Software Engineering Institute

+SAFE, V1.2
A Safety Extension to CMMI-DEV, V1.2

Defence Materiel Organisation, Australian Department of Defence

March 2007

TECHNICAL NOTE
CMU/SEI-2007-TN-006

Software Engineering Process Management Program

Carnegie Mellon

This report was prepared for the

SEI Administrative Agent
ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2100

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

Table of Contents

List of Figures

List of Tables

Executive Summary

+SAFE, V1.2 is an extension to the continuous representation of CMMI® for Development, Version1.2 (CMMI-DEV, V1.2) [SEI 2006]. This extension consists of two process areas added to CMMI-DEV to provide an explicit and focused basis for appraising or improving an organization's capabilities for providing safety-critical products.

The extension was developed because the Australian Defence Materiel Organisation recognized that CMMI is a generically structured framework that requires amplification for specialized areas of engineering such as safety engineering. Developing safety-critical products requires specialized processes, techniques, skills, and experience within an organization. CMMI provides a framework within which safety activities can take place; however, adding safety amplifications to CMMI-DEV would not provide sufficient guidance to make consistent judgments regarding supplier safety capability or improvement priorities.

A key aim of +SAFE is to identify the safety strengths and weaknesses of product and service suppliers, and to address identified weaknesses early in the acquisition process. The safety extension was developed so that CMMI appraisers and users can become familiar with the structure, style, and informative content provided to reduce dependence on safety domain expertise.

This extension was developed for standalone use. It is not intended to be embedded in a CMMI model and it does not rely on any specific safety standards. There are intentional overlaps with CMMI model content and with some safety standards. These overlaps are identified in this document.

The structure of the safety extension is shown in Table 1:

CMMI PA Category	Safety Process Area	Specific Goals
Project Management	Safety Management	SG1 Develop Safety Plans SG2 Monitor Safety Incidents SG3 Manage Safety-Related Suppliers
Engineering	Safety Engineering	SG1 Identify Hazards, Accidents, and Sources of Hazards SG2 Analyze Hazards and Perform Risk Assessments SG3 Define and Maintain Safety Requirements SG4 Design for Safety SG5 Support Safety Acceptance

Table 1: Structure of the Safety Extension

Abstract

+SAFE is an extension to CMMI® for Development (CMMI-DEV) that covers safety management and safety engineering. +SAFE supplements CMMI-DEV with two additional process areas that provide a basis for appraising or improving an organization's processes for providing safety-critical products. Developing such products requires specialized processes, skills, and experience. +SAFE is designed to identify safety strengths and weaknesses and to address identified weaknesses early in the acquisition process.

+SAFE was designed to reduce the dependence of CMMI appraisers on safety domain expertise. This extension was developed for standalone use. It is not intended to be embedded in a CMMI model document, nor does it rely on any specific safety standards. However, there are intentional overlaps with CMMI model content and some safety standards.

Since +SAFE is an extension of CMMI, it adopts the same assumptions, model structure, conventions, and terminology as CMMI and is affected by the general process-area and capability-level interactions inherent in CMMI. This technical report describes the +SAFE extension and how to use it to appraise an organization's capability in developing, sustaining, maintaining, and managing safety-critical products.

1 Introduction

+SAFE is an extension of the continuous representation of CMMI for Development, Version 1.2 (CMMI-DEV, V1.2) and is intended to specifically address safety.

Organizations from industry, government, and the Software Engineering Institute (SEI) jointly developed the CMMI Framework, a set of integrated models, the appraisal method, training materials, and supporting products. CMMI-DEV is the CMMI model released in 2006 that covers the development and maintenance activities applied to both products and services. Organizations from many industries, including aerospace, banking, computer hardware, software, defense, manufacturing, and telecommunications use CMMI-DEV [SEI 2006]. The +SAFE extension of CMMI-DEV presents safety-specific practices for improving the capability of an organization to develop safety-critical products.

1.1 BACKGROUND AND ACKNOWLEDGEMENTS

The Defence Materiel Organisation (DMO), part of the Australian Department of Defence, in conjunction with the Software Verification Research Centre (SVRC) at the University of Queensland, developed a safety extension to CMMI called +SAFE version 1.0, which was released to a limited audience for trial and evaluation. +SAFE was developed by DMO to permit a closer appraisal of an organization's ability to conduct safety-related work for the following reasons:

- DMO's experience has been that safety-related activities can create risks to acquisition cost and schedule performance if not managed and performed with disciplined. These risks arise from a variety of causes including: lack of training, inability to provide guidance to acquirer project offices, insufficient consultation between acquirers and stakeholders, and a lack of understanding of safety requirements and safety engineering.
- DMO is using CMMI and associated appraisal methods as an acquisition risk management tool. Although CMMI models provide a framework in which safety management and engineering can take place, the *required* and *expected* parts of CMMI models do not mention it. The only references to safety are in *informative* parts, and these references are slight.
- There is a risk that an organization that has been evaluated as adequately capable using the CMMI Framework may have inadequate process capability for safety management and safety engineering.

1.1.1 Version 1.0

The original version of +SAFE was developed using input from government, industry, and academia. DMO acknowledges the following contributing authors:

Matt Ashford (Defence Materiel Organisation)

Dr. Mark Bofinger (Software Verification Research Centre)

Prof. Peter Lindsay (Software Verification Research Centre)

Lisa Ming (Defense Contract Management Agency, U.S. DoD)

Adrian Pitman (Defence Materiel Organisation)

Pascal Rabbath (Defence Materiel Organisation)

Neil Robinson (Software Verification Research Centre)

Mick Spiers (Defence Materiel Organisation)

1.1.2 Version 1.1

The development of +SAFE version 1.1 was based on experience gained from the trial use of version 1.0, and a consolidated list of over 300 review comments received worldwide. DMO acknowledges the following individuals for their contribution to releasing version 1.1:

Matt Ashford (Defence Materiel Organisation)

Graham Bower-White (Ball Solutions Group)

Geoff Bowker (Bonket Pty. Ltd.)

Bradley Doohan (Defence Materiel Organisation)

Jennifer Murray (Defence Materiel Organisation)

1.1.3 Version 1.2

The development of +SAFE version 1.2 as an SEI technical note was a response to the Software Engineering Institute's 2006 release of CMMI-DEV, V1.2. Principally, this technical note contains editorial changes made to the Australian Department of Defence +SAFE, V1.1 that aligns it with CMMI-DEV, V1.2. SEI acknowledges the copyrighted work by DMO and the DMO's full support of publishing +SAFE as an SEI technical note. The SEI and DMO acknowledge the following individuals for their contribution to releasing this technical note version:

Mike Phillips (Software Engineering Institute)

Sandy Shrum (Software Engineering Institute)

Mike Konrad (Software Engineering Institute)

Bradley Doohan (Defence Materiel Organisation)

1.2 PURPOSE AND SCOPE

The purpose of +SAFE is to extend CMMI to provide an explicit, specific framework for functional safety with respect to developing complex safety-critical products. +SAFE is provided in a form that can be used standalone by experienced CMMI users with minimal support from safety domain experts.

- +SAFE is an extension of CMMI, so it adopts the same assumptions, model structure, conventions, and terminology as CMMI, and is affected by the general process-area and capability-level interactions inherent in CMMI. These relationships with CMMI are discussed further in section 1.4.
- The +SAFE extension to CMMI does not solely consist of the addition of new process areas, described in the standard CMMI manner, to existing process area categories. This document also contains additional informative components and some overlaps with CMMI. These overlaps are explained in section 1.4.
- The +SAFE framework is not specific to any safety standard, and standards that define safety principles, methods, techniques, work products, and product assessments may be used to satisfy the goals of the framework as appropriate. Relationships with safety standards are discussed further in section 1.5.

The context of +SAFE and its relationships with components, safety standards, and assessment and appraisal methods is shown in Figure 1.

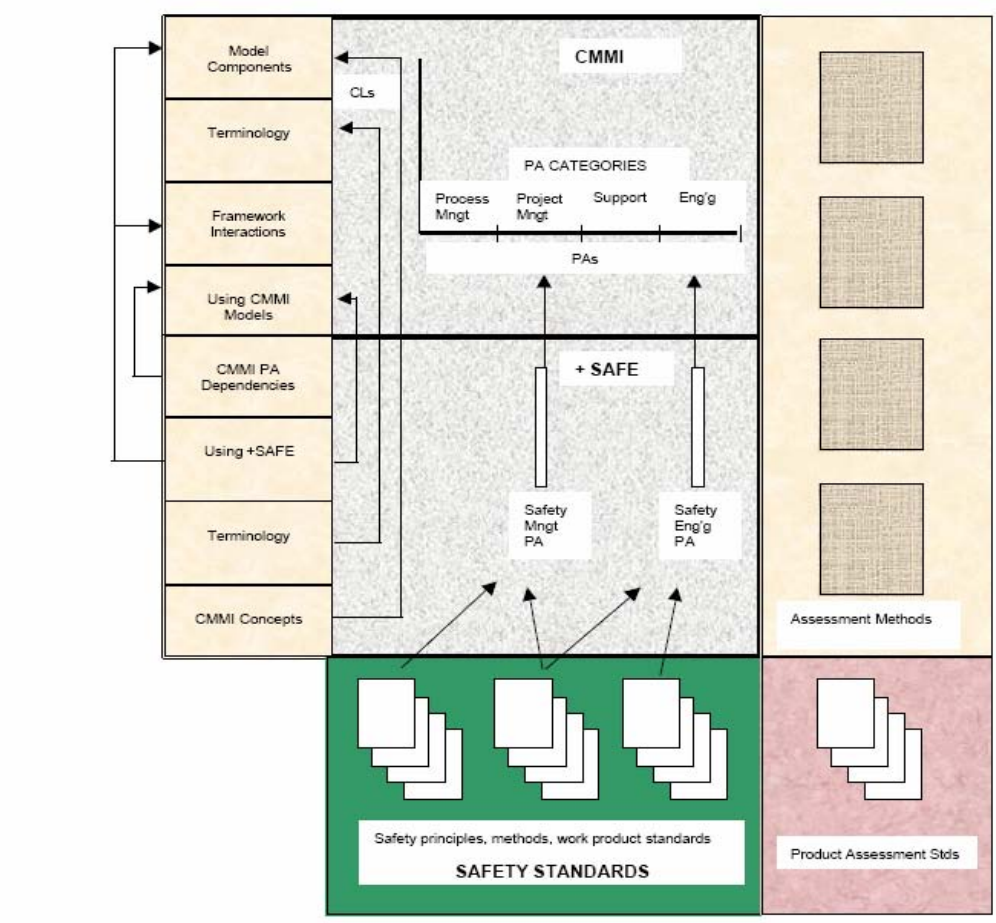

Figure 1: Context of +SAFE

1.3 USES OF +SAFE

+SAFE is used in the same applications as CMMI:

- As a framework for appraising the capability of a supplier or potential supplier of safety-critical products, +SAFE may be used by trained and qualified CMMI appraisers with no specific safety expertise to perform safety capability appraisals using SCAMPI or another suitable appraisal method [SEI 2001].
- As a framework for improving an organization's capability in developing, sustaining, maintaining, and managing safety-critical products, +SAFE may be used by organizations with CMMI and IDEAL[SM] (or equivalent) expertise to improve their safety capability [McFeeley 1996].

A +SAFE appraisal or improvement program may be integrated with a CMMI appraisal or improvement program. +SAFE may be used in appraisals or improvement programs just as any other process area in a CMMI model when a continuous representation is used.

1.4 +SAFE RELATIONSHIPS WITH CMMI-DEV

+SAFE is positioned as a set of additional process areas for CMMI. If the standalone requirement for +SAFE is removed, +SAFE's process areas integrate seamlessly into the Project Management and Engineering process area categories of CMMI, except for the following:

- The level of detail and amount of informative material (e.g., examples in practice descriptions, typical work products, subpractices, notes, discipline amplifications, generic practice elaborations, and references) is above the level typical in a CMMI process area, so that the reliance on subject matter expertise is reduced.
- The level of cross-referencing to other process areas is above the level typical in a CMMI process area, since some CMMI process areas could address safety as a nonfunctional attribute of a product and there is overlap or redundancy with practices in these process areas.
- The generic CMMI conventions where elements are "required" (specific and generic goals), "expected" (specific and generic practices) and "informative" (everything else) are reinforced in +SAFE to ensure that the informative content is not used prescriptively. Terms such as "e.g.", "sample", "indicators may include", and references to external standards explicitly delineate "informative" content from "required" or "expected" content.

In addition, +SAFE contains material that supplements the explanatory sections of CMMI:

- The *Framework Interactions* sub-section, which elaborates on the relationships between certain process area goals and certain capability level goals, is

extended to describe the broad relationships between +SAFE process areas and CMMI process areas (refer to section 1.8.2).

- The *Terminology* section is extended to include safety domain-specific terms (refer to section 1.9).
- The *Using CMMI Models* section is extended to include tailoring guidance for the +SAFE process areas, and identification of the requirements for users intending to apply the model (refer to section 3).

+SAFE also contains material that is fully redundant with CMMI to support its standalone use:

- Section 1.8 provides material on CMMI concepts for safety practitioners who may not be familiar with CMMI and who are required to assist in the application of +SAFE.
- +SAFE contains informative content (e.g., typical work products, subpractices, notes, discipline amplifications, generic practice elaborations, and references) that may be redundant with CMMI.

1.5 +SAFE RELATIONSHIPS WITH SAFETY STANDARDS

+SAFE does not require the use of any specific safety standard. As an extension to CMMI, +SAFE is an extension used for defining goals and for increasing levels of performance capability. The informative components of the extension are indicators of how goals may be achieved, but these components are not prescriptive and an organization can select the approaches it wishes to adopt to achieve the goals, including the selection of specific standards.

+SAFE is intended to be consistent with the Australian Defence Standard, *Safety Engineering in the Procurement of Defence Systems*, and is intended to be consistent with the principles of other contemporary safety standards (e.g., IEC's *Safety of Machinery—Functional Safety of Safety-Related Electrical, Electronic and Programmable Electronic Control Systems*; U.S. military standard, *System Safety Program Requirements*; the U.K. Defence Standard, *Safety Management Requirements for Defence Systems, Part 1, Issues 2 and 3*; and domain-specific safety standards wherever feasible) [ADoD 1998, CEI/IEC 2005, UKMoD 1997, UKMoD 2004, USDoD 1993].

+SAFE is not intended to be used as part of a product assessment (i.e., an appraisal based on this extension is not analogous to a *functional safety assessment* as defined in IEC's *Safety of Machinery—Functional Safety of Safety-Related Electrical, Electronic and Programmable Electronic Control Systems*).

1.6 STRUCTURE OF THE SAFETY EXTENSION

The structure of the safety extension is shown in Table 2 and was developed from the structure of the safety model presented in Australian defence standard, *The Pro-*

curement of Computer-Based Safety-Critical Systems, and the structure of CMMI [ADoD 2000].

CMMI PA Category	Safety Process Area	Specific Goals
Project Management	Safety Management	SG1 Develop Safety Plans SG2 Monitor Safety Incidents SG3 Manage Safety-Related Suppliers
Engineering	Safety Engineering	SG1 Identify Hazards, Accidents, and Sources of Hazards SG2 Analyze Hazards and Perform Risk Assessments SG3 Define and Maintain Safety Requirements SG4 Design for Safety SG5 Support Safety Acceptance

Table 2 Structure of the Safety Extension

1.7 INTENDED AUDIENCES

As discussed in section 1.3, there are two primary audiences for +SAFE:

1. CMMI appraisers who may not have specific safety expertise and the organizations they appraise
2. Organizations with CMMI and (systematic) process improvement expertise

In addition, a secondary audience for +SAFE are safety specialists who may be involved as subject matter experts in both appraisals and improvement programs. This group may not have any CMMI expertise.

1.7.1 Appraisers (Internal or Acquirers)

+SAFE was originally developed to satisfy the need for appraisers acting for an acquirer to undertake an appraisal of a supplier's or potential supplier's safety process capability. Such appraisals could be undertaken either as part of larger CMMI appraisals or as a standalone safety appraisal.

The purpose of these appraisals is to identify strengths and weaknesses in safety processes, and use this information to assist the acquirer in managing risks associated with an acquisition.

+SAFE was developed in the style of CMMI, so that appraisers and other users are familiar with the structure and style. The appraisers using this safety extension are trained CMMI appraisers, and have attended a short training session on +SAFE.

1.7.2 Organizations to Be Appraised

The organization's safety processes may not be structured the same way as the safety processes presented in +SAFE. The organization may also use terminology different from that used in +SAFE.

The organization may have alternative practices that meet the intent of the specific practices in +SAFE; however, the organization must satisfy the intent of the goals of the safety process areas.

1.7.3 Organizations Undertaking Process Improvement

+SAFE provides guidance to organizations on how to improve their safety processes, by describing specific practices that may be performed to achieve the goals of each process area, and by elaborating on the means for implementing the generic practices, which support achievement of the generic goals for each capability level.

To use this guidance effectively, the organization must implement processes from the CMMI Process Management process area category, and apply a systematic approach to process improvement using an improvement process such as SEI's IDEAL model [McFeeley 1996].

1.7.4 Safety Specialists

Safety specialists may be used in the application of +SAFE for both process appraisals and process improvement. In an appraisal, safety specialists may be used, like other subject matter experts in other areas, to assist the appraisal team in evaluating indicators such as alternative practices and work products, and developing appropriate improvement recommendations.

In an improvement program, safety specialists may be used in developing appropriate improvements to safety processes, and providing advice on their implementation. This assistance may include undertaking improvements to reduce risks identified by customers in their appraisal of the organization, and the use of relevant safety standards.

1.8 CMMI PREREQUISITES FOR THE USE OF +SAFE

+SAFE is intended for standalone use and in general does not depend on the process areas documented in CMMI. It does, however, depend on the capability level descriptions, and the general framework interactions inherent in CMMI. It also assumes that users are familiar with the CMMI Framework, terminology, and conventions, and are able to reference relevant sections of CMMI when required.

Several portions of CMMI can be used to provide a context for +SAFE. The text in CMMI Part 1 sections 1-5 and Part 3, *The Appendices and Glossary*, is applicable and should be consulted for further guidance on using and understanding the safety extension. Effective safety management and engineering depend on certain support processes being in place, including Process and Product Quality Assurance, Con-

figuration Management, and Decision Analysis and Resolution, (these CMMI process areas are not covered in detail in this document). The interactions are described in more detail in *CMMI Framework Interactions* on page 9.

1.8.1 Key CMMI Concepts

This section lists some key CMMI concepts important to understand before using +SAFE.

Process Areas Versus Process Descriptions

CMMI is a model that provides guidance for developing processes. It is not a set of process descriptions that can be directly applied in an organization. The actual processes used by an organization depend on many factors, including application domain(s) and organization structure and size. Thus, the process areas of a CMMI model do not typically map one-to-one with the processes used in an organization.

Process Areas and Capability Levels

The CMMI continuous representation supports the independent appraisal and improvement of each of the process areas described in a CMMI model. Any process area, including those described in the +SAFE safety extension, may be used to appraise organization processes, identify strengths and weaknesses, and improve these processes through the achievement of specific and generic goals in the capability levels. An organization focusing on appraising and/or improving its processes related to a process area endeavors to satisfy the goals of each capability level, commencing with level 1 and working upward. The +SAFE extension provides guidance in specific practices and elaborated generic practices in each of its process areas to assist users in identifying strengths and weaknesses, and in designing improvements.

Conventions (Numbering Systems, Abbreviations, Etc.)

CMMI defines a range of terminology, including terms specific to CMMI models, and other words that have a special meaning in CMMI models. These terms are defined in Parts 1 and 3 of CMMI-DEV.

Of particular interest to users of +SAFE is the abbreviation SP for “specific practice”. +SAFE does not use this abbreviation for safety plan, safety practice, safety procedure, or safety principles.

Required, Expected, and Informative Content

Content in CMMI models is classified as either “required” (i.e., specific and generic goals), “expected” (i.e., specific and generic practices), or “informative” (i.e., everything else). Organizations may meet specific and generic goals without performing expected specific and generic practices (i.e., by performing “alternative practices”). Organizations may draw on alternative bodies of knowledge instead of those used for the informative sections of the model. The +SAFE extension contains similarly classified content, and organizations may chose whether or not to adopt +SAFE expected practices or to make use of +SAFE informative material, as

long as the processes they implement meet the required specific and generic goals of the safety process areas.

1.8.2 CMMI Framework Interactions

Part 1 of a CMMI-DEV model identifies a number of interactions and interdependencies among process areas in process area categories, and between process areas and capability levels. +SAFE was designed to recognize these relationships. Further, +SAFE process areas are assigned to process area categories in CMMI in recognition of some of these relationships.

The safety extension also creates some new relationships, which are a by-product of the design decision to structure the extension as a set of separate process areas rather than as an embedded extension of CMMI:

- The relationship between Safety Management and the basic Project Management process areas of CMMI is similar to the relationship between the Risk Management process area and the basic Project Management process areas (refer to Figure 4.4 of CMMI-DEV). Safety Management influences the performance of the Project Planning, Project Monitoring and Control, and Supplier Agreement Management process areas in a similar manner to Risk Management, but it also influences the Risk Management process itself, by treating safety risks as a special case.
- The relationships between Safety Engineering and the Engineering process area category of CMMI is more complex. Safety Engineering is intended to influence the performance of all Engineering process areas. The interactions of the process areas remain as described in Figure 4.5 of CMMI-DEV, but Safety Engineering overlays each process area. Each goal of Safety Engineering is associated with one or more of the Engineering process areas and must be achieved concurrently with the goals of these other process areas.
- The relationships among Safety Management, Safety Engineering, and the Support process areas of CMMI are generic and the interactions described in CMMI-DEV are applicable to the +SAFE process areas.
- The interactions between Safety Management or Safety Engineering and CMM-DEV generic practices are also generic and the interactions described in CMMI-DEV are applicable to the +SAFE process areas. Few of the +SAFE specific practices, sub-practices, or work products are subsumed by generic practices, and it is unlikely that duplicate observations would result from an appraisal using +SAFE specific practices and CMMI generic practices.

1.9 ACRONYMS AND DEFINITIONS

The acronyms and definitions in Table 3 are used in this document. +SAFE terminology, unless specifically noted, is not based on any specific reference standard and is not country specific. Unless a reference is cited, terms have the meaning defined in this section or their dictionary meaning.

Standard CMMI abbreviations and numbering systems are used. Unless +SAFE has extended a CMMI term and the extended definition is included below, refer to Part 3, *The Appendices and Glossary*, of CMMI-DEV for definitions of all other CMMI terms.

Acronym or Glossary Term	Meaning
+SAFE	The safety extension to CMMI.
accident	An event or sequence of events that leads to harm, also known as a "mishap" or "hazardous event."
acceptably safe	The maximum level of risk of a particular technical process or condition that is regarded as acceptable in the circumstances in question.
appropriate	When applied to a method or technique used in safety-related engineering, "appropriate" is intended to mean that there is consensus that the method or technique is suitable for the relevant safety target. Some standards such as Def (Aust) 5679 and IEC 61508 recommend appropriate methods and techniques. There is currently little quantitative evidence that the methods and techniques recommended are actually *effective* in achieving the associated safety targets. Hence +SAFE avoids the word "effective," which is, however, used in CMMI.
CMMI	Capability Maturity Model Integration
CMMI-DEV	Capability Maturity Model Integration for Development
CMMI +SAFE	CMMI with the safety extension.
DMO	Defence Materiel Organisation, Australian Department of Defence.
harm	The consequence when a safety risk matures. Types of harm include harm to people (e.g., fatalities and serious and/or minor injuries), damage to property or the environment, loss of product capability, damage to or loss of data, or economic loss.
hazard	A situation with the potential to lead to an *accident.*

high-level safety argument	A *safety argument* for a major function or component of a safety-critical product.
LOT	level of trust. A measure of the level of confidence or trust that one wishes to have that the product meets a given product safety requirement.
MOTS	military off the shelf
OTS	off the shelf
safety	An acceptable level of risk. Absolute safety (i.e., zero risk) is not generally achievable. Therefore, we define safety in terms of the level of risk that is deemed acceptable.
safety argument	The statement of why a particular characteristic of a product or product component meets safety requirements and safety targets. The statement is usually structured as an argument and its supporting evidence. Also known as “safety case argument.”
safety case	Depending on the domain, the safety case is either: (1) the complete body of evidence that proves an item was designed and integrated correctly to approved standards by competent people in accordance with approved procedures with sufficient mitigation, and tested sufficiently to justify it being safe; or (2) a well-reasoned summary document detailing what the original safety program aims were versus what was actually achieved, and a risk analysis (with recommendations) of the differences. Also known as a system safety assessment (SSA) and assurance case.
safety case argument	See *safety argument*.
safety criteria	The limits of acceptable risk associated with a *hazard*. These limits may be defined (externally) as imposed *safety targets*, or developed from analysis or development policy.
safety critical	A product or product component that, based on a safety assessment, has *safety requirements* that must be satisfied for the product or product component to be accepted for service.
safety function	A functional requirement that is needed to ensure the safety of the product. Also known as *safety functional requirement.*

safety functional requirement	See *safety function*.
safety incident	An event in which injury or damage could have occurred and either: (1) raises concern about the safety of any person, product, mission, or procedure; (2) raises the requirement for a modification or change to procedures or products as a result of the event, or (3) highlights a lesson to be learned from the event.
safety lifecycle	The project or product lifecycle in which safety processes are performed.
safety related	Products, items, or processes used to implement a function or component of safety.
safety risk	When applied to a situation, the (safety) risk presented is a combination of the likelihood and consequence (i.e., severity of any resulting *harm*).
safety principles	Management and engineering principles for developing and operating systems and product components so that they are most likely to meet *safety requirements.*
safety requirement	Any requirement that is needed to ensure the safety of the product. These requirements include *safety functional requirements* and their associated *safety targets.*
SCAMPI	Standard CMMI Appraisal Method for Process Improvement.
SEI	Software Engineering Institute.
(safety) target	A qualitative or quantitative target associated with a safety requirement. A safety target is intended to express how safe an implementation of the safety requirement must be.

Table 3: Acronyms and Definitions

1.10 CHANGES FORECAST

+SAFE Version 1.2 aligns with CMMI-DEV, Version 1.2. The following changes are forecast to +SAFE:

- Development of +SAFE to span and cross reference other CMMI constellations
- Development of additional training and case studies for applying the model for both appraisal and improvement.

- Provision of guidance on target capability profiles and the recommended scope of appraisals.

2 +SAFE

This section consists of the two +SAFE process areas that specifically address safety:

- Safety Management
- Safety Engineering

These process areas are presented in the same format and style as other CMMI process areas.

SAFETY MANAGEMENT

A Project Management Process Area

Purpose

The purpose of Safety Management is to ensure that safety activities (including those relating to suppliers) are planned, the performance and results of safety activities are monitored against the plan, and deviations from plans are corrected.

Introductory Notes

The Safety Management process area involves the following:

- Using safety principles, criteria, and targets to establish plans for safety activities that satisfy safety requirements
- Implementing the plans, monitoring safety incidents, and managing them in accordance with the plans
- Developing and implementing agreements with suppliers for the acquisition of safety-related products and services

The Safety Management process area addresses the need for the project to effectively consider safety requirements and how they may be satisfied by both management activities and technical methods. The integration of safety management with other planning viewpoints (e.g., quality, risk, supplier agreement management, cost, and schedule) ensures that safety activities are given the planning, monitoring, and control focus commensurate with their importance.

When suppliers external to the project are used to provide products, components, and services, safety management ensures that relevant requirements are incorporated into supplier agreements and that these agreements are satisfied.

Safety management is a continuous process that spans the lifecycle of the project, and that adopts these management principles:

- Safety issues should be addressed early in the project lifecycle, and should be tracked throughout.
- Safety assurance requires independent visibility of both the product and the process.

- Safety assurance must be transferable to parties outside the project (including suppliers).
- An iterative, continuous, and evolutionary process must be used.

Related Process Areas

Refer to the Safety Engineering process area for more information about hazard identification and analysis, risk assessment, development of safety requirements, technical solutions, safety verification and validation, and preparation of the safety case.

Refer to the Risk Management process area for more information about risk identification, analysis, and mitigation. (Technical aspects of safety risk management are dealt with in the Safety Engineering process area.)

Refer to the Project Planning process area for more information about developing project plans and integrating different planning viewpoints.

Refer to the Project Monitoring and Control process area for more information about monitoring project activities.

Refer to the Decision Analysis and Resolution process area for more information about using a formal evaluation process to evaluate alternatives, which could be useful for developing a safety strategy.

Refer to the Supplier Agreement Management process area for more information about managing supplier agreements.

Specific Goals

SG 1 **Develop Safety Plans**

Safety plans based on safety requirements, safety criteria, and safety management principles are established and maintained as a basis for managing safety throughout the project lifecycle.

SG 2 **Monitor Safety Incidents**

Safety incidents are monitored, reported, analyzed, and resolved.

SG 3 **Manage Safety-Related Suppliers**

The acquisition of safety-related products and services from suppliers external to the project is managed by means of a formal agreement that includes safety requirements.

Generic Goals

GG 1 **Achieve Specific Goals**

The safety management process supports and enables achievement of the specific goals of the process area by transforming identifiable input work products to produce identifiable output work products.

GG 2 **Institutionalize a Managed Process**

The process is institutionalized as a managed process.

GG 3 **Institutionalize a Defined Process**

The process is institutionalized as a defined process.

GG 4 **Institutionalize a Quantitatively Managed Process**

The process is institutionalized as a quantitatively managed process.

GG 5 **Institutionalize an Optimizing Process**

The process is institutionalized as an optimizing process.

Practice to Goal Relationship Table

SG 1 Develop Safety Plans
- SP 1.1 Determine Regulatory Requirements, Legal Requirements, and Standards
- SP 1.2 Establish Safety Criteria
- SP 1.3 Establish a Safety Organization Structure for the Project
- SP 1.4 Establish a Safety Plan

SG 2 Monitor Safety Incidents
- SP 2.1 Monitor and Resolve Safety Incidents

SG 3 Manage Safety-Related Suppliers
- SP 3.1 Establish Supplier Agreements That Include Safety Requirements
- SP 3.2 Satisfy Supplier Agreements That Include Safety Requirements

GG 1 Achieve Specific Goals
- GP 1.1 Perform Specific Practices

GG 2 Institutionalize a Managed Process
- GP 2.1 Establish an Organizational Policy
- GP 2.2 Plan the Process
- GP 2.3 Provide Resources
- GP 2.4 Assign Responsibility
- GP 2.5 Train People
- GP 2.6 Manage Configurations
- GP 2.7 Identify and Involve Relevant Stakeholders
- GP 2.8 Monitor and Control the Process
- GP 2.9 Objectively Evaluate Adherence
- GP 2.10 Review Status with Higher Level Management

GG 3 Institutionalize a Defined Process
- GP 3.1 Establish a Defined Process
- GP 3.2 Collect Improvement Information

GG 4 Institutionalize a Quantitatively Managed Process
- GP 4.1 Establish Quantitative Objectives for the Process
- GP 4.2 Stabilize Subprocess Performance

GG 5 Institutionalize an Optimizing Process
- GP 5.1 Ensure Continuous Process Improvement
- GP 5.2 Correct Root Causes of Problems

Specific Practices by Goal

SG 1 Develop Safety Plans

Safety plans based on safety requirements, safety criteria, and safety management principles are established and maintained as a basis for managing safety throughout the project lifecycle.

SP 1.1 Determine Regulatory Requirements, Legal Requirements, and Standards

Identify and document regulatory requirements, legal requirements, and applicable standards.

Applicable specific regulatory requirements, legal requirements, or requirements for compliance with standards for processes or work products, are identified and documented. Such requirements may either be directly applicable to the domain (e.g., avionics) or should be tailored to the domain.

Refer to the Requirements Development process area for more information about eliciting, documenting, analyzing, and validating requirements.

Where such requirements are directly applicable to the domain, they should be integrated with requirements that are developed as a result of hazard and risk assessment on the project.

Refer to the Safety Engineering process area for more information about establishing safety requirements based on analysis of project safety risks.

Refer to the Risk Management process area for more information about the identification and analysis of project risks.

Safety standards differ in their approach to safety. The intention of +SAFE is to allow for the approaches described in most modern safety standards; however, safety standards must be applied consistently within a project. In general, it is preferable to use the framework of a single safety standard if this approach is sufficient to cover the scope of the project's requirements. If multiple safety standards are used, consider the compatibility of the standards and the resolution of conflicts.

> An example in which multiple safety standards may be applicable is the production of a missile, which can involve separate standards for the following:
>
> - Ordnance
> - Electromagnetic interference
> - Avionics

Typical Work Products

1. Requirements source lists
2. Requirements categories list
3. Safety requirements specification
4. Product requirements specification (with safety annotations)
5. Safety requirements trace

Subpractices

1. Determine requirements sources.

   Safety requirements may arise from contractual, legal, and regulatory product and work performance standards, or common law sources. Some countries place a legal obligation on suppliers of safety-related equipment or services irrespective of contractual requirements (or lack thereof). For example, under Australian common law, an organization owes a duty of care to its employees and to members of the public who may be inadvertently harmed by that organization's activities.

2. Identify, categorize, and document safety requirements.

   Safety requirements are elicited from the sources identified and collected into related groups or categories where they are organized and documented. This process assists in the subsequent development of safety strategies and plans.

The following factors may be considered when determining safety requirement categories:

- The phases of the project's lifecycle model
- The types of processes used
- The types of products used
- The risk management taxonomy or framework used by the project

Safety requirements may be documented in a safety requirements specification or included with other product requirements. Safety requirements should be traceable to their sources.

Refer to the Requirements Management process area for more information about traceability of requirements to source requirements.

SP 1.2 Establish Safety Criteria

Establish and maintain safety criteria that reflect the level of acceptable safety.

It is a generally accepted concept that absolute safety is unachievable. In this light, the concept of "acceptably safe" is applied through the definition of what is considered to be an acceptable level of risk. The acceptable level of risk may be defined qualitatively or quantitatively, using safety criteria.

Safety criteria may include targets (or failure probability objectives) for various types of harm. Safety targets are usually derived from policies set by government, regulatory bodies, customers, or the organization itself.

The types of harm that may be considered include the following:

- Harm to people (fatalities and serious or minor injuries)
- Damage to property or the environment
- Loss of product capability
- Damage to or loss of data
- Economic loss

Refer to the Requirements Development process area for more information about eliciting needs, which may include safety targets.

Safety criteria may also include risk assessments, defining the likelihood and consequence of each risk, and acceptable levels within these dimensions. The parameters for scaling likelihood and consequence are normally aligned with the parameters used for rating other types of risk.

Refer to the Risk Management process area for more information about the analysis and categorization of project risks and risk mitigation strategies.

The applicability of the targets and the scope of the risk assessment should be recorded to ensure that hazard identification and risk assessment activities are complete and provide a record of the justifications for any exclusions from the assessment scope. The scope of safety targets and the scope of acceptable levels of risk may be apportioned in various ways.

Criteria may be based on the harm attributable to the following:

- All products
- Each product
- Each product component
- Each accident
- Each hazard

Typical Work Products

1. Safety criteria (usually contained in the safety plan) expressed as one or more of the following:

   a. Targets and their applicability

   b. Hazard/risk likelihood/impact matrix, showing acceptable levels of risk

   c. Risk indices

2. Safety strategy (usually contained in the safety plan)

Subpractices

1. Identify requirements for safety criteria.

   The safety requirements or situations in which acceptably safe criteria must be defined are identified and methods for defining acceptably safe levels of risk are selected. These methods may be selected on the basis of other safety requirements (e.g., regulatory requirements that include safety targets) or on aligning them with the broader risk management approach of the project.

2. Determine safety targets and/or acceptable levels of risk.

   Safety targets are defined for each of the safety requirements or situations where a target is required. Acceptable levels of risk are defined for each of the safety requirements.

3. Document safety criteria for required harm types and scopes.

Safety criteria are specified as targets, their applicability, acceptable levels of risk, and their scope. Associated with acceptable levels of risk are thresholds for triggering action to mitigate against exceeding acceptable levels. Any exclusions from the analysis are identified and justified.

SP 1.3 Establish a Safety Organization Structure for the Project

Establish and maintain a safety organization structure for the project, including specifying roles and duties of personnel and groups, providing reporting channels, and ensuring adequate levels of managerial and technical independence.

A safety organization structure for a project should include the need for managerial and technical independence in the conduct of safety-related activities. It should also provide for the resolution of disputes relating to safety, and for the independent audit of safety processes and safety cases.

Independence is important for ensuring the following:

- Staff members in a safety role are not put under unreasonable pressure to acquiesce on safety issues.
- Staff members who are responsible for independent verification, validation, or assessment consider designs from a fresh perspective and reveal problems that might not be identified by those who are closer to the design.

If a person other than the project manager is given responsibility for safety management within the project, then that person should be given a line of appeal outside the project. The line of appeal should be to a person in the organization with authority higher than the project manager.

Example elements of a safety organization structure for a project include the following:

- Safety roles and responsibilities in the project
- The duties for each safety role in the project
- Reporting lines and communication channels between safety roles and from safety roles to other roles in the project
- The level of authority for each safety role in the project structure (e.g., ability to initiate work or financial authority)

Example roles to be documented in the structure of a project safety organization include the following:

- Acceptance body
- Certification body
- Safety management group
- System safety working group
- Safety manager
- Safety engineers
- Safety authority
- Quality assurance

Refer to the Organizational Training process area for more information about establishing strategic training needs, which may include safety-related training.

Typical Work Products

1. Project organization chart and responsibility allocation matrix
2. Project safety plan

For example, an organization chart may include the following:

- A project manager who supervises both a technical manager and a safety manager
- A safety manager who can report to both the project manager and to another manager who is independent of project pressures
- Safety personnel who report to both the technical manager and the safety manager
- Safety representatives from suppliers reporting to a safety manager

SP 1.4 Establish a Safety Plan

Establish and maintain a safety plan.

The safety plan is established using safety management principles and references applicable regulatory requirements and standards, the project safety lifecycle, and use of appropriately trained and knowledgeable personnel. The planning should also cover safety engineering and support processes for safety verification, validation, and independent safety assessment activities, such as audits and evaluations.

Many standards specify particular methods and techniques that are considered to be appropriate for safety-related work. The methods and techniques may vary according to the complexity and/or safety targets

of the products being developed. These issues should be considered in safety planning.

The safety plan is reviewed and accepted by both project management and the independent line of reporting for safety issues.

Refer to the Project Planning process area for more information about establishing, integrating, and gaining commitment to plans.

A safety plan typically addresses or references the following:

- Product description
- Program safety requirements, criteria, and targets
- Integration of the safety engineering lifecycle and processes with product development and the project lifecycle model
- Identification of key safety milestones
- Integration of safety engineering with support processes such as configuration management and change management, and the tracking of dependencies
- Risk assessment procedures and hazard analysis techniques
- Hazard tracking and resolution procedures, including mitigation, review, and acceptance procedures
- A detailed description of the process of deriving safety requirements and the rules and techniques for each level of trust or safety integrity levels.
- Verification techniques
- Schedules for safety evaluation activities and event entry and exit criteria
- Project safety organization, roles and responsibilities, and plans for ensuring project staff have the required level of safety skills and knowledge

Typical Work Products

1. Safety plan
2. Certification plan
3. Safety verification plan
4. Safety validation plan
5. Independent safety assessment plan
6. Safety acceptance plan
7. Safety staff skills and experience matrix
8. Safety training plan

Subpractices

1. Document the project safety lifecycle and its processes.

Document a safety lifecycle for the project and product. The project safety lifecycle should be integrated into the overall project lifecycle. The product safety lifecycle should cover all product lifecycle phases, from initial concept through to disposal. Safety must be ensured throughout each lifecycle. In particular, issues relating to safety should be addressed as early as possible. Where specific processes must be performed to satisfy the safety strategy, these processes should be identified and integrated with other project processes.

2. Plan for safety acceptance.

   Safety acceptance of the project plans and the product should be sought at key points in the project lifecycle. To reduce the risk of major acceptance problems late in the project is reduced, projects should aim to obtain staged acceptance as the project progresses. Planning should document the key stages of the acceptance, what is delivered for assessment, and who provides acceptance at each stage.

   Planning for safety acceptance may be contained in a project verification and validation plan instead of the safety plan.

3. Plan for needed knowledge and skills in the performance of safety-related activities.

   For safety-related activities, it is particularly important that staff have adequate experience, training, and skills. Attitudinal characteristics of safety-related staff are significant selection criteria. In certain domains, selection criteria can also include licensing schemes that ensure staff members are licensed before they undertake unsupervised safety-critical work:

   - Establish competency requirements. (Competency requirements are documented in terms of expected qualifications, skills, years of experience, etc.)
   - Establish training requirements. (Where there are shortfalls against the competency requirements, it may be possible to train people to meet the required competency.)
   - Establish recruitment requirements. (Where there are shortfalls against the competency requirements and it is not possible to train existing staff to the required competency, then it may be necessary to engage specialists.)

SG 2 Monitor Safety Incidents

Safety incidents are monitored, reported, analyzed, and resolved.

SP 2.1 Monitor and Resolve Safety Incidents

Monitor, report, analyze, and resolve safety incidents and maintain safety analyses.

Processes are in place and a culture has been promoted to ensure that safety-related incidents that arise during the project lifecycle are

reported. Reported incidents are resolved by reviewing the existing hazard analysis and risk assessment in the project safety plan, and updating the analysis as necessary. The resolution of such incidents may result in the need for corrective or preventative action, including the update of both safety-related and non-safety-related project artifacts.

Refer to the Measurement and Analysis process area for more information about data collection and reporting.

Refer to the Project Monitoring and Control process area for more information about monitoring activities, which can include monitoring safety incidents and can form the basis for initiating review actions.

Refer to the Causal Analysis and Resolution process area for more information about identifying root causes, which when applies to safety incidents, can enable initiating preventative action.

Typical Work Products

1. Minutes of meetings (e.g., of the safety management group)
2. Updated project safety plan
3. Updated hazard analysis
4. Updated safety case
5. Updated hazard log
6. Incident reports
7. Change requests

Subpractices

1. Monitor and analyze safety incidents.

   The status of safety activities and their results are monitored on a periodic and event-driven basis. Any incidents are reported and logged, and the safety plan is reviewed to ensure that the incidents are effectively managed to closure, or change requests are generated to revise the safety plan. The collection of incident reports is analyzed for trends that may require revisions to the safety plan.

2. Resolve safety incidents.

   Incidents either are managed to closure using the existing safety plan, or the plan (including hazard log, hazard analysis, and safety cases) is revised to manage the incident and to include any required preventative actions.

SG 3 Manage Safety-Related Suppliers

The acquisition of safety-related products and services from suppliers external to the project is managed by means of a formal agreement that includes safety requirements.

SP 3.1 Establish Supplier Agreements That Include Safety Requirements

Analyze the project's needs to acquire safety-related products and services, select suppliers, and include appropriate safety requirements in supplier agreements.

Where a need to acquire a safety-related product or service is identified, select an appropriate supplier and establish an agreement that includes relevant safety requirements.

When procuring safety-related products and services, supplier agreements should allow for necessary monitoring activities and should require the delivery of safety assurance (e.g., a safety case) with any delivered product. The acquirer retains responsibility for the impact that the acquired product components or services has on the safety of the product.

Give particular consideration to the acquisition of off-the-shelf (OTS) products, which may be acquired from commercial suppliers (commercial off-the-shelf or COTS), government (government off-the-shelf or GOTS), or outside the project in the acquirer organization itself (e.g., military off-the-shelf or "MOTS"). The advantages of OTS products could be offset by the unknowns in their safety characteristics, which may not be determined economically from the product itself. Appropriate evaluation activities should be undertaken and the results of these activities used as input to supplier agreement development.

For Software Engineering

Selection of COTS software to use in a product may involve comprehensive review of field-use data with the software vendor, and a design approach that allows for the product to detect failures and operate in a functionally degraded but acceptably safe mode in the event of COTS software failure.

Depending on the criticality of the COTS software component, the integrator or product developer may wish to appraise the development or production processes used by the software supplier as part of the development of the supplier agreement.

Refer to the Decision Analysis and Resolution process area for more information about evaluating and selecting among alternatives, which may include externally-supplied products, services, and suppliers.

Refer to the Supplier Agreement Management process area for more information about developing and managing supplier agreements, including the handling of OTS products.

Refer to the Technical Solution process area for more information about incorporating the results of formal evaluations of OTS products into the design of the solution.

Typical Work Products

1. Supplier agreements that include safety requirements
2. Supplier management plan (or relevant section of the project management plan)
3. Subcontractor management plan (or relevant section of the project management plan)

Subpractices

1. Ensure that all products and services to be acquired are assessed to establish whether or not they are safety-related.

   In general, the project should assume that all products and services to be acquired are safety-related unless proven otherwise.

2. Establish safety requirements for each safety-related product and service.
3. Include consideration of safety risk when selecting suppliers.

   Suppliers should be assessed to ensure they have appropriate processes, skills, and experience for supplying safety-related products and services.

4. Include safety requirements in the supplier agreements.

   The supplier agreement should include safety requirements for the product or service. It should cover the following:

   - How the supplier interacts with the project on safety matters (e.g., lines of communication for safety matters that link into the project safety organization structure)
   - The commitment of both the project and the supplier to participate in ongoing safety activities (e.g., through participation in a safety working group)
   - The need to deliver a safety case as part of the safety-related product or service
   - The commitment of the supplier to report all project-related safety incidents to the project in a timely manner

5. Create an appropriate level of involvement between the organization and its supplier.

   The supplier agreement should include the responsibility of the organization and the supplier to provide support for each other's activities. This support may involve the presence of personnel on the product safety working groups and other groups set up by the other organization.

SP 3.2 Satisfy Supplier Agreements That Include Safety Requirements

Execute supplier agreements that include safety requirements and ensure that safety assurance is delivered with the product or service.

Supplier agreements are executed and monitored. Procedures should be in place to monitor progress and performance of safety-related suppliers (e.g., through regular progress reviews and/or audits examining safety-related activities). Special provisions for the acquisition of "off the shelf" (OTS) products may require specific monitoring and review.

The project should ensure that suitable safety assurance is delivered with any product delivered as part of the agreement (e.g., in the form of a safety case).

Refer to the Supplier Agreement Management process area for more information about establishing and managing supplier agreements, including the handling of OTS products.

Refer to the Verification process area for more information about ensuring that products and services meet their requirements.

Refer to the Requirements Management process area for more information about managing the traceability of requirements, including safety requirements.

Typical Work Products

1. Safety requirements specifications
2. Product requirements specifications (with safety annotations)
3. Review minutes
4. Audit records
5. Supplier assessment records and recommendations
6. Product or service verification records

Subpractices

1. Establish traceability of safety issues between the organization and the supplier.

   In general, the majority of safety requirements flow from the organization to the supplier. Assumptions made by either party must be propagated throughout the system to check their validity.

   Safety analysis of the supplier may need to be constructed and used in the context of a wider safety analysis of the organization.

Other issues requiring traceability include schedules, competencies, and other support practices.

2. Monitor and support the technical performance of the supplier.

   Periodic meetings and reviews may be part of monitoring.

   Supporting the supplier may involve the inclusion of the organization in meetings of groups within the supplier such as the system safety working group.

Considerations that are important when acquiring OTS products include the following:

- Transferring existing safety assurance of the OTS product into a suitable form for the project
- Securing the operational history of the OTS product
- Ensuring compatibility of the organization's environment with the original environment of an OTS product when transferring assurance or using operational histories
- Accurately identifying the configuration or version of OTS products
- Ensuring any transferred assurance or operational history applies to the version of the OTS product supplied
- Identifying and analyzing unspecified functionality of OTS products
- Securing ongoing support of the OTS product

Generic Practices by Goal

GG 1 Achieve Specific Goals

The safety management process supports and enables achievement of the specific goals of the process area by transforming identifiable input work products to produce identifiable output work products.

GP 1.1 Perform Specific Practices

Perform the specific practices of the safety management process to develop work products and provide services to achieve the specific goals of the process area.

GG 2 Institutionalize a Managed Process

The process is institutionalized as a managed process.

GP 2.1 Establish and Maintain an Organizational Policy

Establish and maintain an organizational policy for planning and performing the safety management process.

Elaboration:

Policies for the safety processes of the organization are established. Regulatory requirements, legal requirements, and standards that are applicable to most of the organization's projects are identified and documented.

The policies should be appropriate for projects to develop safety processes. Projects determine the applicability of these requirements and standards and, if necessary, tailor these requirements for their specific needs.

GP 2.2 Plan the Process

Establish and maintain the plan for performing the safety management process.

Elaboration:

Typically, elements of the plan for performing the safety management process are part of the project plan (as described in the Project Planning process area). The project and subordinate plans address the specific needs and objectives for the project. However, some parts of the plan may reside outside the project with one or more independent groups, such as safety assurance, the certification authority liaison, or contract management. These parts of the plan address both project and organizational viewpoints.

Refer to the Project Planning process area for more information about planning, which can be applied to planning the safety management process.

GP 2.3 Provide Resources

Provide adequate resources for performing the safety management process, developing the work products, and providing the services of the process.

Elaboration:

Examples of resources provided include the following:

- Project-independent oversight and escalation of safety issues
- Specialists that provide technical advice (e.g., user requirements representatives and specialist engineers [human factors, software, systems, quality])
- Specialist supplier and contract management staff
- Preferred supplier lists
- Requirements trace and incident tracking programs
- Hazard log tracking tools (containing analysis arguments or references)
- Failure mode and effects analysis tools

GP 2.4 Assign Responsibility

Assign responsibility and authority for performing the process, developing the work products, and providing the services of the safety management process.

Elaboration:

The concerns described in SP 1.3 for management independence in the conduct of safety-related activities, and provision for the resolution of disputes relating to safety apply to the assignment of responsibility for performing the safety management process.

Typically, independence considerations can be dealt with in the organization (i.e., distinct from the project) structure by providing safety staff that are not attached to specific projects. Safety staff within projects can then be provided with lines of appeal to independent safety staff within the organization as a whole.

Example elements of a safety organization structure at the organization level include the following:

- Safety roles and responsibilities in the organization
- The duties for each safety role in the organization
- How the safety roles in the organization as a whole interact with individual projects
- Reporting lines and communication channels between safety roles and from safety roles to other roles in the organization

GP 2.5 Train people

Train the people performing or supporting the safety management process as needed.

Elaboration:

Effective performance of the safety management process requires people with a combination of safety discipline and application domain skills, knowledge, and experience; and a culture that ensures safety planning and management is appropriately prioritized with other planning and management viewpoints.

Examples of training topics include the following:

- Safety awareness programs
- Product safety
- Safety planning
- Safety incident reporting
- Hazard identification and analysis
- Causal analysis
- Application domain-specific training (e.g., flight systems)
- Related process areas: Project Planning, Project Monitoring and Control, Risk Management, Process and Product Quality Assurance, and Configuration Management

Refer to the Organizational Training process area for more information about identifying and meeting training needs.

GP 2.6 Manage Configurations

Place designated work products of the safety management process under appropriate levels of control.

Elaboration:

The level of configuration management deemed appropriate may depend on the safety requirements for the product in question. Traceability of safety requirements to agents such as external suppliers or certifiers also generates configuration management requirements for both work products and inputs of the safety management process.

Example work products to be placed under configuration management include the following:

- Safety plans
- Hazard log
- Hazard analysis
- Safety analysis
- Designations of safety-critical items (identity, location)
- Safety checklists
- Incident reports

Refer to the Configuration Management process area for more information about the management of configuration items.

GP 2.7 Identify and Involve Relevant Stakeholders

Identify and involve the relevant stakeholders of the safety management process as planned.

Elaboration:

Stakeholders may have a safety-related interest in the outcome of the project. The identification of such stakeholders is important, not only to involve them in the project and to keep them informed of outcomes, but to ensure that independence is not compromised by a conflict of interest.

Some standards require the establishment of a safety working group to aid in involving stakeholders in managing and performing safety activities.

Example stakeholder groups include the following:

- Customer requirement representatives
- Engineering discipline experts
- Regulatory authorities
- Test and evaluation centers
- Stores clearance specialists
- Explosive safety boards

Example work products requiring stakeholder involvement in their development or approval include the following:

- Safety plans
- Safety requirements
- User safety constraints
- Customer-related safety instructions

GP 2.8 Monitor and Control the Process

Monitor and control the safety management process against the plan for performing the process and take appropriate corrective action.

Elaboration:

The project is monitored against the project safety plan, typically by a team (e.g. the safety working group or a milestone review team). Corrective action is taken when the project deviates significantly from the project safety plan. Corrective action may include updates to the safety plan.

A hazard log provides one mechanism for checking the progress of safety activities. Residual risk levels can be monitored expecting that there will be gradual rectification.

Refer to the Project Monitoring and Control process area for more information about monitoring activities and managing corrective action.

GP 2.9 Objectively Evaluate Adherence

Objectively evaluate adherence of the safety management process against its process description, standards, and procedures, and address noncompliance.

Elaboration:

Perform safety product and process audits periodically as a means of confirming that the safety process is implemented as planned and that it satisfies applicable safety policies, procedures, requirements, standards, and objectives. Audits are carried out throughout the project lifecycle by independent auditors with dual lines of reporting.

Refer to the Process and Product Quality Assurance process area for more information about objective evaluations.

Examples of safety activities reviewed include the following:

- Safety planning
- Safety verification

Safety audits do not cover the scope of a functional safety assessment or independent safety assessment.

Refer to the Safety Engineering process area for more information about independent safety evaluations.

Examples of safety work products include the following:

- Audit reports
- Defect reports
- Updated safety plan
- Safety requirements specification
- Hazard analysis and hazard log
- Risk assessment reports
- Review and walkthrough checklists

GP 2.10 Review Status with Higher Level Management

Review the activities, status, and results of the safety management process with higher level management and resolve issues.

Elaboration:

Reviews of the project safety status are held on a periodic and event-driven basis with appropriate levels of management, including independent reporting lines, to provide visibility into project safety risk exposure and appropriate corrective action.

Typically, these reviews include a summary of progress against safety criteria, the status of risk mitigation efforts, and any safety issues that require escalation.

Refer to the Project Monitoring and Control process area for more information about progress and milestone reviews.

GG 3 Institutionalize a Defined Process

The process is institutionalized as a defined process.

GP 3.1 Establish a Defined Process

Establish and maintain the description of a defined safety management process.

GP 3.2 Collect Improvement Information

Collect work products, measures, measurement results, and improvement information derived from planning and performing the safety management process to support the future use and improvement of the organization's processes and process assets.

Elaboration:

Examples of works products, measures, measurement results, and improvement information include the following:

- Results of safety management reviews
- Results from analysis of safety incidents
- Supplier performance reports
- Independent evaluations of supplier safety work products

GG 4 Institutionalize a Quantitatively Managed Process

The process is institutionalized as a quantitatively managed process.

GP 4.1 Establish Quantitative Objectives for the Process

Establish and maintain quantitative objectives for the safety management process that address quality and process performance based on customer needs and business objectives.

GP 4.2 Stabilize Subprocess Performance

Stabilize the performance of one or more subprocesses to determine the ability of the safety management process to achieve the established quantitative quality and process performance objectives.

GG 5 Institutionalize an Optimizing Process

The process is institutionalized as an optimizing process.

GP 5.1 Ensure Continuous Process Improvement

Ensure continuous improvement of the safety management process in fulfilling the relevant business objectives of the organization.

GP 5.2 Correct Root Causes of Problems

Identify and correct the root causes of defects and other problems in the safety management process.

SAFETY ENGINEERING

An Engineering Process Area

Purpose

The purpose of Safety Engineering is to ensure that safety is adequately addressed throughout all stages of the engineering process.

Introductory Notes

The Safety Engineering process area involves the following:

- Identification of hazards, accidents, and sources of hazards; and analysis of those identified to assess safety-related risk
- Development of safety requirements that address safety-related risks
- Application of safety principles throughout the project lifecycle to ensure that safety requirements are satisfied
- Development of an audit trail that can support safety acceptance and provide the information needed to validate safety strategies, plans, and plan implementation

The Safety Engineering process area addresses the technical analysis and engineering of safety requirements and the application of safety engineering principles in the development of a technical solution. The integration of safety engineering with other engineering processes (involving requirements, technical solution, integration, and verification) ensures that safety aspects of the requirements and technical solution are engineered at appropriate points in the project lifecycle, and that their priority relative to other requirements or characteristics of the solution is explicitly addressed.

The specific practices in Safety Engineering employ the technical safety principles that safety is best achieved by using tried and trusted techniques; that an iterative, continuous, and evolutionary development process is required; that critical functions should be as simple as possible, and isolated from the rest of the product; and that for the most critical cases, formal mathematical proof of correctness may be appropriate.

Refer to the Safety Management process area for more information about safety criteria, planning, monitoring and control, and supplier management.

Refer to the Requirements Development process area for more information about elicitation, analysis, and validation of requirements.

Refer to the Technical Solution process area for more information about developing a technical solution that meets requirements.

Refer to the Product Integration process area for more information about the iterative, incremental assembly of the product.

Refer to the Verification process area for more information about verifying that work products satisfy their requirements.

Refer to the Validation process area for more information about acceptance criteria.

Refer to the Process and Product Quality Assurance process area for more information about activities that verify that process descriptions, procedures, and standards are adhered to during the development process.

Specific Goals

SG 1 **Identify Hazards, Accidents, and Sources of Hazards**

Hazards, accidents, and sources of hazards are identified.

SG 2 **Analyze Hazards and Perform Risk Assessments**

Analyze hazards and perform risk assessments.

SG 3 **Define and Maintain Safety Requirements**

Safety requirements are developed and maintained to address the hazards.

SG 4 **Design for Safety**

Safety principles are applied throughout the project lifecycle and safety requirements are satisfied.

SG 5 **Support Safety Acceptance**

The process of safety acceptance is supported by establishing and maintaining a hazard log and safety case, through independent safety assessments, and through validation of the assumptions of safety activities.

Generic Goals

GG 1 **Achieve Specific Goals**

The safety engineering process supports and enables achievement of the specific goals of the process area by transforming identifiable input work products to produce identifiable output work products.

GG 2 **Institutionalize a Managed Process**

The process is institutionalized as a managed process.

GG 3 **Institutionalize a Defined Process**

The process is institutionalized as a defined process.

GG 4 **Institutionalize a Quantitatively Managed Process**

The process is institutionalized as a quantitatively managed process.

GG 5 **Institutionalize an Optimizing Process**

The process is institutionalized as an optimizing process.

Practice to Goal Relationship Table

SG 1 Identify Hazards, Accidents, and Sources of Hazards
- SP 1.1 Identify Possible Accidents and Sources of Hazards
- SP 1.2 Identify Possible Hazards

SG 2 Analyze Hazards and Perform Risk Assessments
- SP 2.1 Analyze Hazards and Assess Risk

SG 3 Define and Maintain Safety Requirements
- SP 3.1 Determine Safety Requirements
- SP 3.2 Determine a Safety Target for Each Safety Requirement
- SP 3.3 Allocate Safety Requirements to Components

SG 4 Design for Safety
- SP 4.1 Apply Safety Principles
- SP 4.2 Collect Safety Assurance Evidence
- SP 4.3 Perform Safety Impact Analysis on Changes

SG 5 Support Safety Acceptance
- SP 5.1 Establish a Hazard Log
- SP 5.2 Develop a Safety Case Argument
- SP 5.3 Validate Product Safety for the Intended Operating Role
- SP 5.4 Perform Independent Evaluations

GG 1 Achieve Specific Goals
- GP 1.1 Perform Specific Practices

GG 2 Institutionalize a Managed Process
- GP 2.1 Establish an Organizational Policy
- GP 2.2 Plan the Process
- GP 2.3 Provide Resources
- GP 2.4 Assign Responsibility
- GP 2.5 Train People
- GP 2.6 Manage Configurations
- GP 2.7 Identify and Involve Relevant Stakeholders
- GP 2.8 Monitor and Control the Process
- GP 2.9 Objectively Evaluate Adherence
- GP 2.10 Review Status with Higher Level Management

GG 3 Institutionalize a Defined Process
- GP 3.1 Establish a Defined Process
- GP 3.2 Collect Improvement Information

GG 4 Institutionalize a Quantitatively Managed Process
- GP 4.1 Establish Quantitative Objectives for the Process
- GP 4.2 Stabilize Subprocess Performance

GG 5 Institutionalize an Optimizing Process
- GP 5.1 Ensure Continuous Process Improvement
- GP 5.2 Correct Root Causes of Problems

Specific Practices by Goal

SG 1 Identify Hazards, Accidents, and Sources of Hazards

Hazards, accidents, and sources of hazards are identified.

Hazard identification, hazard analysis, and risk assessment are steps in an iterative process that may be revisited multiple times during the project lifecycle.

SP 1.1 Identify Possible Accidents and Sources of Hazards

Identify possible accidents and sources of hazards.

The identification of potential accidents is a useful first step in the hazard identification process. Different standards use different terminology to describe accidents. Refer to section 1.9, Acronyms and Definitions, for examples of alternate terms.

The following are examples of potential accidents:

- A mid-air collision of aircraft
- An explosion in a processing plant

Identifying sources of hazards helps to provide a structure to hazard identification.

The following are examples of potential sources of hazards:

- Separation of turbine blades in an aircraft engine while under load
- Containment failure and leakage of toxic materials in a processing plant

For Software Engineering

An example of a potential source of hazard is dead (unused) code.

Methods for identifying sources of hazards include referencing standard safety practices appropriate to the product and referencing regulatory requirements.

For Software Engineering

An example of a standard safety practice for software that uses data from field (physical) sources is range checking of all input data.

Typical Work Products

1. Hazard checklist
2. Hazard log
3. Accident list
4. Hazard source lists (external and internal)
5. Hazard category lists

SP 1.2 Identify Possible Hazards

Identify and document possible hazards using an appropriate model of the product as a basis.

It is important that hazard identification is as complete as possible. The earlier hazards are identified in the project lifecycle, the easier and more cost-effective it is to deal with them.

Information about hazards is logged, typically in a hazard log.

The success of hazard identification and analysis depends largely on the model of the product used. This model should genuinely reflect the current system concept and design and should provide sufficient detail on the intended functionality of the product to allow a systematic hazard analysis. A graphical representation of the product can help the hazard identification and analysis team understand the product.

Typical Work Products

1. Product environment and boundary definition
2. Hazard analysis scope definition
3. Functional model of the product
4. Hazard and operability analysis (HAZOP) tables
5. Functional failure analysis (FFA) tables
6. Hazard log

Subpractices

1. Document the scope and interfaces of the product to be delivered.

   Documenting the scope and interfaces of the product to be delivered enables identification of hazards on that boundary.

Refer to the Requirements Development process area for more information about identifying interfaces and documenting requirements, which will help you in documenting system boundaries.

2. Define the functionality of the product.

   A functional model of the product can provide an effective basis for hazard identification and analysis.

Refer to the Requirements Development process area for more information about establishing operational concepts and scenarios and defining required functionality, which provide the basis for creating a functional model of the product.

3. Use the model of the product as the basis for hazard identification and hazard analysis.

Refer to the Technical Solution process area for more information about designing the product.

4. Use a systematic approach that includes consideration of all phases of the project lifecycle.

   Systematic approaches include hazard and operability analysis (HAZOP) and functional failure analysis (FFA).

Teams of personnel should be formed to perform the hazard analysis, with consideration given to the effectiveness of those teams. Appropriate personnel should be involved, which may include personnel with the following experience:

- Relevant domain experience
- Knowledge of all parts of the project lifecycle (e.g. commissioning, operation, and maintenance)
- Experience with hazard identification

Historical data should be used, including information on past incidents and accidents, and checklists specific to the domain.

Refer to the Safety Management process area for more information about the consideration of all lifecycle phases.

5. Document all hazards identified.

Cross reference each hazard to all of the following:

- Related analysis
- Related safety requirements
- Related verification requirements and records

SG 2 Analyze Hazards and Perform Risk Assessments

Hazards are analyzed and risk assessments performed.

SP 2.1 Analyze Hazards and Assess Risk

For each hazard, analyze possible causes, likelihood, and consequence, and assess the severity of the risk presented by that hazard.

Apply a structured, systematic method or methods to determine potential consequences, likelihood, and preconditions for each hazard. Combine these elements to determine the potential risk posed by the hazard, and compare the potential risk with criteria for risk mitigation and management strategies.

Some standards do not require the development of risk indices as a combination of likelihood and consequence, but use other alternate measures to analyze and classify risks.

An example of an alternative measure that is applied in analyzing risk is the use of assigned "levels of trust," which are based on the level of control that the product has over the initiation or prevention of the hazard.

Refer to the Risk Management process area for more information about identifying and analyzing risks.

Typical Work Products

1. Failure modes and effects analysis reports
2. Failure modes, effects, and criticality analysis reports
3. Event tree analysis reports
4. Fault tree analysis reports
5. Risk assessment reports
6. Hazard logs

Subpractices

1. Assess and determine potential consequences of hazards.

   Determine all potential consequences, including accidents, of each hazard related to the product. Approaches to systematic consequence analysis include failure modes and effects analysis.

   Consequences may be assessed qualitatively (e.g., catastrophic, major, or minor) or quantitatively (e.g., 10 fatalities, 1 fatality, or 1 severe injury).

2. Determine sequences of events leading to hazards.

   Determine the conditions and events that lead to hazards. Systematic causal analysis approaches include fault tree analysis and event tree analysis.

3. Assess the likelihood of potential accidents.

   The likelihood of the hazard leading to accidents is assessed.

   Likelihood may be assessed qualitatively (e.g., frequent, rare, or extremely rare) or quantitatively (e.g., 1 occurrence in 10 years, 1 occurrence every 10,000 operations, or 1 occurrence every 100 missions).

   A quantitative measure of the likelihood of a potential accident is based on the analysis of the hazards for which that accident is a possible consequence. The likelihood of each individual event in the event sequence that results in an accident may be drawn from sources such as the following:

   - Manufacturer's specifications of involved equipment
   - Historical data from previous accidents

   When systematic failures are seen as contributing to the likelihood of an accident (e.g., where software failures may cause the accident), quantitative analysis is generally seen as inappropriate. Instead, the process is often reversed to set safety targets for system failure rates.

4. Combine consequence and likelihood to obtain the estimate of risk presented by each hazard.

Refer to the Risk Management process area for more information about defining risk parameters.

5. Compare the risk presented by each hazard with the criteria for acceptability.

   Where a risk exceeds criteria, a risk management strategy is invoked to mitigate against the maturing of the risk.

SG 3 Define and Maintain Safety Requirements

Safety requirements are developed and maintained to address the hazards.

Safety requirements are developed that specify the safety functions addressing the hazards, risks, and safety criteria, and specify the required safety target for each safety function. These requirements are maintained throughout the project lifecycle.

SP 3.1 Determine Safety Requirements

Determine the safety requirements based on the outcome of the hazard identification, hazard analysis, and risk assessment.

Where the hazard analysis and risk assessment identify hazards that are either unacceptable or must be reduced, these hazards shall be addressed by safety requirements. Typically, the requirements specify the means of mitigating or detecting and reducing the exposure time of the hazard.

Typical Work Products

1. Safety requirements specification
2. Product requirements specification (with safety annotations)

Refer to the Safety Management process area for more information about the regulatory, legal, and standards sources of safety requirements and targets.

Refer to the Requirements Development process area for more information about the development of requirements.

SP 3.2 Determine a Safety Target for Each Safety Requirement

Determine an applicable safety target for each safety requirement.

Safety targets may be specified qualitatively or quantitatively. A target may apply to one or more requirements.

Quantitative targets may be expressed as a frequency of hazardous failure.

A qualitative target may be expressed as requirements for processes used in the development or testing of components to meet safety requirements.

Where qualitative targets have been derived from quantitative targets, achievement of the qualitative target is intended to satisfy (but generally does not guarantee satisfaction of) the quantitative target.

Where products suffer from systematic failures (e.g., software products), quantitative targets are often replaced by qualitative targets. The required reliability of a safety function may be translated to requirements for the processes used to develop and test that safety function. However, the requirements for the processes do not replace the target for the safety function. Satisfying qualitative process targets does not necessarily satisfy quantitative targets.

Refer to the Safety Management process area for more information about the regulatory, legal, and standards sources of safety requirements and targets, and on selection of product safety standards.

Typical Work Products

1. Safety requirements specification
2. Product requirements specification (with safety–related requirements annotated)
3. Records of traceability between requirements and targets

Subpractices

1. Determine any hazards associated with each safety requirement.

   This determination can be achieved through derivation from the risk assessment of each hazard. Hazards may be eliminated during the development of a technical solution.

2. Determine the acceptability of the hazards associated with each safety requirement.

   This determination can be achieved through derivation of the acceptable risk that was set for each hazard during hazard analysis and risk assessment.

3. Compare the assessed risk against the acceptable risk.

   Compare the assessed risk for each safety requirement with the acceptable risk for each safety requirement.

4. Set a safety target for each safety requirement.

   The safety target should ensure the level of risk presented by the product is less than or equal to the acceptable risk, and should ensure the estimates of assessed risk used in the hazard analysis and risk assessment are carried forward into product design.

It may be infeasible to determine if a safety target has been met (e.g., where failures are systematic in nature or where failure rates are sufficiently low to make testing prohibitively time consuming). In such cases, safety targets may be used in determining how the product is to be developed. However, such translations from quantitative targets to qualitative methods are generally not applicable in reverse. Use of appropriate qualitative methods does not ensure that safety targets have been satisfied.

SP 3.3 Allocate Safety Requirements to Components

Safety requirements are allocated to product components and safety-related products.

Safety requirements may be allocated to product components or combinations of components. In cases where combinations of components are responsible for satisfying the requirement, the performance should be partitioned for unique allocation to each product component as a derived requirement.

Refer to the Requirements Development and Technical Solution process areas for more information about allocating product component requirements.

This specific practice provides information for defining the allocation of safety requirements but must interact with the specific practices in the Technical Solution process area to establish solutions to which the requirements are allocated.

Refer to the Decision Analysis and Resolution process area for more information about identifying, evaluating, and selecting alternatives.

Typical Work Products

1. Technical data package that addresses safety
2. Requirement allocation sheets
3. Records of traceability for requirements and safety targets

Subpractices

1. Allocate requirements and design constraints to functions.

   Note that this allocation may create a need for new solution components.

2. Allocate requirements to components of the solution.

   Safety requirements are allocated to components in a manner consistent with the capabilities of the components.

3. Document relationships among allocated requirements and traceability of targets.

The allocation of safety requirements also allocates safety targets to solution components.

SG 4 Design for Safety

Safety principles are applied throughout the project lifecycle and safety requirements are satisfied.

Safety principles are applied at appropriate points in the project lifecycle and in the performance of all processes to ensure that safety requirements are satisfied.

Refer to the Technical Solution process area for more information about solution design and development.

The specific practices of this goal provide information on how safety requirements may be satisfied but must interact with the specific practices in the Technical Solution process area to deliver solutions that satisfy all requirements.

Refer to the Verification process area for more information about how verify that requirements are met.

SP 4.1 Apply Safety Principles

Select solutions based on safety principles.

The chosen solution should be appropriate to meet the safety requirements, based on the available knowledge at the time when the decision is made. However, safety principles have broader application than to the safety requirements for the solution and its components. These principles may affect the solution development process, its methods and tools, and the resources used in the process.

Refer to the Technical Solution process area for more information about how a technical solution is developed and selected.

Many of the specific practices of the Technical Solution process area may be affected by the application of safety principles, such as Develop Alternative Solutions and Selection Criteria, Select Product Component Solutions, and Perform Make, Buy or Reuse Analysis.

Examples of alternative solutions that may be applied to a particular problem include the following:

- Redundancy in architecture
- Diversity in architecture
- Isolation of critical components
- Alarms and warnings
- Protective clothing
- Emergency procedures and responses

The selection of alternative solutions may be applied according to an order of precedence; alternatives are not mutually exclusive.

An example order of precedence might be to apply the following (from highest precedence to lowest precedence):

- Redesign to eliminate the risk due to the hazard
- Redesign to reduce the risk due to the hazard
- Incorporate safety devices
- Incorporate warning devices
- Develop training and operational procedures

The extent to which solutions are developed to address safety may also be determined according to safety principles.

The principles applied may include "as low as reasonably practicable" (ALARP) and the precedence in which to apply mitigations.

ALARP is the principle of applying mitigations until the costs of applying such mitigations outweigh the benefit gained. Where a level of acceptability has been set, ALARP may result in reduction beyond that level.

Refer to the Decision Analysis and Resolution process area for further information on how to evaluate identified alternatives using a formal evaluation process.

Typical Work Products

1. Alternative solutions incorporating safety principles
2. Solution selection criteria addressing safety
3. Safety-related decisions and rationales as applied in product-component selection

Subpractices

1. Establish selection criteria for safety principles at relevant points in the development lifecycle.

2. Use selected safety principles to contribute to the development of alternate solutions.

   Ensure simplicity in the design of the safety-related product. Consider means of detecting faults, recovering from faults, and limiting the effects of damage resulting from faults.

3. Use selected safety principles to contribute to the selection of the product component solution that best satisfies the criteria established.

SP 4.2 Collect Safety Assurance Evidence

Ensure that evidence to validate the safety case is developed and collected in all the processes involved in the production of the product throughout the project lifecycle.

Ensure that supporting evidence is collected that will make the safety case valid.

The actual evidence is determined by the activities planned for and the outcomes of safety activities, including setting safety targets for safety requirements. Evidence may also be influenced by the safety standard chosen and the practices recommended or not recommended under various circumstances.

Refer to the Safety Management process area for more information about safety assurance in purchased components and services.

Refer to the Requirements Management, Requirements Development, Technical Solution, Verification, Validation, Configuration Management, and Process and Product Quality Assurance process areas for more information about some of the activities that may be called on for supporting evidence.

Typical Work Products

1. Analysis reports
2. Review minutes and comments
3. Test records
4. Implemented design
5. Validation test reports
6. Audit reports

Subpractices

1. Use appropriate implementation methods to develop the safety-related product.

The implementation techniques used should be appropriate to the safety requirements and safety targets. Some standards suggest techniques to use at different levels of risk.

For Software Engineering

For critical software components, implementation methods may include techniques such as the following:

- *Use of a safe subset of a high level programming language*
- *Use of multiple redundancy, multiple language implementations, and voting systems*
- *Use of trusted kernels and services*

Where use of an off-the-shelf product has been selected as the preferred method of implementation, the acquirer has little or no control over the selection of implementation techniques by the supplier. However, the attributes of the implementation techniques used by the supplier, and their effect on the safety characteristics of the product must be evaluated.

For Software Engineering

Selection of COTS software for use in a product may involve appraisal of the development and production processes used by the software supplier and collection of assurance data from the appraisal.

Refer to the Technical Solution process area for more information about solution implementation.

2. Use appropriate verification techniques.

Verification techniques used should be appropriate to the safety requirements and safety targets.

Example analysis and design techniques include the following:

- The use of formal (mathematical) proofs in high-assurance cases
- Verification of components and the product using simulation

For Software Engineering

Review and inspection techniques may include the use of structured reviews such as the software technique called a Fagan inspection.

Testing techniques may require testing to a particular level of structural, data, or path coverage.

Evidence that off-the-shelf products were verified by the product supplier may not be available to the acquirer. Alternate techniques for verification may need to be adopted.

Example verification techniques include the following:

- Use of field-use data, including reference sites and service histories
- Accelerated service-life testing

Refer to the Verification process area for more information about work product verification.

3. Document the results of safety verification.

   All verification evidence should be collected and documented to demonstrate that the safety requirements and targets have been satisfied.

4. Trace verification activities to safety requirements and targets.

Refer to the Requirements Management process area for more information about the traceability between requirements and work products, which can include verification plans and results.

5. Analyze the results of verification.

   Corrective action may be required as a result of verification activities.

Refer to the Verification process area for more information about establishing verification procedures and criteria as well as analyzing verification results.

6. Use appropriate safety validation techniques.

   The validation techniques used should be appropriate to the safety requirements and targets. If validation is carried out using simulation, then the validity of the simulation should be confirmed.

   For example, confirming a validation may include the use of statistical testing techniques to demonstrate a quantitative requirement has been satisfied.

Refer to the Validation process area for more information about establishing validation procedures and criteria.

7. Document the results of safety validation.

Refer to the Validation process area for more information about documenting validation procedures and results.

8. Trace validation activities to safety requirements and targets.

Refer to the Requirements Management process area for more information about traceability between requirements and work products, which can include validation plans and results.

SP4.3 Perform Safety Impact Analysis on Changes

When changes are proposed to the requirements or the design, an impact analysis is carried out to assess the impact on safety.

It is important that proposed changes are assessed in terms of their impact on safety. In particular, changes should not violate any of the assumptions in the hazard and risk assessment. Where a change affects a hazard and risk assessment carried out in earlier parts of the project lifecycle, it may be necessary to repeat the analysis.

Changes are approved before they are made and all changes are documented. Hazard information is kept up to date with changes as they occur.

Typical Work Products

1. Change proposals
2. Change records
3. Impact analysis
4. Updated hazard analysis and hazard log

SG 5 Support Safety Acceptance

The process of safety acceptance is supported by establishing and maintaining a hazard log and safety case (or equivalents) through independent safety assessments and through validation of the assumptions of safety activities.

Some safety standards identify alternate practices to the specific practices covered under this specific goal, or use different mechanisms to achieve the same result. Safety acceptance is often dependent on external factors and agencies (e.g., regulatory bodies) and each may impose its own requirements for acceptance evidence.

Refer to the Validation process area for more information about acceptance testing.

The specific practices of this goal provide information on how safety acceptance may be supported, but must interact with the specific practices in the Validation process area to gain acceptance of all requirements.

SP 5.1 Establish a Hazard Log

Establish and maintain a method of logging and tracking hazard status.

Once a hazard has been identified and documented, its status should be tracked to closure. The status of hazards provides a good basis for monitoring and controlling project progress against safety matters.

To effectively track a hazard to closure, the status of each hazard must be monitored regularly.

Typical Work Products

1. Hazard log
2. Hazard status summaries
3. Action requests

Example hazard information to be logged includes the following:

- A complete description of the hazard
- Who identified the hazard and when
- The consequences of the hazard and the severity of any resulting accidents
- What could cause the hazard
- Risk assessment of the hazard
- How the hazard is detected, controlled, or mitigated
- The subsequent impact of risk management actions on risk likelihood and consequences
- Safety requirements that are derived from the hazard
- Where the safety requirements are addressed in the design
- Verification requirements that are derived from the safety requirements
- Verification records
- Cross references to other documents (that may document the above hazard information).

SP 5.2 Develop a Safety Case Argument

An argument is developed to outline how it will be shown that the product is acceptably safe.

A safety case presents an argument for the safety of the product being developed by the project. A safety case should consist of two parts:

1. A coherent argument for the safety of the product
2. The supporting evidence for the argument

Not all safety standards require the development of a safety case. In such cases, other documents may be used to achieve the same goal (e.g., safety assessment report).

It can be advantageous to release the safety case in incremental stages throughout the project to gain early acceptance of the project safety approach and to support project lifecycles in which incremental safety acceptance is a requirement. For some products, it is helpful to produce multiple documents that make up the overall safety case; in these instances the structure of the documents should be clear.

An example stage-based safety case release is the use of developmental phase and aircraft kit-proof (first article) phase safety cases in aircraft development.

The safety argument should be clear, consistent, complete, comprehensible (to all stakeholders), and defensible, and should cover all stages of the project lifecycle. To ensure the argument is readable, supporting evidence is cross-referenced from the main body of the argument.

Examples of safety case content include the following:

- A high-level summary of the safety argument
- Relevant standards and regulatory requirements
- The configuration baseline
- All identified hazards and the residual risk of each
- All operational and support assumptions
- All safety-related design decisions and features and the rationale for each

Typical Work Products

1. High-level safety argument
2. Cross references to supporting evidence
3. Supporting evidence

Typically, the supporting evidence is the safety documentation developed throughout the project safety lifecycle. It includes plans, specifications, analysis reports, verification reports, and validation reports. Supporting evidence for a safety case includes the following:

- evidence of hazard identification and risk assessment activities
- evidence of system hazard analysis activities
- evidence of all safety assurance activities, including the results of safety assessments

SP 5.3 Validate Product Safety for the Intended Operating Role

Validate that the safety requirements and safety targets for the product's intended use are satisfied in the product's intended environment, either through validating on site or through simulation.

Refer to the Validation process area for more information about the validation of products.

Typical Work Products

1. Validation plan and procedures
2. Validation environment
3. Validation results

Subpractices

1. Validate the assumptions that are used in the safety case.
2. Continue to validate the product when in operation.

   It is important to confirm that product performance in operation meets its specified performance and that assumptions made in the safety analysis are validated in operation.

SP 5.4 Perform Independent Evaluations

Perform independent evaluations of the product, safety processes, and the safety case.

An independent evaluation is carried out by investigating the project and the products developed by the project. The evaluation includes the following:

- Familiarization with the product
- Familiarization with the hazards of the product
- Review and analysis of project deliverables

The evaluation may also include reworking parts of the safety work carried out by the project. Typically, the evaluator presents findings and recommendations to the person responsible for safety acceptance. The recommendations of the evaluator are used as part of the final decision of the acceptance body.

Independence is important for ensuring the following:

- Evaluators are not put under unreasonable pressure to acquiesce on safety issues.
- Evaluators consider the design from a fresh perspective and reveal problems that might not be identified by those who are closer to the design.

Some standards specify levels of independence to achieve sufficient objectivity.

Refer to the Safety Management process area for further information on the independence of evaluators.

Refer to the Process and Product Quality Assurance process area for more information about independent evaluation of work products, services, and processes.

Typical Work Products

1. Safety evaluation report
2. Independent safety assessment report

Generic Practices by Goal

GG 1 Achieve Specific Goals

The process supports and enables achievement of the specific goals of the process area by transforming identifiable input work products to produce identifiable output work products.

GP 1.1 Perform Specific Practices

Perform the specific practices of the safety engineering process to develop work products and provide services to achieve the specific goals of the process area.

GG 2 Institutionalize a Managed Process

The process is institutionalized as a managed process.

GP 2.1 Establish an Organizational Policy

Establish and maintain an organizational policy for planning and performing the safety engineering process.

Elaboration:

Policies for the safety processes of the organization are established. Regulatory requirements, legal requirements, and standards that are applicable to most of the organization's projects are identified and documented.

The policies should be appropriate for projects to develop safety processes. Projects determine the applicability of these requirements and standards and, if necessary, tailor these requirements for their specific needs.

GP 2.2 Plan the Process

Establish and maintain the plan for performing the safety engineering process.

Elaboration:

Typically, elements of the plan for performing the safety engineering process are part of the safety plan, although these elements may be contained in the project plan (as described in the Project Planning process area). However, some parts of the plan may reside outside the project with one or more independent groups, such as safety assurance, the certification authority liaison, or contract management. These parts of the plan address both project and organizational viewpoints.

The plan for safety engineering may take on various formats according to the requirements of regulatory agencies.

Examples of safety engineering process plans include the following:

- System safety plan
- System safety program plan
- Plan for software aspects of certification
- Safety management plan
- Verification and validation plan

Refer to the Project Planning process area for more information about planning activities.

GP 2.3 Provide Resources

Provide adequate resources for performing the safety engineering process, developing the work products, and providing the services of the process.

Elaboration:

Examples of resources provided include the following:

- Specialist technical staff (e.g., user requirements representatives and specialist engineers [human factors, software, systems, quality])
- Hazard log tracking tools (containing analysis arguments or references)
- Failure mode or effects analysis tools

GP 2.4 Assign Responsibility

Assign responsibility and authority for performing the process, developing the work products, and providing the services of the safety engineering process.

Elaboration:

The safety plan or project plan, the organization's safety policies, statutory and regulatory requirements, and requirements for independence determine who is assigned responsibility and authority for safety engineering practices.

GP 2.5 Train People

Train the people performing the safety engineering process as needed.

Elaboration:

Effectively performing the safety engineering process requires people with a combination of safety discipline; engineering discipline; the application domain skills, knowledge, and experience; and a culture that ensures that safety engineering is appropriately prioritized relative to other engineering viewpoints.

Examples of training topics include the following:

- Safety awareness
- System safety
- Safety incident reporting
- Hazard identification and analysis
- Causal analysis
- Application domain-specific topics (e.g., flight systems)

Refer to the Organizational Training process area for more information about training for activities.

GP 2.6 Manage Configurations

Place designated work products of the safety engineering process under appropriate levels of control.

Elaboration:

The level of configuration management deemed appropriate may depend on the safety requirements for the product in question. Traceability of safety requirements to agents, such as external suppliers or certifiers, also generates configuration management requirements for work products and inputs of the Safety Engineering process.

Example work products to be placed under configuration management include the following:

- Hazard log
- Hazard analysis
- Safety analysis
- Safety checklists
- Incident reports

Refer to the Configuration Management process area for more information about managing configuration items.

GP 2.7 Identify and Involve Relevant Stakeholders

Identify and involve the relevant stakeholders of the safety engineering process as planned.

Elaboration:

Stakeholders may have a safety-related interest in the engineering activities of the project.

For example, if the project is developing a product that resides in the vicinity of other safety-related products, then the suppliers of those products may be concerned about electro-magnetic interference from the new product and should be included as stakeholders.

Relevant stakeholders of many of the engineering activities are those with the domain, technology, or product experience required to perform those activities.

For example, a hazard analysis should be performed by a diverse range of personnel to ensure that the analysis addresses the wide range of aspects that may affect safety.

GP 2.8 Monitor and Control the Process

Monitor and control the safety engineering process against the plan for performing the process and take appropriate corrective action.

Elaboration:

The project is monitored against the project safety plan, typically by a team (e.g., the safety working group, design review group). Corrective action is taken when the project deviates significantly from the project safety plan. The corrective action may include updates to the safety plan.

A hazard log provides one mechanism for checking the progress of safety activities. Residual risk levels can be monitored expecting that there will be gradual rectification.

Refer to the Project Monitoring and Control process area for more information about monitoring and controlling activities.

GP 2.9 Objectively Evaluate Adherence

Objectively evaluate adherence of the safety engineering process against its process description, standards, and procedures, and address noncompliance.

Elaboration:

Perform safety product and process audits periodically as a means of confirming that the safety engineering process is implemented as planned and satisfies safety policies, requirements, standards, and objectives. Audits are performed throughout the project lifecycle.

Audit safety processes against safety planning documentation and applicable procedures.

Audit the work products of safety processes to ensure they comply with requirements and applicable process descriptions, standards, and procedures.

Examples of safety activities that are audited include the following:

- Analysis of hazards
- Selection of product components
- Derivation and allocation of safety requirements

Examples of safety work products that are audited include the following:

- Safety cases
- Hazard logs

Refer to the Process and Product Quality Assurance process area for more information about evaluating work products.

GP 2.10 Review Status with Higher Level Management

Review the activities, status, and results of the safety engineering process with higher level management and resolve issues.

Elaboration:

Reviews of project safety status are held on a periodic and event-driven basis with appropriate levels of management, including independent reporting lines, to provide visibility into project safety risk exposure and appropriate corrective action.

Typically, these reviews include a summary of progress against safety criteria, the status of risk mitigation efforts, and any safety issues that require escalation.

Refer to the Project Monitoring and Control process area for more information about the review of project status and conducting progress reviews.

GG 3 Institutionalize a Defined Process

The process is institutionalized as a defined process.

GP 3.1 Establish a Defined Process

Establish and maintain the description of a defined safety engineering process.

GP 3.2 Collect Improvement Information

Collect work products, measures, measurement results, and improvement information derived from planning and performing the safety engineering process to support the future use and improvement of the organization's processes and process assets.

GG 4 Institutionalize a Quantitatively Managed Process

The process is institutionalized as a quantitatively managed process.

GP 4.1 Establish Quantitative Objectives for the Process

Establish and maintain quantitative objectives for the safety engineering process that address quality and process performance based on customer needs and business objectives.

GP 4.2 Stabilize Subprocess Performance

Stabilize the performance of one or more subprocesses to determine the ability of the safety engineering process to achieve the established quantitative quality and process performance objectives.

GG 5 Institutionalize an Optimizing Process

The process is institutionalized as an optimizing process.

GP 5.1 Ensure Continuous Process Improvement

Ensure continuous improvement of the safety engineering process in fulfilling the relevant business objectives of the organization.

GP 5.2 Correct Root Causes of Problems

Identify and correct the root causes of defects and other problems in the safety engineering process.

3 Usage Guidelines

This section describes guidelines for the use of +SAFE for appraisals and process improvement.

3.1 PROCESS APPRAISAL CONSIDERATIONS

+SAFE may be used with any of the appraisal methods applicable to CMMI. The safety extension has been written assuming appraisers have undertaken normal CMMI appraiser training, and the additional training module for +SAFE (available from DMO). +SAFE does not assume that appraisers will have a high level of knowledge in safety, but, as with the appraisal of any CMMI process area, the appraisal team must evaluate the level of expertise it has available and supplement its subject matter expertise if required.

Although +SAFE process extension presents the safety-related processes separate from CMMI-DEV, V1.2 process model, this approach is intended only to encourage a focus on safety during an appraisal. +SAFE process areas may be appraised as part of a broader CMMI–based appraisal, or independently, in the same way as other CMMI process areas.

3.1.1 Using +SAFE with CMMI

Where +SAFE process areas are appraised independently, as with other CMMI process areas, *CMMI Framework Interactions* on page 9 should be referenced to identify the implications for the appraisal and its results. The related process areas and cross references to CMMI process areas identified in each +SAFE process area highlight the benefits that may be gained if a +SAFE appraisal is performed as part of, or in addition to, a broader CMMI appraisal.

Table 4 summarizes the cross references (by +SAFE specific goal) to CMMI process areas.

CMMI process area	**Safety Management**			**Safety Engineering**				
	SG1	SG2	SG3	SG1	SG2	SG3	SG4	SG5
Causal Analysis and Resolution		√						
Configuration Management							√	
Decision Analysis and Resolution			√			√	√	
Measurement and Analysis		√						
Organizational Training	√							
Process and Product Quality Assurance							√	√
Project Monitoring and Control		√						
Project Planning	√							
Requirements Development	√			√		√	√	

Requirements Management	√		√				√	
Risk Management	√				√			
Supplier Agreement Management			√					
Technical Solution			√	√		√	√	
Validation							√	√
Verification			√				√	

Table 4: Summary of Cross References to CMMI Version 1.2

As with the standard components of CMMI, an organization's process descriptions and the organization of these descriptions reflect the processes used in its operations rather than the generic processes described in +SAFE. To simplify and shorten the appraisal, a mapping should be created prior to the appraisal that illustrates the relationships between the organization's safety processes and terminology, and the processes and terminology used in this extension. This mapping may also identify parts of the +SAFE process areas that may be tailored for a specific appraisal.

3.1.2 Tailoring for an Appraisal

Tailored appraisal results have a specific purpose, and are not reusable in other contexts. For example, the results of an appraisal that tailors out specific practices relating to management of external suppliers will have limited use for internal process improvement and for acquisition risk management, if the appraised organization uses external suppliers.

The three basic alternatives regarding safety that are generally seen in projects are as follows:

1. The product is safety-critical and safety activities are attempted.
2. The product is safety-critical or its safety characteristics are unknown and safety activities are not attempted.
3. The product is not safety-critical and safety activities are not attempted.

Ideally, a +SAFE appraisal should include samples of each alternative, since both safety critical and non-safety-critical projects influence the way an organization performs safety activities.

The decision to include a particular project as a sample in a +SAFE appraisal thus relies on a safety appraisal (by suitably qualified appraisers) of whether the project is safety critical. The determination of safety criticality is not a task that should be left to a +SAFE appraisal team on the basis of a brief understanding of the nature of a product. However, the +SAFE appraisal team should determine whether to appraise one or more projects that do not attempt any safety activities on the basis of the influence that the inclusion of these project will have on the overall appraisal of an organization to perform safety activities.

The following guidelines should be applied in determining which parts of the extension are applied to each project under appraisal. Some tailoring must be performed during the appraisal.

- If a project *may be* safety related, it should be appraised against the specific goals of the Safety Management process area, and against *SG1 Identify Hazards, Accidents, and Sources of Hazards* and *SG5 Support Safety Acceptance* of the Safety Engineering process area.
- If a project achieves SG1 and SG5 of the Safety Engineering process area, and thus determines that the project is safety-related, it should be appraised against *SG2 Analyze Hazards and Perform Risk Assessments* of the Safety Engineering process area.
- If a project achieves SG2 of the Safety Engineering process area, and thus determines that there are safety requirements, it should be appraised against *SG3 Define and Maintain Safety Requirements* and *SG4 Design for Safety* of the Safety Engineering process area.

Table 5 illustrates the process areas and goals that can be selected.

Project	**Safety Management**			**Safety Engineering**				
	SG1	SG2	SG3	SG1	SG2	SG3	SG4	SG5
Project is not safety-rated								
Project may be safety-rated 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 acceptable	√	√	√	√	√	√	√	√

Table 5: Sample Selection of Process Areas

The evaluation of the correctness of project decisions, including their classification as safety-critical or non-safety-critical, is not part of an appraisal against the +SAFE extension.

3.2 PROCESS IMPROVEMENT CONSIDERATIONS

The +SAFE extension provides guidance on how an organization may achieve capabilities in safety activities. As with other CMMI process areas, the guidance consists of the following:

- What the organization must achieve in performing its safety activities, in other words, the specific and generic goals of the process areas, which are the “required” parts
- How the organization might achieve these goals, in other words, the “expected” and “informative” parts, including components such as specific practices, generic practice elaborations, discipline amplifications, and subpractices
- The structure of the process areas using capability levels, in other words, the guidance on improvement priorities and dependencies

Besides the general guidance on systematic improvement found in the Process Management process area category, effective use of +SAFE as a guide for improvement of safety process capability relies on the

same prerequisites as improvement in other process areas, and these prerequisites are described in CMMI for Development, V1.2 and the IDEAL model [McFeeley 1996].

Although the +SAFE extension presents safety-related processes separate from the main CMMI process model, this presentation is not intended to discourage organizations from integrating safety processes with other processes. +SAFE makes frequent reference to the need for integrated use of +SAFE and other CMMI process areas.

Specific guidelines for using the safety process areas are as follows:

- +SAFE does not require the use of specific safety standards. If an organization has selected specific standards, or if these standards are imposed by contract, the +SAFE framework is intended to accommodate the methods and techniques of the standard, including, where applicable, alternative practices for the +SAFE specific and generic practices.
- Safety processes are highly dependent on the Support process areas, particularly Configuration Management, Process and Product Quality Assurance, and Decision Analysis and Resolution. To a lesser extent, safety processes are dependent on Measurement and Analysis and Causal Analysis and Resolution process areas. Effective implementation of these process areas is important for sustainable improvement in safety capability.
- Safety processes place a significant emphasis on the independence of verification and validation resources, and the need for independent lines of reporting for safety management and practitioners, particularly for issue escalation. Organizational independence may also be a factor in fostering functional expertise among safety practitioners.

Appendix Contact for Further Information

Australian Department of Defence, Defence Materiel Organisation maintains configuration of +SAFE. Please address comments, inquiries, and requests for further information to

DMO Head of Engineering

Electronic and Weapons Systems Division
Russell Offices
Department of Defence
CANBERRA ACT 2600

Approving Authority

Chief Executive Officer
Defence Materiel Organisation
Russell Offices R2-5-C131
CANBERRA ACT 2600

References/Bibliography

[ADoD 1998]
Australian Department of Defence. *The Procurement of Computer-Based Safety Critical Systems* (DEF [AUST] 5679). Defence Science and Technology Organisation, South Australia, August, 1998.

[ADoD 2000]
Australian Department of Defence. *Safety Process* Model Version 0.7 (CA38809-362), Defence Materiel Organisation, Canberra, September 1, 2000.

[ADoD 2001]
Australian Department of Defence. *+SAFE – A Safety Extension to CMMI v1.0* (CA38809-364). Defence Materiel Organisation, Canberra, December 19, 2001.

[CEI/IEC 2005]
International Electrotechnical Commission. *Safety of machinery—Functional Safety of Safety-Related Electrical, Electronic and Programmable Electronic Control Systems* (CEI IEC 62061). Geneva, Switzerland: International Electrotechnical Commission, 2005.

[McFeeley 1996]
McFeeley, Bob. *IDEAL: A User's Guide for Software Process Improvement* (CMU/SEI-96-HB-001). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1996. http://www.sei.cmu.edu/publications/documents/96.reports/96.hb.001.html.

[SEI 2006]
CMMI Product Development Team. *CMMI for Development, Version 1.2* (CMU/SEI-2006-TR-008, ESC-TR-2006-08). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, August 2006. http://www.sei.cmu.edu/publications/documents/06.reports/06tr008.html.

[SEI 2002]
CMMI Product Development Team. *CMMI for Systems Engineering/Software Engineering, Version 1.1 Continuous Representation* (CMU/SEI-2002-TR-003, ESC-TR-2002-003). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, December 2001. http://www.sei.cmu.edu/publications/documents/02.reports/02tr003.html.

[SEI 2001]
CMMI Product Development Team. *SCAMPI v1.1, Standard CMMI Appraisal Method for Process Improvement, Version 1.1: Method Definition Document* (CMU/SEI-2001-HB-001). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, December, 2001. http://www.sei.cmu.edu/publications/documents/06.reports/06hb002.html.

[UKMoD 2004]
United Kingdom Ministry of Defence. *Safety Management Requirements for Defence Systems, Part 1, Issue 3* (Def Stan 00-56). Glasgow, Scotland, UK: Defence Procurement Agency, U.K. Defence Standardization, December 14, 2004.
http://www.dstan.mod.uk/data/00/056/01000300.pdf.

[UKMoD 1997]
United Kingdom Ministry of Defence. *Safety Management Requirements for Defence Systems, Part 1, Issue 2* (Def Stan 00-56). Glasgow, Scotland, UK: Defence Procurement Agency, U.K. Defence Standardization, August 1, 1997.
http://www.dstan.mod.uk/data/00/055/01000200.pdf.

[USDoD 1993]
U.S. Department of Defense. *System Safety Program Requirements* (MIL-STD-882C). Washington, DC: United Stated Department of Defense, January 19, 1993.
http://www.weibull.com/mil_std/mil_std_882c.pdf.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	March 2007	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
+SAFE, V1.2: A Safety Extension to CMMI Version 1.2	FA8721-05-C-0003

6. AUTHOR(S)

Defence Materiel Organisation, Australian Department of Defence

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2007-TN-006

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	CMU/SEI-2007-TN-006

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

+SAFE is an extension to CMMI® for Development (CMMI-DEV) that covers safety management and safety engineering. +SAFE supplements CMMI-DEV with two additional process areas that provide a basis for appraising or improving an organization's processes for providing safety-critical products. Developing such products requires specialized processes, skills, and experience. +SAFE is designed to identify safety strengths and weaknesses and to address identified weaknesses early in the acquisition process.

+SAFE was designed to reduce the dependence of CMMI appraisers on safety domain expertise. This extension was developed for standalone use. It is not intended to be embedded in a CMMI model document, nor does it rely on any specific safety standards. However, there are intentional overlaps with CMMI model content and some safety standards.

Since +SAFE is an extension of CMMI, it adopts the same assumptions, model structure, conventions, and terminology as CMMI and is affected by the general process-area and capability-level interactions inherent in CMMI. This technical report describes the +SAFE extension and how to use it to appraise an organization's capability in developing, sustaining, maintaining, and managing safety-critical products.

14. SUBJECT TERMS	15. NUMBER OF PAGES
safety management, safety engineering, CMMI, safety	66

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18 298-102