment. However the additional overhead of another set of generic goals and practices was found to be too onerous.

Finally, many more minor changes were made in order to create a uniform level of detail across the process model and to improve its consistency.

THE +SAFE TRIALS

Overview. Seven trial appraisals have been performed using +SAFE. The organisations undergoing appraisals have included both Australian and international organisations, and included procurers, prime contractors and subcontractors.

The outcomes of the +SAFE trials have been split below into those relating to the findings against the model, and those relating to possible improvements to the model.

The findings of the organisations against the model.

A direct comparison of the findings from the trials is made slightly more complicated due to the reorganisation of the process areas, and some changes in the delineation between specific practices. Comparisons can be made using a mapping from the older versions of +SAFE to the latest version. This presents an estimate of how the organisations would have been appraised against the current version.

In general, the findings against +SAFE have tallied with the expectations of the personnel performing the appraisals and the organisations appraised. In particular, the later trials have been reported as more accurately reflecting the capability of an organisation to deliver safety-critical systems. This has been partly seen as relating to the introduction of the tailoring guidance table.

Some findings related closely to the legal requirements of the organisations in question. This was prominent where safety was not adequately addressed in the relationship between multiple organisations and/or where differences of opinion existed over legal duty of care. As +SAFE is intended to address best practice as a primary concern rather than legal or contractual requirements, these were seen as weaknesses against the organisations.

The data from the trial appraisals was aggregated to produce statistics on which practices were generally poorly or well performed. In Safety Management the following activities were often poorly performed:

- *The establishment of safety criteria*
- *The establishment of a safety organisational structure*
- *The flow down of safety requirements to suppliers*

In Safety Engineering the following activities were often poorly performed:

- *The determination of safety targets for requirements*
- *The application of safety principles*
- *Ensuring the application of rigour.*

Another constant theme was that safety critical software was generally poorly managed in organisations that do not apply a software safety development standard such as RTCA DO 178B or Def (AUST) 5679.

It was also found that systemic organisational issues

that prevented satisfaction of generic practices and goals across the CMMI process areas also affected the +SAFE process areas.

Table 3 below, shows the percentage of organisations that satisfied each of the goals of +SAFE. Only one organisation achieved Capability Level 2 in both process areas with all other organisations achieving Capability Level 0.

Safety Process Areas	Specific Goals	Percent Satisfied
Safety Management	Develop Safety Plans	25%
	Monitor Safety Incidents	50%
	Manage Safety-related Suppliers	33%
Safety Engineering	Identify Hazards, Accidents and Sources of Hazards	25%
	Analyze Hazards and Perform Risk Assessment	25%
	Develop Safety Requirements	50%
	Apply Safety Principles and Requirements	33%
	Support Safety Acceptance	75%

Table 3 – Percentage of Organisations Satisfying +SAFE Goals

The findings for improvement to the model.

One of the organisations appraised was seen as a world leader in the development of safety critical systems. This organisation came up very favourably against +SAFE with the model accurately reflecting their safety practices. This is an indication that the model is a true reflection of system safety best practice.

Feedback from users. Much early feedback from +SAFE users has been incorporated into the model, and has been discussed above. This has been possible due to the staggered nature of the first seven trials, with improvements being made between appraisals. This situtation is not expected to continue once +SAFE has been released to a wider audience.

Feedback from the users of the model has generally been very positive considering the relative immaturity of +SAFE.

One important piece of feedback that has differed greatly from trial to trial was useability. This can be attributed to the relative expertise and experience in safety management and engineering of the assessors. The model includes elaborations to enlighten the appraisers as to what sort of practices are generally related to a given process area. However, the appraisers should be aware of the nature of safety management and engineering practices before attempting to appraise an organisation against +SAFE.

Discussion. Although the trials have resulted in considerable interest in +SAFE, and improvements have been made, there are still some issues outstanding. These issues include the lack of a stand-alone trial of the model and the clarity for appraisers inexperienced in safety. The model has been exposed to a variety of international organisations, but has not yet been exposed to appraisal teams with no previous knowledge of safety or the development of the model.

Another aspect that is yet to be addressed in the model is the differing levels of safety criticality. An appraisal of an organisation that has been developing low integrity safety related systems could occur with good results. However, if this organisation was to develop a high integrity system they may encounter new difficulties.

FUTURE OF +SAFE

The +SAFE model was released to a group of interested parties from Australia, the US and Europe at the end of 2001. The model has now been put under the control of a change-control board. Comments will be rolled into +SAFE and further trials will be conducted, possibly including a stand-alone appraisal. Following this initial round of consultation and trials, the DMO will release the model in the public domain.

Some modifications and additions to the model are expected, including elaborations to enable:

- appraisers without a safety background to use +SAFE
- judgements of an organisation's capability to develop systems of varying levels of integrity (such as SILs).

RELATED WORK

Since the limited release of +SAFE in 2001, several organisations have embarked on related work. The UK Ministry of Defence, Qinetiq, and the University of York have conducted workshops to discuss the application of +SAFE in the UK. The US DoD and the FAA will embark on a collaborative effort with the Australian DMO to further advance +SAFE for possible insertion to the FAA-iCMM. This work will also include investigation of the development of a System Security model extension.

CONCLUSION

The aim of the extended CMMI model is to enable assessments to identify potential programme weaknesses early in acquisition.

We have established that an extension of CMMI (continuous representation) for safety-related applications is feasible and defined a large portion of the safety process model. The exercise revealed some shortcomings of the CMMI approach when extending for additional disciplines.

The safety extension has been used in a variety of trials to assess organisations' capability in safety-related applications. Initial results have been positive; appraisers have been able to understand the model and results have been agreed upon.

REFERENCES

Australian Defence Standard Def(Aust) 5679, *The Procurement of Computer-based Safety Critical Systems,* 1998.

CMMI Product Development Team, "CMMI-SE/SW: Capability Maturity Model – Integrated for Systems Engineering/Software Engineering, Version 1.0 Continuous Representation", Software Engineering Institute technical report CMU/SEI-2000-TR-019, Carnegie Mellon University, USA, August 2000.

IEC International Standard 61508, *Functional safety of electrical / electronic / programmable electronic safety-related systems*, 1998.

NATO Standardization Agreement STANAG 4404, *Safety Design Requirements and Guidelines for Munition Related Safety Critical Computing Systems*, Edition 1.

Robinson, N., Lindsay P., Pitman A., "Extending the Integrated Capability Maturity Model (CMMI) for Safety-related Applications *Proceedings of INCOSE 2001*. INCOSE, New York, 2001.

RTCA DO-178B, *Software Considerations in Airborne Systems and Equipment Certification*, RTCA, 1992.

UK Ministry of Defence DefStan 00-55, *The Procurement of Safety Critical Software in Defence Equipment*, 1997.

UK Ministry of Defence 2nd Draft DefStan 00-56, *Safety Management Requirements for Defence Systems Containing Programmable Electronics*, 1996.

BIOGRAPHY

Dr. Mark Bofinger is a Senior Research Fellow in the Software Verification Research Centre (SVRC). Having previously studied at and worked for the SVRC in a research role, he is now working full-time providing consultancy and training services for clients in defence, transportation and processing. His work includes performing and facilitating safety analyses, systems and software engineering, and process improvement, focusing on high integrity and safety-critical systems.

Neil Robinson is a Senior Research Officer in the Software Verification Research Centre (SVRC). He is a Chartered Engineer, a Member of the British Computer Society and holds an Honours degree from the University of Reading. At the SVRC, Neil provides consultancy and training in safety-critical system development and conducts research in the areas of visualisation, requirements engineering and safety-critical systems. Neil's background includes systems engineering management and systems engineering for safety-critical systems as Principal Systems Engineer at Adtranz (DaimlerChrysler Rail Systems), as well as contract design and verification work, research into formal methods and lecturing in discrete mathematics.

Professor Peter Lindsay is Deputy Director of the Software Verification Research Centre, at the University of Queensland, Australia. He is co-author of two books on formal specification and verification of software systems. In recent years he has been involved with safety and security critical applications in areas such as embedded medical devices, ship-board defence, emergency service dispatch systems, and an international diplomatic network. He is a member, and past chair, of the Australian Computer Society's National Technical Committee on Safety Critical Systems. His current research interests include techniques for the analysis, development and assurance of trusted systems.

Mick Spiers is the Director of Software Engineering for the Defence Materiel Organisation (DMO). Mick is also a Software Engineering Institute (SEI) authorised SCAMPI Lead Appraiser with extensive appraisal experience using the CMMI. He is responsible for the development and oversight of software engineering and system safety policy for the DMO.

Matt Ashford is the software exhange officer in the Defence Materiel Organisation. He is currently on exchange with the US OSD and DCMA. Matt is also a highly experienced CMMI appraiser. He has assisted many projects to establish their system safety programs and has been instrumental in the development of +SAFE and system safety policy for the DMO.

Adrian Pitman is the Director of Quality Systems in the Defence Materiel Organisation. Adrian is also a candidate SCAMPI Lead Appraiser with extensive experience in capability maturity models including the CMMI.