
**Safety and Security Extensions
for
Integrated Capability Maturity Models**

**Linda Ibrahim
Joe Jarzombek
Matt Ashford
Roger Bate
Paul Croll
Mary Horn
Larry LaBruyere
Curt Wells**

**and the Members of the
Safety and Security Extensions Project Team**

September 2004

Published by the United States Federal Aviation Administration, 2004.

This work has been developed in part by adapting portions of the following documents.

Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 2.1, Common Criteria Project Sponsoring Organizations, 1999.

The Common Criteria (CC) is freely available for public use. Copyright information in the document exists to protect the integrity of the CC and to prevent the contents from being copyrighted by another individual or organization.

Defence Standard 00-56, Safety Management Requirements for Defence Systems, Ministry of Defence, United Kingdom, December 1996.

This is public domain material.

IEC 61508, Functional Safety of electrical/electronic/programmable electronic safety-related systems, International Electrotechnical Commission, 1997.

This document is copyright protected and referenced only by paragraph numbers and titles in the mapping tables appendix. Interested readers should obtain a copy of this document for additional information on the details.

ISO/IEC 17799:2000(E): Information technology – Code of practice for information security management, International Organization for Standardization, First edition 2000-12-01.

This document is copyright protected and referenced only by paragraph numbers and titles in the mapping tables appendix. Interested readers should obtain a copy of this document for additional information on the details.

Military Standard System Safety Program Requirements, MIL-STD-882C, United States Department of Defense, January 1993.

This is public domain material.

Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology, Special Publication 800-30, 2001.

This is public domain material.

Standard Practice for System Safety, MIL-STD-882D, United States Department of Defense, February 2000.

This is public domain material.

Systems Security Engineering Capability Maturity Model®, *SSE-CMM®*, Model Description Document, Version 3.0, June 15, 2003. (*ISO/IEC 21827*)

Copyright © 1999

Systems Security Engineering Capability Maturity Model (SSE-CMM) Project

Permission to reproduce this product and to prepare derivative works from this product is granted royaltyfree, provided the copyright is included with all reproductions and derivative works. This document includes excerpts from “A Systems Engineering Capability Maturity Model, Version 1.1,” CMU/SEI-95-MM-003, published in November 1995.

® CMM and Capability Maturity Model are Service Marks of Carnegie Mellon University NOT-FORPROFIT CORPORATION PENNSYLVANIA 5000 Forbes Avenue Pittsburgh PENNSYLVANIA 15213

Excerpts from the following documents are included in this work.

The Federal Aviation Administration Integrated Capability Maturity Model[®] (FAA-iCMM[®]), Version 2.0, Federal Aviation Administration, September 2001.

This is public domain material.

Capability Maturity Model[®] Integration (CMMI[®]), Version 1.1 - CMMI for Systems Engineering, Software Engineering, Integrated Product and Process Development, and Supplier Sourcing (CMMI-SE/SW/PPD/SS, v1.1) Continuous Representation, CMU/SEI-2002-TR-011, ESC-TR-2002-011, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, March 2002.

Copyright 2002 by Carnegie Mellon University

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

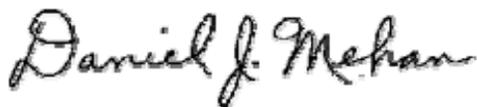
[®] Capability Maturity Model, CMM, CMM Integration, CMMI, and SCAMPI are registered trademarks in the U.S. Patent and Trademark Office.

FOREWORD

The Federal Aviation Administration (FAA) is recognized throughout the federal government, as well as nationally and internationally, as a leader in process improvement. The FAA was the first major organization to develop and use an integrated model as an effective and efficient framework to guide process improvement efforts. The FAA's integrated Capability Maturity Model (FAA-iCMM) has undergone two major releases since its inception in 1997. The current Version 2.0 has been in use since September 2001 and has helped many organizations both within and outside of the FAA to achieve significant improvements in their processes and the accompanying performance benefits such as enhanced productivity, higher quality, better control of acquisitions, and better communications and teamwork.

The ability to sustain and build upon improvements that have already been realized requires a strong commitment to continuous process improvement. Since the needs of the FAA's customers and employees are constantly changing, as are the technology and business environments in which the FAA must operate, it is essential that our business and technical processes also change. The FAA's strong commitment to safety requires that we constantly look to improvements that will enhance an already unprecedented safety record. We also need to refine and implement our "android" cyber defense model to protect the National Airspace System and other cyber assets from deliberate or unintentional harm through disruption or corruption of our critical data flow. It is with these safety and security objectives in mind that we have developed the Safety and Security Extensions to the FAA-iCMM that are contained in this document.

The safety and security best practices that are reflected herein were developed under joint sponsorship by organizations within the Department of Defense and the FAA. The team that developed this document included over 30 experts from across government, industry, and the international community. The best practices that are included are drawn from recognized standards and guidelines that are used by safety and security professionals in the conduct of their work activities. I am not aware of any other product that has been developed to date that brings together in one body the best practices of these two critical disciplines and also integrates them with other best practices for systems engineering and software engineering. In addition to codifying these best practices in one document, an additional benefit of bringing together the best practices of these two disciplines is that it should result in greater collaboration and synergy between the safety and security engineering processes and the professionals who perform them. I am very proud of the team that developed this document, and I am looking forward to seeing the benefits of their work as these best practices are applied within the FAA.



Daniel J. Mehan, Ph.D.
FAA Chief Information Officer and
Assistant Administrator for Information Services

MESSAGE FROM THE PROJECT MANAGERS

Today the need for safe and secure products and services is widely recognized. To be relevant in the global environment, capability maturity models that support process improvement need to include standards-based safety and security practices. Both the CMMI and iCMM provide process improvement frameworks in which safety and security activities can take place. However, some practices specific to safety and security are not addressed in these models, nor is there sufficient guidance for interpreting the models' practices in a safety and security context.

The FAA approved a project to address both safety and security in the iCMM, and the CMMI Steering Group and CMMI user community have discussed addressing safety and security. In light of similar needs to enhance both models, organizations in the FAA, DoD, and other agencies collaborated with industry on developing safety and security extensions to both the iCMM and the CMMI with the intent being that common content could be included in both models. This document reflects the attempt to harmonize safety and security goals, practices, and terminology. It is intended to provide an efficient and effective mechanism that synthesizes and harmonizes best practices from eight safety and security standards and provides a construct with guidance to facilitate their use as expected practices within the context of the existing models. This makes safety and security practices explicitly visible, improvable, and appraisable.

With the release of this document, the FAA has incorporated the use of these safety and security extensions for all users of the iCMM. While these practices can be used with the CMMI, as of the publication date of this report, there is no formal endorsement or requirement for use of safety and security extensions with the CMMI. Although no formal decision has been made by the CMMI project at this time regarding incorporation of safety and security into the CMMI, formal change requests to the CMMI project have been provided by our safety and security project team to address these extensions. As always, implementing organizations should adopt those practices and methods that best help them achieve mission and business objectives.

This project has sought harmonization on several fronts, and we have been delighted to work over the past two years with such a distinguished team of experts and reviewers representing many stakeholder perspectives. Our hope is that the resulting body of knowledge will be broadly applied to support process improvement that includes strong consideration for safety and security.

Linda and Joe

Linda Ibrahim, PhD
Chief Engineer for Process Improvement
Office of the Assistant Administrator for
Information Services and Chief Information Officer
Federal Aviation Administration
Email: linda.ibrahim@faa.gov

Joe Jarzombek, PMP
Deputy Director for Software Assurance
Information Assurance Directorate
Office of Assistant Secretary of Defense
(Networks and Information Integration)
Email: joe.jarzombek@osd.mil

Table of Contents

Foreword	i
Message from the Project Managers	ii
Introduction	1
Project Overview	1
Product Overview	6
Safety and Security Application Area	13
Application Area Summary	13
AP 01.01 Ensure Safety and Security Competency	17
AP 01.02 Establish Qualified Work Environment	19
AP 01.03 Ensure Integrity of Safety and Security Information	21
AP 01.04 Monitor Operations and Report Incidents	23
AP 01.05 Ensure Business Continuity	25
AP 01.06 Identify Safety and Security Risks	27
AP 01.07 Analyze and Prioritize Risks	29
AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan	32
AP 01.09 Determine Regulatory Requirements, Laws and Standards	34
AP 01.10 Develop and Deploy Safe and Secure Products and Services	36
AP 01.11 Objectively Evaluate Products	41
AP 01.12 Establish Safety and Security Assurance Arguments	44
AP 01.13 Establish Independent Safety and Security Reporting	47
AP 01.14 Establish a Safety and Security Plan	49
AP 01.15 Select and Manage Suppliers, Products and Services	52
AP 01.16 Monitor and Control Activities and Products	55
Glossary	59
Work Environment Process Area	61
Process Area Summary	61
Practice 01 Determine Work Environment Needs	63
Practice 02 Establish Work Environment Standards	65
Practice 03 Establish Work Environment	66
Practice 04 Maintain the Qualification of Components	68
Practice 05 Maintain the Qualification of Personnel	69
Practice 06 Maintain Technology Awareness	70
Practice 07 Ensure Work Environment Continuity	71
Bibliography and References	72
Appendix A: Project History and Approach	75
Appendix B: Mapping Tables	78
Table 1: Safety and Security Application Practices Mapped to Sources	79
Table 2: Safety Sources Mapped to Safety and Security Application Practices	102
Table 3: Security Sources Mapped to Safety and Security Application Practices	118
Table 4: Work Environment Practices Mapped to Sources	134

Introduction

This section introduces this report by providing information on the project that created it, along with an overview of major project outputs. First, the Safety and Security Extensions project is described including its participants and the general approach used by the project team. Then brief overview information is provided for each major product component including the Safety and Security Application Area, the Work Environment Process Area, and mapping tables. Since an application area is a new concept introduced by this project, the product overview includes a series of questions and answers regarding application area structure and use.

Project Overview

What are the Project Objectives?

Organizations within the U.S. Federal Aviation Administration (FAA) and the U.S. Department of Defense (DoD) sponsored this project with the objective of identifying best safety and security practices for process improvement and appraisal use in combination with the two integrated capability maturity models:

- FAA integrated Capability Maturity Model[®] (FAA-iCMM[®] or iCMM) version 2.0 (available at www.faa.gov/ipg), and
- Capability Maturity Model Integration[®] for Systems Engineering, Software Engineering, Integrated Product and Process Development, and Supplier Sourcing (CMMI[®] - SE/SW/IPPD/SS or CMMI) version 1.1 (available at www.sei.cmu.edu).

The safety and security practices produced from this project were required to be:

- based on widely recognized safety and security standards and sources, and
- harmonized to represent the commonality among the safety and security disciplines, where possible.

Why Is It Important?

Safety and security are critical to the DoD and the FAA, as well as to many other government and industry organizations. Both the CMMI and the iCMM provide process improvement frameworks in which safety and security activities can take place. Yet some practices specific to safety and security are not necessarily addressed in these models, nor is there sufficient guidance for interpreting the models' practices in a safety and security context. The FAA approved a project to address both safety and security in the iCMM, and the CMMI Steering Group had discussed addressing safety and security. In light of similar needs to enhance both models, the FAA and the DoD organizations decided to collaborate on developing safety and security extensions to both the iCMM and the CMMI, the intent being that common content could be included in both models. Safety and security are closely coupled by objectives, methods, tools, and techniques, but separated to some extent by terminology. This document has attempted to harmonize safety and security goals, practices, and terminology in order to provide an integrated approach for assuring safety and security.

Who Will Use This Work?

It is expected that these practices will be utilized for process improvement in several contexts: strategically to support enterprise-wide safety and security work; in any program/organization that deals with safety and security assurance of products and services at any lifecycle phase; by those groups responsible for a safe and secure work environment; and by acquisition programs in evaluating the capability of suppliers to deliver safe and secure products and services.

Introduction

Who Has Been Involved?

This document reflects the shared work of many organizations and people. The project was co-managed by the FAA Chief Engineer for Process Improvement and the Deputy Director for Software Assurance in DoD, with broad participation from government and industry and the international community. The project team comprised over 30 expert participants from FAA, DoD, Army, Navy, Air Force, National Aeronautics and Space Administration, Department of Energy, Defence Materiel Organization (Australia), Defense Contract Management Agency, Software Engineering Institute, Northrop Grumman, Lockheed Martin, Computer Sciences Corporation, Harris Corporation, I-Metrics, and Praxis Critical Systems Ltd (U.K.). In addition, many individuals and organizations participated as reviewers, and in safety and security pilot appraisals. Without the dedication of all these expert volunteers, this project could not have been launched or completed. These participants are acknowledged for their very valuable contributions and are listed below.

Members of the Safety and Security Extensions Project Team

Sponsors	Gregg Dvorak Joe Jarzombek Arthur Pyster (Emeritus sponsor)	U.S. Federal Aviation Administration U.S. Office of Secretary of Defense Science Applications International Corporation (previously with U.S. Federal Aviation Administration)
Project Managers	Linda Ibrahim Joe Jarzombek	U.S. Federal Aviation Administration U.S. Office of Secretary of Defense
Safety Team	Matt Ashford (Lead) Brenda Coblenz Ray Conrad Janet Gill Lisa Ming Ron Stroup (Lead) Ray C. Terry Martha Wetherholt	Defence Materiel Organisation (Australia) U.S. Department of Energy Lockheed Martin Transportation and Security Solutions U.S. Navy, NAVAIR Software System Safety Defense Contract Management Agency U.S. Federal Aviation Administration U.S. Navy, NAVAIR Systems Safety Division National Aeronautics and Space Administration
Security Team	Tim Courington (Lead) Sartaj Dhami Ronda Henning (Lead) Mary Horn Tom Jackson Feisal Keblawi Victor Kemens Martha J. Leonette Gerald Miller Raju B. Patel Hal Pierson Douglas Roseboro Marty Simmons Sandra Stuart	Northrop Grumman Information Technology Northrop Grumman Information Technology Harris Corporation U.S. Federal Aviation Administration Lockheed Martin Transportation and Security Solutions U.S. Federal Aviation Administration U.S. Federal Aviation Administration U.S. Federal Aviation Administration Northrop Grumman Information Technology U.S. Air Force, Wright Patterson Air Force Base U.S. Federal Aviation Administration U.S. Federal Aviation Administration Lockheed Martin Integrated Systems and Solutions U.S. Federal Aviation Administration

Introduction

Members of the Safety and Security Extensions Project Team (continued)

Harmonization Team	David Cooper Paul Croll (Lead) Joe Jarzombek Scott VanBuren	Praxis Critical Systems Ltd (U.K.) Computer Sciences Corporation U.S. Office of Secretary of Defense U.S. Federal Aviation Administration
Model Alignment Team	Dennis Ahern Roger Bate Linda Ibrahim (Lead) Wayne Sherer Curt Wells	Northrop Grumman Electronic Systems Software Engineering Institute U.S. Federal Aviation Administration U.S. Army, Picatinny Arsenal I-Metrics LLC
Pilot Appraisal Team	Brenda Coblentz Ray Conrad Linda Ibrahim Larry LaBruyere (Lead) Raju B. Patel Curt Wells	U.S. Department of Energy Lockheed Martin Transportation and Security Solutions U.S. Federal Aviation Administration Northrop Grumman Information Technology U.S. Air Force, Wright Patterson Air Force Base I-Metrics LLC

Reviewers and Pilot Appraisal Participants

Julia Allen	Software Engineering Institute
Shonnag Allison	Ministry of Defence (U.K.)
Jim Armstrong	Software Productivity Consortium
Roger Bate	Software Engineering Institute
William Bath	The Boeing Company
Christie Batten	BAE Systems
Ilene Becker	Booz Allen Hamilton
Pauly Bernard	THALES Research and Technologies (France)
Diane Bloodworth	BIT (Diversified International Sciences Corporation)
Barbara J. Brown	U.S. Federal Aviation Administration
Klaus Bruegge	Q-Labs (Germany)
Jim Chelini	Verocel
Henry Christian	THALES Research and Technologies (France)
Brenda Coblentz	U.S. Department of Energy
Roger Cooley	U.S. Federal Aviation Administration
David Cooper	Praxis Critical Systems Ltd (U.K.)
Tim Courington	Northrop Grumman
Sartaj Dhami	Northrop Grumman
Matt Dombrowski	Booz Allen Hamilton
Bradley Doohan	Defence Materiel Organization (Australia)
Georgette Dubain	THALES Research and Technologies (France)
Siegfried Eisinger	DNV (Det Norske Veritas) Consulting (Germany)
Dennis Emerick	U.S. Federal Aviation Administration
Elaine Fedchak	ITT Industries
Donald Firesmith	Software Engineering Institute
Don Fitts	U.S. Federal Aviation Administration
Janet Gill	U.S. Navy, NAVAIR
Natalie Givans	Booz Allen Hamilton

Introduction

Reviewers and Pilot Appraisal Participants (continued)

M. Griffith	Programmatix
C. Hagaman	Programmatix
Mikael Hagerby	DNV (Det Norske Veritas) Consulting (Germany)
Anthony Hall	Independent (U.K.)
Stuart D. Hann	The Boeing Company
Ronda Henning	Harris Corporation
Welsey Higaki	SYMANTEC
Marlo Higgins	Dynamic Security Concepts, Inc. (DSCI)
John Hopkinson	International Systems Security Engineering Association
Mary Horn	U.S. Federal Aviation Administration
Charles C. Howell	The MITRE Corporation
Linda Ibrahim	U.S. Federal Aviation Administration
Scott Jackson	The Boeing Company
Kenneth Johnson	Programmatix
Larry LaBruyere	Northrop Grumman
Karen LaFond	U.S. Army TARDEC
Clive Lee	ERA Technology (U.K.)
John Leggett	Jacobs Sverdrup
Robert T. Lentz	General Dynamics Land Systems
Peter Lindsay	University of Queensland (Australia)
Frank Maguire	Wright Patterson Air Force Base
Robert Manners	Apptis
Tom McGibbon	ITT Industries
Kris McKenzie	U.S. Federal Aviation Administration
Patti Dee McNeill	U.S. Federal Aviation Administration
Nancy R. Mead	Software Engineering Institute
Julie Mehan	Booz Allen Hamilton
James W. Moore	The MITRE Corporation
Keith Morrell	Savanna River Site, U.S. Department of Energy
Michele Moss	Booz Allen Hamilton
John Murdoch	University of York (U.K.)
Tom Murphy	BAE Systems
Networked Systems Survivability Program	Software Engineering Institute
Thomas O'Keefe	U.S. Federal Aviation Administration
Kristin Parker	Booz Allen Hamilton
Bernard Pauly	Thales (France)
William Peterson	Software Engineering Institute
William R. Porter	U.S. Federal Aviation Administration
Philippe Robert	IsoScope (France)
Neil Robinson	University of Queensland (Australia)
George Romanski	Verocel
Glenn Rosander	Booz Allen Hamilton
SafSec Project	SafSec (U.K.)
Joseph M. Saur	Georgia Tech Research Institute
Joseph Schanne	U.S. Federal Aviation Administration
Horst Schubotz	DNV (Det Norske Veritas) Consulting (Germany)
Roger Shaw	ERA Technology (U.K.)
Robert Small	Software Productivity Consortium

Introduction

Reviewers and Pilot Appraisal Participants (continued)

Dave Smith	U.S. Federal Aviation Administration
Debra Sparkman	U.S. Department of Energy
Ronald L. Stroup	U.S. Federal Aviation Administration
Sandra Stuart	U.S. Federal Aviation Administration
Mark Sutters	Ministry of Defence (U.K.)
Joan Tarbell	Booz Allen Hamilton
William Teppig	BAE Systems
Scott VanBuren	U.S. Federal Aviation Administration
Michael Virga	U.S. Federal Aviation Administration
John Weiler	Interoperability Clearinghouse
Curt Wells	I-metrics LLC
Joan S. Weszka	Lockheed Martin Mission Systems
Diane Wilson	U.S. Federal Aviation Administration
Harold G. (Hal) Wilson	Northrup Grumman Mission Systems
Carol Woody	Software Engineering Institute
Karen Zimmie	Booz Allen Hamilton

What was the Project Approach?

The following summarizes selected features of the project approach. Further details on project approach and history are provided in Appendix A.

Selection of Source Material

Experts within the respective communities of practice selected source documents for safety and for security. Source documents are the documents from which the safety and security practices are derived. Mapping of safety and security practices to source practices is required, and coverage of source documents, at an appropriate level of detail, is demonstrated.

Synthesis and Harmonization of Practices and Initial Community Review

The safety expert team and the security expert team analyzed their respective source documents and synthesized practices from source material. Then safety practices and security practices were harmonized into a single set of practices, which was distributed for broad community review.

Analysis in Relation to the Reference Models

The harmonized practices (revised based on initial community review) were analyzed in relation to content of the iCMM and CMMI reference models. Based on this analysis, a new construct was proposed for addressing the safety and security practices. This construct is called an Application Area (explained below). Additionally, the team proposed a new Work Environment Process Area to address safety and security requirements that were not adequately covered in either reference model and to address a broader, generic need for guidance to improve the work environment.

Further Community Review and Validation via Pilot Appraisals

Pilot appraisals were carried out in several different organizational settings and the Safety and Security Application Area and Work Environment Process Area were distributed for further broad community reviews. The team addressed comments received, along with lessons learned from pilot appraisals, and incorporated them into this final product.

Introduction

Product Overview

Source Material

The following source standards were selected and endorsed by experts from safety and security communities of practice. They were used to develop the Safety and Security Application Area and the Work Environment Process Area presented in this report.

For safety:

- *MIL-STD-882C*: System Safety Program Requirements, Military Standard, January 1993.
- *MIL-STD-882D*: Standard Practice for System Safety, Department of Defense, February 2000.
- *IEC 61508*: Functional Safety of Electrical/ Electronic/ Programmable Electronic Systems, International Electrotechnical Commission, 1997.
- *DEF STAN 00-56*: Safety Management Requirements for Defence Systems, Ministry of Defence, December 1996.

For security:

- *ISO/IEC 17799*: Information Technology - Code of practice for information security management, International Organization for Standardization, 2000.
- *ISO/IEC 15408*: Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, v2.1, Common Criteria Project Sponsoring Organizations, 1999.
- *ISO/IEC 21827*: Systems Security Engineering Capability Maturity Model (SSE-CMM), v3.0, SSE-CMM Project, 2003.
- *NIST 800-30*: Risk Management Guide for Information Technology Systems, Special Publication 800-30, National Institute of Standards and Technology, 2001.

Safety and Security Application Area – Overview

The Safety and Security application area (AA) identifies standards-based application practices (APs) expected to be used as criteria in guiding process improvement and in appraising an organization's capabilities for providing safe and secure products and services. These application practices are used in conjunction with existing practices in the CMMI and/or the iCMM.

The purpose of the Safety and Security application area is to establish and maintain a safety and security capability, define and manage requirements based on risks attributable to threats, hazards, and vulnerabilities, and assure that products and services are safe and secure throughout their life cycle. Goals and practices of the application area are:

Goal 1. An infrastructure for safety and security is established and maintained.

- AP 01.01 Ensure Safety and Security Competency
- AP 01.02 Establish Qualified Work Environment
- AP 01.03 Ensure Integrity of Safety and Security Information
- AP 01.04 Monitor Operations and Report Incidents
- AP 01.05 Ensure Business Continuity

Goal 2. Safety and security risks are identified and managed.

- AP 01.06 Identify Safety and Security Risks
- AP 01.07 Analyze and Prioritize Risks
- AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan

Introduction

Goal 3. Safety and security requirements are satisfied.

AP 01.09	Determine Regulatory Requirements, Laws, and Standards
AP 01.10	Develop and Deploy Safe and Secure Products and Services
AP 01.11	Objectively Evaluate Products
AP 01.12	Establish Safety and Security Assurance Arguments

Goal 4. Activities and products are managed to achieve safety and security requirements and objectives.

AP 01.13	Establish Independent Safety and Security Reporting
AP 01.14	Establish a Safety and Security Plan
AP 01.15	Select and Manage Suppliers, Products, and Services
AP 01.16	Monitor and Control Activities and Products

Each application practice is implemented by performing specifically identified *implementing practices* from the reference models. These implementing practices are performed in accordance with the guidance provided with each application practice and in such a way as to achieve the goals of the application area. As with process areas in the iCMM and CMMI, generic practices are applied to guide process improvement and to support appraisal of safety and security process capability.

Work Environment Process Area - Overview

The Work Environment process area provides details of what is to be accomplished in AP 01.02 Establish Qualified Work Environment. Note that this process area is not specific to safety and security, and it could be used for other applications or disciplines. As such, its practices are derived from a variety of other sources in addition to the safety and security source standards (see Appendix B). “Work Environment” would be added as a new process area to the iCMM and the CMMI.

The purpose of the Work Environment process area is to ensure that people have infrastructure and working procedures to perform their work effectively. Work Environment goal and practices are:

Goal. A work environment that meets stakeholder needs and requirements is established and maintained.

Practice 01	Determine Work Environment Needs
Practice 02	Establish Work Environment Standards
Practice 03	Establish Work Environment
Practice 04	Maintain the Qualification of Components
Practice 05	Maintain the Qualification of Personnel
Practice 06	Maintain Technology Awareness
Practice 07	Ensure Work Environment Continuity

Mapping Table Appendix – Overview

The mapping table appendix (Appendix B) contains maps showing the sources of each application practice and each work environment practice. These tables show the standards used for deriving each practice and also indicate where users can find more detail and additional guidance regarding each practice. A map is also provided for each safety and security source standard demonstrating where each clause/practice/activity is mapped to an application practice(s), at an appropriate level of detail. For the work environment mapping table, additional sources (beyond the safety and security standards) are also indicated. All sources and references are listed in the Bibliography and References section of this document.

Introduction

Application Area – Description and Considerations

Since the application area construct is a new idea generated by this project, this section is devoted to providing more information about an application area in general and the safety and security application area in particular.

What is an application area?

An application area (AA) is a construct intended for use with both the iCMM and the CMMI reference models. An application area groups together related application practices (APs) that are considered essential for achieving the requisite outcomes particular to the application or discipline. The application practices are implemented by performing practices that are already in process areas of the reference models, with explicit guidance derived from source standards for the respective disciplines of application. Thus, application areas provide a guide or overlay for identifying which selected process areas and practices in a reference model need to be implemented to address the purpose of the application area. The application practices provide additional guidance for ways that the practices in the reference model might be implemented in the particular context of the application.

Why are only safety and security addressed?

An application area could be developed for another discipline, and indeed others are being considered to help in focusing appraisals and process improvement in the context of a specific discipline. For now, safety and security have been considered because of their importance in government and industry. Moreover, this focus has enabled a better harmonization of practices between the two disciplines.

How would organizations or individuals use the safety and security application area?

It is expected that this application area will be used for process improvement and benchmarking in several contexts: strategically, to support enterprise-wide safety and security work; in any program/organization that deals with safety and security assurance of products and services at any phase of the life cycle; in the work environment, by those groups responsible for ensuring people have tools and facilities needed for safe and secure development, operation and maintenance of products and services; and by acquisition programs in evaluating the capability of suppliers to deliver safe and secure products and services. The safety and security application practices described are harmonized since so many activities are common to both safety and security. However, this application area can be used in the context chosen by the organization, which may be to improve and appraise security or safety or both safety and security.

How does this safety and security application area relate to safety and security standards?

The application practices in the safety and security application area are the harmonized safety and security practices that were synthesized from the source standards identified by subject matter experts in the safety and security communities of practice. The source standards are a selection of safety and security standards in community-wide use, and those standards with industry-specific guidance would be accommodated via the application practice AP 01.09 Determine Regulatory Requirements, Laws, and Standards (see further discussion of standards below).

Introduction

Why aren't these harmonized practices being proposed as CMMI "amplifications" or iCMM "notes" in relation to the existing practices?

In order to make the practice of safety and security in organizations explicitly improvable and appraisable, the safety and security application practices need to be structured as "expected" practices. The informative nature of amplifications and notes does not meet this need. Simply adding informative material to existing practices in the reference models provides no assurance that safety and security would be included in process improvement or appraisal of capabilities. The AA also provides direct visibility, in a single location, to those practices needed for safety and security.

Why are these harmonized safety and security application practices being proposed as an application area rather than a new process area?

The harmonized safety and security application practices are already addressed in a more general fashion in reference model existing practices, without sufficient explicit consideration for safety or security concerns. To introduce new practices that are already addressed, though generally, in the reference models would be confusing and would be largely redundant. Also, the harmonized application practices do not offer the breadth and depth of reference model practices regarding practice implementation details.

How is an application area constructed?

An application area is similar to a process area since it contains a purpose statement, goals (application goals), and expected practices (application practices). Application goals reflect outcomes to be achieved for the application area to be considered successfully implemented. They are useful in establishing process improvement objectives and are required components for appraisal purposes. Application practices are mapped to goals, and they are the activities that, when performed, are expected to result in achievement of those goals. Application practices are implemented, however, by performing the indicated "implementing practices" in the reference models, as interpreted in the particular application context described by the information provided for each application practice. These application practices, as elaborated by their associated implementing practices or acceptable alternatives to them, are expected to be present in the planned and implemented processes of the organization before application goals can be considered satisfied. Typical work products are also provided for each application practice and these are generically named examples of what outputs could result from carrying out this practice. Lastly there are notes for each application practice which provide further information and elaboration including conceptual examples, potential techniques, methods, guidance, etc

How does an application area relate to the new CMMI architecture?

The application area concept is compatible with and supportive of the new CMMI architecture. This is how it works. An application area provides named groups of amplifications, elaborations, and additions by means of its application practices (named Safety and Security for example). It also denotes the components that would form the primitive model, and the placements for the named groups in that primitive model, by means of the way that application practices identify their implementing practices and associated process areas, for each application practice. (Those implementing practices and process areas become the primitive model.) By generating a releasable CMMI model from the primitive model and its named additions, amplifications, and elaborations, that CMMI model would then reflect the application area. Releasable CMMI models would identify target stagings and maturity levels, but such staging would not be provided in an application area. The application area is only used for determining AA capability levels, not maturity levels.

Introduction

How does an application area relate to the iCMM architecture?

The iCMM is structured to offer flexibility for organizations to pursue process improvement via capability levels in selected process areas or via maturity levels in sets of process areas. This architecture is called a “continuous with staging” representation. An application area simply provides a guide to the process areas that need to be implemented in the context of the application area. Since the iCMM approach has always been to provide a single model, for selective use by the implementing organizations, the application area construct does not disrupt this idea. Application areas provide guidance, for process improvement and appraisal purposes, regarding ways the existing process areas in the iCMM model can be used in the context of the application area. An application area, like a process area, can be at any capability level. However, an application area is not staged at a particular maturity level.

How is an application area appraised?

The Standard CMMI Appraisal Methodology for Process Improvement (SCAMPI[®]), the FAA iCMM Appraisal Method (FAM), and other Appraisal Requirements for CMMI (ARC) Class A appraisal methods can be applied to application areas by employing the generic practices of either the iCMM or the CMMI. Thus an application area could be appraised at any capability level. The goals of the application area would be used in appraisal, and the practices mapped to those goals would be the implementation practices in the reference models, considered in the context of the guidance provided in the application area. In an application area stand-alone appraisal, only the application area goals (and not process area goals of the reference models) need to be considered, if that is the desired scope. Of course ARC Class B and C appraisals could also be used to gain an understanding of process capabilities relative to safety and security.

How do maturity levels relate to application areas?

Application areas may be appraised concurrently with other appraisal scopes, including a maturity level appraisal. Application area ratings, however, do not affect maturity levels. While much of the evidence presented would be applicable to both aspects of an appraisal, ratings would be assigned independently.

How are application practices used in an appraisal?

Each application practice has associated implementing practices, identified in this way: "This application practice is implemented by performing the following practices in such a way as to <application practice statement>". Therefore, in order to satisfy the application practice, all of the reference model (CMMI/iCMM) implementing practices should, in fact, be implemented (fully or largely) so as to address the specific context of the application practice. The focus should be that application practices are performed and application goals are achieved. For example, in appraising application practice AP 01.01 Ensure Safety and Security Competency, the implementing practices regarding training would be examined to ascertain that safety and security competency is ensured.

What happens if some application area activities are outside the scope of my organizational unit?

This determination should be made in the appraisal-planning phase that would clearly identify who is responsible for those activities and why it is outside the scope of the organization. If such an argument is accepted, those activities would not be appraised and would not affect the appraisal results. This information should also be clearly documented in the Appraisal Disclosure Statement. Note that application area activities are critical to safety and security, and their omission could present significant risk. Thus, the organizational unit should attempt to ensure that the unit

Introduction

responsible carries out these activities. Note also that appraisals could include multiple organizational units if the responsibilities for safety and/or security are dispersed among them.

What if I only want to look at one aspect (safety or security, but not both) in an appraisal?

When applying the safety and security application area to your organization, the scope (safety, security, or both) should be clearly identified in the appraisal-planning phase and in the Appraisal Disclosure Statement. The practices should be used to focus on that particular aspect of the organizational function (e.g., if a configuration management practice is appraised it should focus on the configuration management of the safety and/or security items).

How does use of the safety and security application area relate to system/product certification/ accreditation and acceptance testing?

The safety and security application area complements (but does not replace) certification/ accreditation and acceptance testing of systems and products. If requisite application practices are implemented, they should contribute to the delivery of safe and secure products and services, and their artifacts should more readily support achievement of certification/accreditation expected outcomes.

How does the safety and security application area relate to other standards?

- The National Institute of Standards and Technology (NIST) implements guidelines responsive to Public Law 104-106 (Clinger-Cohen Act of 1996) and OMB Circular A-130. Other related standards and publications have not been explicitly referenced in this application area. However, as written, this application area lends itself to full support of the NIST 800-series publications that provide an organization with further tools for bolstering their security processes. NIST issued the October 2003 draft of “Recommended Security Controls For Federal Information Systems,” NIST Special Publication 800-53, which details controls the government will require in 2005 and is expected to influence controls to be used by other governments and business (csrc.nist.gov/publications/drafts.html). Security controls are the management, operational, and technical safeguards and countermeasures prescribed for a computer system that, taken together, adequately protect the confidentiality, integrity, and availability of a system and its information. Management safeguards range from risk assessment to security planning, operational safeguards include factors such as personnel security and hardware and software maintenance, and technical safeguards include audit trails and communications protection.
- The Federal Information Security Management Act contains guidelines about establishing security standards and requirements for information and information systems, including business process improvement and states “Federal agencies should follow NIST guidelines, if applicable and whenever feasible.”
- ISO/IEC 15026:1997, System and Software Integrity Levels, was used by the Harmonization Team as a basis for harmonizing terminology and concepts between the safety and security communities. ISO/IEC JTC1/SC7 WG9 is the international working group that produced this standard and includes members of both communities. WG9 has recently redefined its terms of reference to include *development of standards and technical reports for system and software assurance. System and software assurance addresses management of risk and assurance of safety, security, and dependability within the context of system and software life cycles.* WG9 is also in the process of revising 15026 and will continue to collaborate in the development and evolution of this application area.

Introduction

- Useful discussions have taken place with the U.K. Ministry of Defence (MoD) and Praxis Critical Systems regarding the SafSec Project, a research study on Integrating Safety and Security for Integrated Modular Avionics, funded by the U.K. MoD. The synergy with the SafSec project lies in the similar aims of combining safety and security for improved effectiveness.

How does the safety and security application area relate to industry-specific regulatory guidance? Standards and laws that provide more detailed industry-specific guidance for safety and security would be addressed via the application practice AP 01.09 Determine Regulatory Requirements, Laws and Standards. For example, RTCA DO-178B “Software Considerations in Airborne Systems and Equipment Certification,” would be required for avionics systems and software.

AA 01: Safety and Security

Application Area Summary

Purpose

The purpose of the Safety and Security application area is to establish and maintain a safety and security capability, define and manage requirements based on risks attributable to threats, hazards, and vulnerabilities, and assure that products and services are safe and secure throughout their life cycle.

Major points addressed

The Safety and Security application area involves establishing and maintaining an infrastructure that ensures appropriate safety and security awareness, guidance, and competency, and that provides a safe and secure work environment. It addresses ensuring that required safety and security information is identified, retained, and protected. Operations and the environment are monitored, safety and security incidents and operational anomalies are analyzed and reported, and corrective actions are initiated. Plans are in place to ensure business continuity.

This application area involves the management of risks attributable to vulnerabilities, security threats, and safety hazards. These risks are identified, analyzed, and managed to achieve acceptable levels of risk. Safety and security requirements are determined, including regulatory requirements, laws, standards, policies, and required safety and security levels and methods. Safety and security levels are assigned to components and used to guide design decisions and rigor of evaluation. Products and services are developed, deployed, operated and sustained to satisfy safety and security needs and requirements. Throughout the life cycle, safety and security assurance arguments and supporting evidence are created, updated, and retained.

This application area also addresses safety and security management so that safety and security activities are planned and tracked, with independent reporting of safety and security status and issues. Acquired products and services are selected and managed using safety and security criteria. Safety and security activities are measured and monitored, products are controlled, and processes are improved.

Goals and application practices (APs)

Goal 1. An infrastructure for safety and security is established and maintained.

AP 01.01 Ensure Safety and Security Competency

Ensure safety and security awareness, guidance and competency.

AP 01.02 Establish Qualified Work Environment

Establish and maintain a qualified work environment that meets safety and security needs.

AP 01.03 Ensure Integrity of Safety and Security Information

Establish and maintain storage, protection and access and distribution control to ensure the integrity of safety and security information.

AP 01.04 Monitor Operations and Report Incidents

Monitor operations and environmental changes, report and analyze safety and security incidents and anomalies, and initiate corrective actions.

AA 01: Safety and Security Application Area

AP 01.05 Ensure Business Continuity

Establish and maintain plans to ensure continuity of business processes and protection of assets.

Goal 2. Safety and security risks are identified and managed.

AP 01.06 Identify Safety and Security Risks

Identify risks and sources of risks attributable to vulnerabilities, security threats, and safety hazards.

AP 01.07 Analyze and Prioritize Risks

For each risk associated with safety or security, determine the causal factors, estimate the consequence and likelihood of an occurrence, and determine relative priority.

AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan

Determine, implement, and monitor the risk mitigation plan to achieve an acceptable level of risk.

Goal 3. Safety and security requirements are satisfied.

AP 01.09 Determine Regulatory Requirements, Laws, and Standards

Determine applicable regulatory requirements, laws, standards, and policies and define levels of safety and security.

AP 01.10 Develop and Deploy Safe and Secure Products and Services

Develop and deploy products and services that meet safety and security needs, and operate and dispose of them safely and securely.

AP 01.11 Objectively Evaluate Products

Objectively verify and validate the work products and delivered products and services to assure safety and security requirements have been achieved and services fulfill intended use.

AP 01.12 Establish Safety and Security Assurance Arguments

Establish and maintain safety and security assurance arguments and supporting evidence throughout the life cycle.

Goal 4. Activities and products are managed to achieve safety and security requirements and objectives.

AP 01.13 Establish Independent Safety and Security Reporting

Establish and maintain independent reporting of safety and security status and issues.

AP 01.14 Establish a Safety and Security Plan

Establish and maintain a plan to achieve safety and security requirements and objectives.

AP 01.15 Select and Manage Suppliers, Products, and Services

Select and manage products and suppliers using safety and security criteria.

AP 01.16 Monitor and Control Activities and Products

Measure, monitor, and review safety and security activities against plans, control products, take corrective action, and improve processes.

Notes

The Safety and Security application area addresses safety and security in several contexts:

- Strategically, to support enterprise-wide safety and security work;

AA 01: Safety and Security Application Area

- At a program-level, for any program or organization that deals with safety and security of products and services across the life cycle;
- In the work environment, for ensuring people have tools and facilities needed for safe and secure development, operation, maintenance, and support of products and services; and
- By acquisition programs, for evaluating the capability of suppliers to deliver safe and secure products and services

The safety and security application practices are harmonized in this application area since so many activities are common to both safety and security. However, the practices can be implemented in the context chosen by the organization, which may be security or safety or both safety and security.

When considering the practices, there may be different parts of the organization responsible for different aspects of safety and security, such as physical, personnel, organizational, environmental, or information security. Successful implementation of the practices may require appropriate coordination and information exchange.

Further information on each practice can be obtained by reviewing the sources that are mapped to each practice, as indicated in the mapping table appendix. The mapping tables show the source standards that were used for deriving each practice and also indicate where safety and security application area users can find more detail and additional guidance regarding each practice.

Relationships between this application area and the reference models

This application area is to be used in conjunction with the Capability Maturity Model Integration v1.1 (CMMI) or the FAA integrated Capability Maturity Model v2.0 (iCMM).

Process Areas: This application area draws on implementing practices from the following process areas (PAs) for use with either the iCMM or CMMI. Where indicated, material from the iCMM PAs would be adopted for use in CMMI to provide the necessary practices for implementation of practices of the safety and security source standards. The particular implementing practices from these PAs are indicated along with the discussion of each application practice.

iCMM PAs	CMMI PAs (<i>including extensions from iCMM</i>)
PA 22 Training	Organizational Training
PA 19 Work Environment*	Work Environment*
PA 17 Information Management	<i>PA 17 Information Management (from iCMM)</i>
PA 10 Operation and Support	<i>PA 10 Operation and Support (from iCMM)</i>
PA 13 Risk Management	Risk Management
PA 00 Integrated Enterprise Management	<i>PA 00 Integrated Enterprise Management (from iCMM)</i> Organizational Environment for Integration Organizational Innovation and Deployment
PA 01 Needs PA 02 Requirements	Requirements Development Requirements Management
PA 03 Design PA 06 Design Implementation PA 07 Integration	Technical Solution Product Integration
PA 08 Evaluation	Verification Validation
PA 15 Quality Assurance & Management	Process and Product Quality Assurance

* Work Environment is a new Process Area for iCMM and proposed for CMMI

AA 01: Safety and Security Application Area

iCMM PAs	CMMI PAs (including extensions from iCMM)
PA 11 Project Management	Project Planning Project Monitoring and Control Integrated Project Management Quantitative Project Management
PA 16 Configuration Management	Configuration Management
PA 18 Measurement and Analysis	Measurement and Analysis
PA 05 Outsourcing PA 12 Supplier Agreement Management PA 09 Deployment, Transition, & Disposal	Supplier Agreement Management Integrated Supplier Management <i>PA 09 Deployment, Transition, & Disposal (from iCMM)</i>
PA 21 Process Improvement	Organizational Process Focus

Generic Practices: As with process areas in the CMMI and the iCMM, generic practices are applied to an application area to guide process improvement and to support appraisal of capabilities. The generic practices of the iCMM and the CMMI are depicted below:

	iCMM Generic Practices	CMMI Generic Practices
Capability Level 1	1.1 Identify the Work Scope 1.2 Perform the Process	1.1 Perform Base Practices
Capability Level 2	2.1 Establish Organizational Policy 2.2 Document the Process 2.3 Plan the Process 2.4 Provide Adequate Resources 2.5 Assign Responsibility 2.6 Ensure Skill and Knowledge 2.7 Establish Work Product Requirements 2.8 Consistently Use and Manage the Process 2.9 Manage Work Products 2.10 Objectively Assess Process Compliance 2.11 Objectively Verify Work Products 2.12 Measure Process Performance 2.13 Review Performance with Higher-level Management 2.14 Take Corrective Action 2.15 Coordinate With Participants & Stakeholders	2.1 Establish an Organizational Policy 2.2 Plan the Process 2.3 Provide Resources 2.4 Assign Responsibility 2.5 Train People 2.6 Manage Configurations 2.7 Identify and Involve Relevant Stakeholders 2.8 Monitor and Control the Process 2.9 Objectively Evaluate Adherence 2.10 Review Status with Higher Level Management
Capability Level 3	3.1 Standardize the Process 3.2 Establish and Use a Defined Process 3.3 Improve Processes	3.1 Establish a Defined Process 3.2 Collect Improvement Information
Capability Level 4	4.1 Stabilize Process Performance	4.1 Establish Quantitative Objectives for Process 4.2 Stabilize Subprocess Performance
Capability Level 5	5.1 Pursue Process Optimization	5.1 Ensure Continuous Process Improvement 5.2 Correct Root Causes of Problems

Glossary

A glossary is attached at the end this application area (see pages 58 and 59).

AA 01: Safety and Security Application Area

AP 01.01 Ensure Safety and Security Competency

Ensure safety and security awareness, guidance, and competency.

Description

Ensure all persons involved in any safety and security activity, including management activities, have the appropriate training, technical knowledge, experience, and qualifications relevant to the specific duties they have to perform. Determine and assess appropriate training, technical knowledge, experience, and qualifications in relation to the attributes of the particular safety and security application.

Identify needed improvements in safety and security skill and knowledge throughout the organization using the projects’ needs, organizational strategic plan, and existing employee skills as guidance. Train personnel to have the skills and knowledge needed to perform their assigned roles. Assess the effectiveness of the training to meet the identified training needs. Manage safety and security awareness, training, and education programs.

Provide safety and security related guidance to other groups to enable informed decisions about architecture, design, and implementation choices. Provide safety and security related guidance to operational system users and administrators so they know what must be done to install, configure, operate, maintain, and decommission the system in a safe and secure manner. Provide safety and security related guidance to the organization.

Implementing Practices

This application practice is implemented by performing the following practices in such a way as to ensure safety and security awareness, guidance, and competency.

<i>iCMM Implementing Practices</i>	<i>CMMI Implementing Practices</i>
<p><i>PA 22 Training</i> BP 22.01 Identify training needs for the organization, projects, teams, and support groups. BP 22.02 Establish and maintain a training plan. BP 22.03 Establish and maintain training capability and delivery mechanisms to address identified training needs. BP 22.04 Train individuals to have the skills and knowledge needed to perform their assigned roles. BP 22.05 Establish and maintain records of training and experience. BP 22.06 Assess the effectiveness of training to meet identified training needs. BP 22.07 Establish and maintain an environment that encourages learning.</p> <p><i>PA 19 Work Environment</i> BP 19.05 Ensure that personnel have the required competencies and qualifications to access, use, and maintain the work environment.</p>	<p><i>Organizational Training (OT)</i> OT SP 1.1-1 Establish and maintain the strategic training needs of the organization. OT SP 1.2-1 Determine which training needs are the responsibility of the organization and which will be left to the individual project or support group. OT SP 1.3-1 Establish and maintain an organizational training tactical plan. OT SP 1.4-1 Establish and maintain training capability to address organizational training needs. OT SP 2.1-1 Deliver the training following the organizational training tactical plan. OT SP 2.2-1 Establish and maintain records of the organizational training. OT SP 2.3-1 Assess the effectiveness of the organization’s training program.</p> <p><i>Work Environment (WE)</i> WE SP 1.5 Ensure that personnel have the required competencies and qualifications to access, use, and maintain the work environment.</p>

AA 01: Safety and Security Application Area

<i>iCMM Implementing Practices</i>	<i>CMMI Implementing Practices</i>
	<i>Project Planning (PP)</i> PP SP 2.5 Plan for knowledge and skills needed to perform the project

Typical Work Products

- human capital plan
- training plans
- safety or security certificates
- skills assessment
- competency assessment

Notes

Consider the following factors when assessing the competence of persons to carry out their duties. These factors pertain to those engaged in safety and security activities including, for example, acquirers, developers, suppliers, maintainers, operators, and managers.

- engineering knowledge appropriate to the application
- engineering knowledge appropriate to the technology (for example electrical, electronic, programmable electronic, software engineering, accident investigation, human factors)
- knowledge of the legal and regulatory frameworks and applicable industry guidelines
- the consequences in the event of failure of safety and security related systems - the greater the consequences the more rigorous should be the specification and assessment of competence
- the safety and/or security levels - the higher the levels the more rigorous should be the specification and assessment of competence
- the novelty of the design, design procedures, or application - the newer or more untried the designs, design procedures, or application the more rigorous should be the specification and assessment of competence should be
- previous experience and its relevance to the specific duties to be performed and the technology being employed - the greater the required competence levels, the closer the fit should be between the competencies developed from previous experience and those required for the specific duties to be undertaken
- relevance of qualifications to specific duties to be performed
- awareness of safety and security implications associated with supply chains contributing to products or services used or delivered

The training, experience and qualifications of all persons involved in safety and security activities should be documented.

If safety and security expertise does not exist within the organization, appropriate expertise should be acquired (see AP01.15).

AA 01: Safety and Security Application Area

AP 01.02 Establish Qualified Work Environment

Establish and maintain a qualified work environment that meets safety and security needs.

Description

The work environment is a critical component of the design, development, evaluation, operation, and maintenance of safety and security related systems. An appropriate work environment (including the set of integrated tools, techniques, services, measures, and standards) needs to be selected, applied, available, and qualified to satisfy the required safety and security level across the life cycle.

Perform calibrations of equipment and tools against, or traceable to, appropriate standards or vendor specifications. Maintain the work environment to continuously support the organizations and projects that depend on it. Identify new product technologies or enabling infrastructure that will help the organization acquire, develop, and apply technology for competitive advantage. Maintain awareness of the technologies that support the organization's safety and security goals and insert new technologies into the work environment based on the organization's business goals and the project's needs.

Establish, maintain, and monitor written agreements with third parties who access an organization's assets (i.e., information, facilities, and systems). Establish an authorization process for new information processing facilities (such as hardware and software). Establish, operate, and maintain the work environment including: facilities, information systems, information technology, safety and security personnel, physical safety and security, and personnel safety and security.

Implementing Practices

This application practice is implemented by performing the following practices in such a way as to establish and maintain a qualified work environment that meets safety and security needs.

<i>iCMM Implementing Practices</i>	<i>CMMI Implementing Practices</i>
<i>PA 19 Work Environment (NEW)</i> BP 19.01 Establish and maintain the needs and requirements to implement, operate, and sustain work environments. BP 19.02 Establish and maintain a description of work environment standards and tailoring guidelines that meet identified needs and requirements. BP 19.03 Establish and maintain a work environment, tailored from the work environment standards, to meet the specific needs. BP 19.04 Maintain the required qualification of work environment components. BP 19.05 Ensure that personnel have the required competencies and qualifications to access, use, and maintain the work environment. BP 19.06 Monitor, evaluate, and insert, as appropriate, new technology for improving the work environment. BP 19.07 Plan and provide for continuity of the work environment.	<i>Work Environment (WE) (NEW)</i> WE SP 1.1 Establish and maintain the needs and requirements to implement, operate, and sustain work environments. WE SP 1.2 Establish and maintain a description of work environment standards and tailoring guidelines that meet identified needs and requirements. WE SP 1.3 Establish and maintain a work environment, tailored from the work environment standards, to meet the specific needs. WE SP 1.4 Maintain the required qualification of work environment components. WE SP 1.5 Ensure that personnel have the required competencies and qualifications to access, use, and maintain the work environment. WE SP 1.6 Monitor, evaluate, and insert, as appropriate, new technology for improving the work environment. WE SP 1.7 Plan and provide for continuity of the work environment.

AA 01: Safety and Security Application Area

Typical Work Products

- equipment and tools needed to develop, maintain, and operate products and services at required safety and security levels
- safety and security procedures for use in the work environment
- safe and secure style guides
- qualified work environment components
- authorized, qualified personnel accessing the work environment
- a safe and secure work environment that complies with stakeholder needs and requirements
- agreements with external organizations
- process for authorizing facilities

Notes

Address special challenges created by a mobile workforce, or by facilities that are outsourced, to assure that these environments are safe and secure.

Address safety and security needs and requirements for the work environments at both the site and for specific programs, such as product development or maintenance programs. Collaboration is needed between those responsible for these environments.

The work environment should be included as part of any functional safety and security assessment of the system (see AP 01.11).

Safety and security regulations and standards pertaining to the work environment may be determined in AP 01.09.

Requirements for the work environment, e.g., requirements on specific tools, services, the level of automation, procedures, health and safety, etc., are determined when performing the implementing practices.

AA 01: Safety and Security Application Area

AP 01.03 Ensure Integrity of Safety and Security Information

Identify required safety and security information and maintain storage, protection, and access and distribution control for it.

Description

Identify required safety and security documents and information. Manage and control required information, including documentation, data, and assurance evidence, to ensure its integrity. Ensure that artifacts related to safety and security assurance monitoring and evaluation are suitably protected and distributed to authorized stakeholders.

Implementing Practices

This application practice is implemented by performing the following practices in such a way as to identify required safety and security information and maintain storage, protection, and access and distribution control for it.

<i>iCMM Implementing Practices</i>	<i>CMMI Implementing Practices (from iCMM)</i>
<i>PA 17 Information Management</i> BP 17.01 Establish and maintain a strategy and requirements for information management. BP 17.02 Establish an infrastructure for information management including repository, tools, equipment, and procedures. BP 17.03 Collect, receive, and store information according to established strategy and procedures. BP 17.04 Disseminate or provide timely access to information to those that need it. BP 17.05 Protect information from loss, damage, or unwarranted access. BP 17.06 Establish requirements and standards for content and format of selected information items.	<i>PA 17 Information Management (from iCMM)</i> BP 17.01 Establish and maintain a strategy and requirements for information management. BP 17.02 Establish an infrastructure for information management including repository, tools, equipment, and procedures. BP 17.03 Collect, receive, and store information according to established strategy and procedures. BP 17.04 Disseminate or provide timely access to information to those that need it. BP 17.05 Protect information from loss, damage, or unwarranted access. BP 17.06 Establish requirements and standards for content and format of selected information items.

Include requirements for safety and security information when implementing BP 17.01 and BP 17.06.

Typical Work Products

- strategy for management of safety and security information
- list of required safety and security information to be placed in information repository
- information access and security requirements
- information repository
- information capture, storage, protection, and access procedures
- privacy requirements and controls
- list of authorized users, which may include customers, certifiers, signatory authorities, and other users
- requirements and standards for content and format of safety and security information

Notes

The safety and security assurance evidence repository could take various forms, e.g., a database, engineering notebook, test results, or evidence log.

AA 01: Safety and Security Application Area

Assure transmission/dissemination (verbal, written, or electronic) of safety and security information among all authorized stakeholders, including persons and equipment involved in the acquisition, development, operation, and maintenance of the product or service, as appropriate. An example is to allow users to check whether a product has been subject to a safety recall.

Different safety and security standards may require different documents and information to be retained in safety and security records and assurance arguments.

See AP 01.12 for further information regarding typical safety and security assurance information to be stored, protected, and controlled.

AA 01: Safety and Security Application Area

AP 01.04 Monitor Operations and Report Incidents

Monitor operations and environmental changes, report and analyze safety and security incidents and anomalies, and initiate corrective actions.

Description

Detect, collect, analyze, and report safety and security related incidents that arise throughout the life cycle. Initiate timely corrective actions on all incidents that may have an impact on safety and security. Ensure all breaches of, attempted breaches of, or mistakes that could potentially lead to a breach of safety and security are identified and reported.

Monitor changes in threats, hazards, vulnerabilities, impacts, risks, and the environment. Monitor operations and the performance and functional effectiveness of safety and security safeguards. Monitoring performance includes detection of early warning signals and assuring awareness of potential problems. This may include identification and analysis of new trends regarding threats and hazards.

Review the safety and security posture of the product or service and report anomalies or conditions that require corrective action.

Implementing Practices

This application practice is implemented by performing the following practices in such a way as to monitor operations and environmental changes, report and analyze safety and security incidents and anomalies, and initiate corrective actions.

<i>iCMM Implementing Practices</i>	<i>CMMI Implementing Practices (from iCMM)</i>
<i>PA 10 Operation and Support</i> BP 10.02 Monitor and evaluate capacity, service, and performance of the system, product, or service. BP 10.05 Perform failure identification actions when a non-compliance has occurred in the product or delivered service. BP 10.06 Take corrective action when appropriate (e.g., defective part, human error), or initiate corrective action for product or service modification. BP 10.07 Establish a service to answer customer and user questions and help resolve problems they encounter.	<i>PA 10 Operation and Support (from iCMM)</i> BP 10.02 Monitor and evaluate capacity, service, and performance of the system, product, or service. BP 10.05 Perform failure identification actions when a non-compliance has occurred in the product or delivered service. BP 10.06 Take corrective action when appropriate (e.g., defective part, human error), or initiate corrective action for product or service modification. BP 10.07 Establish a service to answer customer and user questions and help resolve problems they encounter.

Ensure that safety and security incidents are included when implementing BP 10.02, and that failure analysis is performed when implementing BP 10.05.

Typical Work Products

- updated threat/hazard analyses and logs
- updated assurance argument
- reports of changes in the environment that may affect safety and security
- incident reports, including source of incident, any damage, response taken, and further action required
- periodic incident summaries

AA 01: Safety and Security Application Area

- failure analysis reports
- change requests
- operational problem reports

Notes

This practice includes reporting and analyzing incidents and monitoring changes that occur in the work environment used for product or service development, as well as in the environment where those products or services are operating. Both the internal and external environments are included.

Various tools, methods, and technologies may assist in detection and analysis including intrusion detection systems, incident analysis hardware and software, automated detection capabilities, and centralized logging systems. Problem reports from users are another detection mechanism. Incidents include anomalies reported when product or service behavior differs from expected behavior in the eyes of the operator.

Use analysis data to identify systematic weaknesses, insecure or unsafe features, and components with high incident rates. Perform causal analysis to find errors contributing to poor implementation and/or poor operation. Examine historical incident records (including compositions of log records) for relevant safety and security information to help determine cause of the incident, how it proceeded, and likely future events. Collect the conclusions to inform maintenance decisions for redesign and/or reimplementation. Assure that incidents and their analyses are recorded in logs and event records to assist future analyses.

Analysis may result in preventive recommendations to minimize the probability of an initial occurrence, as well as corrective recommendations to minimize probability of a repeat occurrence.

Incidents may cause initiation of risk mitigation planned actions (see AP 01.08) or of more detailed investigations. Environmental changes may initiate re-evaluations (see AP 01.11).

AA 01: Safety and Security Application Area

AP 01.05 Ensure Business Continuity

Establish and maintain plans to ensure continuity of business processes and protection of assets.

Description

Maintain plans to protect business processes and assets and counteract potential disruptions to business processes and activities from internal and external adverse conditions, failures, and threats. Maintain protection and continuity plans for the infrastructure, operational, and development environments. Use appropriate risk management practices to identify business continuity risks and to develop continuity plans. Test and evaluate business continuity plans with appropriate frequency to ensure they are up to date and effective in protecting assets and restoring business operations within needed time scales following interruptions or failures.

Implementing Practices

This application practice is implemented by performing the following practices in such a way as to maintain plans that ensure continuity of business processes.

<i>iCMM Implementing Practices</i>	<i>CMMI Implementing Practices</i>
<p><i>PA 19 Work Environment</i> BP 19.07 Plan and provide for continuity of the work environment.</p> <p><i>PA 13 Risk Management</i> BP 13.01 Establish and maintain an approach for managing risk that is the basis for identifying, assessing, mitigating, and monitoring risks for the life of the project. BP 13.02 Identify project risks by examining objectives, alternatives, and constraints in the context of established sources of risk. BP 13.03 Assess risks to determine their likelihood of occurrence and the consequences if they occur. BP 13.04 Develop risk mitigation plans for risks that meet risk action criteria defined by the risk management approach. BP 13.05 Implement, monitor, and control risk mitigation activities in accordance with risk mitigation plans.</p> <p><i>PA 00 Integrated Enterprise Management</i> BP 00.03 Establish and maintain the enterprise strategic plans that identify business objectives to be achieved, areas of business to be pursued and their interrelationships, and the significant goals to be accomplished.</p>	<p><i>Work Environment (WE)</i> WE SP 1.7 Plan and provide for continuity of the work environment.</p> <p><i>Risk Management (RSKM)</i> RSKM SP 1.1-1 Determine risk sources and categories. RSKM SP 1.2-1 Define the parameters used to analyze and categorize risks, and the parameters used to control the risk management effort. RSKM SP 1.3-1 Establish and maintain the strategy to be used for risk management. RSKM SP 2.1-1 Identify and document the risks. RSKM SP 2.2-1 Evaluate and categorize each identified risk using the defined risk categories and parameters, and determine its relative priority. RSKM SP 3.1-1 Develop a risk mitigation plan for the most important risks to the project, as defined by the risk management strategy. RSKM SP 3.2-1 Monitor the status of each risk periodically and implement the risk mitigation plan as appropriate.</p> <p><i>PA 00 Integrated Enterprise Management (from iCMM)</i> BP 00.03 Establish and maintain the enterprise strategic plans that identify business objectives to be achieved, areas of business to be pursued and their interrelationships, and the significant goals to be accomplished.</p>

Note: This application practice depends on using risk management practices at either the enterprise level or project level.

AA 01: Safety and Security Application Area

Typical Work Products

- business continuity plan
- business impact analysis
- information technology contingency plan
- business contingency plan
- business continuity test plan
- business continuity Training exercises
- business continuity test results

Notes

This application practice is a specific instance of risk management applied to ensuring continuity of the business. Business continuity plans should be developed for programs that accept high safety or security risk, as well as cases where the cost of business continuity activities would be reasonable with respect to the risk of loss. Considerations for business continuity planning include: analysis of threats (natural and human) and vulnerabilities, hazards, tampering, hardware failures, software bugs, operator error (accidental deletions), and loss of key personnel/skills. Business continuity plans may be called: security contingency plans, safety contingency plans, emergency plans, or other names. Plans should address alternate facilities and equipment, regular backups, offsite storage, and testing of business continuity plans and procedures. A comprehensive discussion on planning for business continuity related to security can be found in ISO/IEC 17799:2000-12-01.

Infrastructure for which continuity is to be planned includes facilities, tools, equipment, computing resources, communications systems, techniques, standards, work space, laboratories, procedures, office equipment and supplies. Protection and continuity for the operations and development environment should address workers, organization and enterprise management, customers, and other stakeholders, including the general public.

Business vulnerabilities are varied, including: insecure communications links, document disposal, access procedures, and lack of encryption for security. For safety they may include: geographic location (sites at low elevations or in coastal areas, tornado zones, etc), hazardous materials used in products or production, and inherently unsafe design features. Threats include any entity with potential for causing harm (malicious or not, human or not), such as foreign or domestic agents, other governments, hackers, hurricanes and floods, or solar storms.

AA 01: Safety and Security Application Area

AP 01.06 Identify Safety and Security Risks

Identify risks and sources of risks attributable to vulnerabilities, security threats, and safety hazards.

Description

Identify all credible security threats or safety hazards. Identify known safety or security controls. Identify vulnerabilities, faults, and failures that could be exercised by potential threat or hazard sources arising from natural sources, as well as man-made sources, both accidental and deliberate. Maintain a list of risks and their sources resulting from vulnerabilities, security threats, and safety hazards.

Implementing Practices

This application practice is implemented by performing the following practices, in such a way to identify risks and sources of risk attributable to vulnerabilities, threats, and hazards.

<i>iCMM Implementing Practices</i>	<i>CMMI Implementing Practices</i>
<i>PA 13 Risk Management</i> BP 13.02 Identify project risks by examining objectives, alternatives, and constraints in the context of established sources of risk.	<i>Risk Management (RSKM)</i> RSKM SP 1.1-1 Determine risk sources and categories RSKM SP 1.2-1 Define risk parameters RSKM SP 2.1-1 Identify and document the risks.

Typical Work Products

- accident list
- hazard or threat source lists (external and internal)
- hazard or threat log
- hazard or threat category lists
- system environment and boundary definition
- hazard or threat analysis scope definition
- system functional model
- hazard or threat model
- hazard and operability analysis
- functional failure analysis (FFA) tables
- preliminary hazard or threat list
- threat and vulnerability matrix

Notes

Identify risks and their potential sources, including sources pertaining to potential lack of management, operational, and technical controls, during all life cycle phases.

Monitor changes to security threats and safety hazards, which could result from changes in the environment, such as new requirements or insertion of new technology (see also AP 01.04).

For safety:

In determining hazards, a detailed description of the product or service, including the boundary, physical equipment, operating environment, and interfaces (physical, functional, and logical) is useful, as well as a high level functional model of the product or service in its environment. This

AA 01: Safety and Security Application Area

model includes the current product or service design and provides detail on the target functionality to allow a systematic hazard analysis. An understanding of the required control functions and its physical environment is essential. Define the physical equipment to be included in the scope of the hazard and risk analysis.

The types of hazard sources or accident-initiating events to consider include component failures, procedural faults, human error, and energy sources. The review of safety experiences on similar systems, including incident hazard tracking logs, lessons-learned, checklists, and history, provides a good foundation for the hazard identification process. The hazards and hazardous events of the system are determined based on credible circumstances. This includes all relevant human factors issues, giving particular attention to abnormal or infrequent modes of operation. Consider hazards due to interaction with other equipment sited in physical proximity, including interaction with equipment that is not under safety control. Information about the determined hazards is obtained (for example, toxicity, electromagnetic interference, explosive conditions, corrosiveness, reactivity, and flammability). Document all hazards identified. Cross-reference each hazard to any related safety requirements and record logs.

For security:

It is important to identify product and service assets, including personnel, equipment, and information assets, and categorize them based on their value to operational, business, or mission requirements. Reviewing similar products and services provides a good foundation for identifying vulnerabilities that could be exercised or exploited by known threat sources. A preliminary threat-vulnerability matrix should be developed, which contains threat source and its definition, potential vulnerability(ies) that could be exercised, and current security controls. The matrix will be updated in AP 01.07 to document the analysis of the likelihood and impact of a security threat if vulnerability is successfully exercised.

AA 01: Safety and Security Application Area

AP 01.07 Analyze and Prioritize Risks

For each risk associated with safety or security, determine the causal factors, estimate the consequence and likelihood of an occurrence, and determine relative priority.

Description

For each threat or hazard, determine the causal factors associated with the product or service environment, including hardware, software, human, and environmental factors. Develop a list of causal factors that are both accidental and deliberate in nature. For all potential consequences, assess the severity and likelihood of an occurrence. The severity and likelihood are combined to obtain an estimate of risk for each threat or hazard. Aggregate risk may also be determined based on a combination of threats or hazards. Determine the adverse impact resulting from a hazard or threat. Select the most appropriate quantitative or qualitative methods to determine relative priority. Risks are prioritized by likelihood and adverse impact, including the capability to protect critical assets.

Implementing Practices

This application practice is implemented by performing the following practices in such a way to determine the causal factors, estimate the consequence and likelihood of an occurrence, and determine the relative priority for each risk.

<i>iCMM Implementing Practices</i>	<i>CMMI Implementing Practices</i>
<i>PA 13 Risk Management</i> BP 13.02 Identify project risks by examining objectives, alternatives, and constraints in the context of established sources of risk. BP 13.03 Assess risks to determine their likelihood of occurrence and the consequences if they occur.	<i>Risk Management (RSKM)</i> RSKM SP 2.1-1 Identify and document the risks. RSKM SP 2.2-1 Evaluate and categorize each identified risk using the defined risk categories and parameters, and determine its relative priority.

Typical Work Products

- failure modes and effects analysis reports
- failure modes effects and criticality analysis reports
- event tree analysis reports
- fault tree analysis reports
- risk assessment report
- risk indices
- risk hazard index
- threat analysis report
- safety criteria report
- system threat analysis report
- threat log
- feasible controls list
- cost-benefit analysis
- security requirements checklist
- causal factors list

AA 01: Safety and Security Application Area

Notes

For Safety:

To determine the conditions and sequences of events that lead to hazards, consider the types of accident-initiating events. The types of accident-initiating events include:

- system, subsystem, or component failure or malfunction (hardware and software)
- environmental conditions
- design inadequacies
- procedural deficiencies (faults)
- accidental and deliberate human error
- dependent failure mechanisms that can cause accident sequences to occur

Document causal factors, ensuring traceability is maintained between the causal factors, hazards, and accidents.

Severity may be assessed qualitatively (e.g., catastrophic, major, or minor) or quantitatively (e.g., 10 fatalities, 1 fatality, 1 severe injury). 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, 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 and source of each individual event may be drawn from manufacturer's specifications or historical data from previous accidents.

Where systematic failures are seen as contributing to the likelihood of an accident, a quantitative analysis may be an inappropriate method to assign system failure rates. Instead, the process is reversed to set safety targets for system failure rates. Different standards use different terms, such as safety integrity levels, claim limits, or levels of trust, for this concept of assigning qualitative indicators to the required level of protection against systematic failures. Varying levels of methods, techniques, rules, and standards should be associated with the different levels of required protection.

For Security:

To determine an overall likelihood rating, consider the probability that a potential vulnerability will be exercised within the construct of the target environment. Consider three governing factors: threat-source motivation and capability, nature of the vulnerability, and existence and effectiveness of existing security controls. The likelihood and severity is qualified, e.g., as high, medium, or low. Then conduct an impact analysis resulting from a threat-exploiting system vulnerability.

Before an impact analysis can be conducted, understand system mission, system and data criticality (value to an organization), and system and data sensitivity. The system or information owner is the principal source of this information. If the documentation does not exist, the system and data sensitivity can be determined based on the level of protection required to maintain the system and data's availability, integrity, and confidentiality.

Some impacts are measured quantitatively, such as cost of repairing the system. Other impacts (e.g., loss of public confidence) are not measured in specific units, but in terms of high, medium, and low impact. Before conducting the impact analysis, consideration should be given to advantages and disadvantages of quantitative versus qualitative assessments. The assessment measurement used

AA 01: Safety and Security Application Area

allows the determination of the magnitude of the impact and its relative priority to the other identified risks. The results of the assessment are documented in a risk assessment report.

AA 01: Safety and Security Application Area

AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan

Determine, implement, and monitor the risk mitigation plan to achieve an acceptable level of risk.

Description

Compare risk presented by each hazard or threat with the acceptable levels of safety and security. The feasibility and effectiveness of the recommended control options are analyzed. Select the most appropriate and cost-effective control(s) or countermeasure(s) to reduce risk to an acceptable level, with minimal adverse impact on resources and mission. After risk mitigations are determined, repeat the risk analysis (see AP 01.07) to determine how recommended mitigations may affect the risks associated with safety and security, paying particular attention to mitigations that may have added new risks or increased existing risks. Develop a risk mitigation plan that documents the approach and associated activities to ensure that objectives are implemented. Execute the risk mitigation plan. Monitor risk mitigation activities to ensure the needed results are obtained.

Implementing Practices

This application practice is implemented by performing the following practices in such a way as to determine, implement and monitor the risk mitigation plan to achieve an acceptable level of risk.

<i>iCMM Implementing Practices</i>	<i>CMMI Implementing Practices</i>
<i>PA 13 Risk Management</i> BP 13.04 Develop risk mitigation plans for risks that meet risk action criteria defined by the risk management approach. BP 13.05 Implement, monitor, and control risk mitigation activities in accordance with risk mitigation plans.	<i>Risk Management (RSKM)</i> RSKM SP 3.1-1 Develop a risk mitigation plan for the most important risks to the project, as defined by the risk management strategy. RSKM SP 3.2-1 Monitor the status of each risk periodically and implement the risk mitigation plan as appropriate.

Typical Work Products

- probability targets
- risk log
- recommended safety and security requirements
- risk mitigation plan
- hazard record/report
- safety action record
- security incident log
- hazard database

Notes

Identifying the appropriate risk mitigation measures requires a good understanding of the causal factors contributing to the occurrence of a threat or hazard, since mechanisms may have to modify one or more of these factors to be effective in reducing risk.

Essential mitigation measures, which are necessary for the product and/or service to meet the safety or security criteria, are referred to as safety or security requirements. These are integrated with other product and/or service requirements (see AP 01.10). Development of the product and/or service should not proceed until all these requirements are agreed upon and the risk mitigation plan is accepted by stakeholders and approving authorities. As the product and/or service proceeds through

AA 01: Safety and Security Application Area

implementation, particular attention is paid, when evaluating the results of performance monitoring, to verifying that mitigation measures are working as intended. The objective is to identify risks that are not fully addressed and determine whether additional control(s) or measure(s) are needed. After the appropriate controls are in place for risks, the approving authority signs a statement accepting the residual risk and authorizing the operation of the product and/or service (see also AP 01.12).

The earlier in the life cycle that threats or hazards are identified, the easier it is to change the design if necessary. As product and/or service development nears implementation, changing the design becomes more difficult and costly and may result in reducing the available mitigation options to address hazards or threats that are not identified until a later stage of development. When new threats or hazards are discovered throughout the life cycle, examine closely whether implementing the associated mitigation measures might introduce new hazards or threats and then evaluate the acceptability of the risk with the proposed mitigation measures in place.

If the risk does not meet the acceptability criteria (see AP 01.10), an attempt must be made to reduce it to a level that is acceptable. Risk mitigation activities should address reducing the probability of occurrence and the severity of the consequences. To mitigate risks, consider technical, management, and operational safety and security controls, or a combination of these, to maximize their effectiveness in an operating environment. Achieving the desired level of risk reduction may require implementing more than one mitigation measure.

Possible approaches to risk mitigation include:

- assumption of risk by the appropriate stakeholders
- risk avoidance, by eliminating causal factors or consequences
- risk limitation, by implementing safeguards and controls
- risk transference, such as buying insurance
- reducing vulnerabilities or hazards through system, product, or service design, or design revision
- modification of operational procedures
- changes to staffing arrangements
- training of personnel to deal with the hazard or threat

The implemented controls may lower the risk level but still not eliminate the risk. The remaining risk after the implementation of new or enhanced control is known as residual risk. The risk reduction strategy must address how residual risk will be handled.

AA 01: Safety and Security Application Area

AP 01.09 Determine Regulatory Requirements, Laws, and Standards

Determine applicable regulatory requirements, laws, standards, and policies and define levels of safety and security.

Description

Gather external influences that affect safety and security including laws, mandates, regulatory requirements, standards, and policies. Determine which are applicable and resolve conflicts if they arise. Establish and maintain criteria that reflect levels of safety and security. Select the standards, methods, techniques, rules, and tools required to address safety and security during each phase of the life cycle in accordance with the defined levels of safety and security. Establish organizational policy, including rules, directives, and practices required for safety and security at various levels of detail, as appropriate.

Implementing Practices

This application practice is implemented by performing the following practices in such a way as to determine applicable regulatory requirements, laws, standards, and policies and define levels of safety and security.

<i>iCMM Implementing Practices</i>	<i>CMMI Implementing Practices</i>
<p><i>PA 02 Requirements</i> BP 02.02 Identify requirements and constraints pertaining to processes used in providing the required product or service, and pertaining to the context or intended operational environment.</p> <p><i>PA 00 Integrated Enterprise Management</i> BP 00.01 Establish, maintain, and communicate a strategic vision that identifies long-term goals, values, performance expectations, and core activities.</p> <p>BP 00.07 Address the impacts on society of planned activities, products, services, and operations, considering regulatory and legal requirements and risks associated with products, services, and operations.</p>	<p><i>Requirements Development (RD)</i> NEW RD PRACTICE PROPOSED: RD SP 3.25-1 Determine applicable standards: Determine regulatory and legal requirements, policies, and standards that will be applied to the product and its development, manufacturing, operation and support processes.</p> <p><i>PA 00 Integrated Enterprise Management (from iCMM)</i> BP 00.01 Establish, maintain, and communicate a strategic vision that identifies long-term goals, values, performance expectations, and core activities.</p> <p>BP 00.07 Address the impacts on society of planned activities, products, services, and operations, considering regulatory and legal requirements and risks associated with products, services, and operations.</p>

When implementing BP 02.02, note that nonfunctional requirements and constraints may include regulations, laws, mandates, standards, organizational policy, practices, or principles that are required to be applied in developing or providing a product or service at any or all phases of the life cycle. A new CMMI practice to address this topic is proposed, as indicated above.

Typical Work Products

- list of regulatory and legal requirements, selected application standards, and external policies
- organizational policies
- criteria reflecting levels of safety and security
- safety and security principles and constraints
- standards, methods, tools, rules, techniques, and process requirements appropriate to each safety or security level, for use during the life cycle

AA 01: Safety and Security Application Area

- justification for selection of standards

Notes

Identify and select standards and laws that provide more detailed industry-specific guidance for safety and security, as applicable. Regulatory requirements, legal requirements, and standards may either be directly applicable to the domain, e.g., avionics, or tailored to the domain. In general, it is preferable to use the framework of a single standard. If multiple standards are used, consideration needs to be given to the compatibility of the standards.

When there are choices among standards and regulatory frameworks, identify selection criteria and justify the decisions made. Conflicts may occur between laws and regulations that are applicable in different countries or different types of business. Some countries may place a legal obligation on suppliers of safety or security related equipment or services irrespective of contractual requirements (or lack thereof). There may be potential conflicts among global and local policies, or among relevant standards. When these occur, such conflicts should, at a minimum, be identified and resolved if possible.

Safety and security levels denote an expression of trust that a product or service will perform as expected. Each level designates a range of values indicating the extent to which the safety or security risks associated with a product or service have been contained. Levels are usually derived from policies set by government, regulatory bodies, customers, or internally within the organization. Criteria may involve levels for accidents that are classified as catastrophic or critical, or levels for fatalities caused by the product or service, or both. The types of harm to consider may include harm to people (fatalities and/or injuries), damage to the environment, loss of functionality, and loss of assets.

Determine appropriate tools, techniques, and methods (e.g., regarding project management, documentation, formal methods, evaluation methods, risk analysis, detection tools, coding standards, and degree of independence) depending on safety and security levels and other factors such as application sector and its accepted good practices and legal and regulatory requirements.

Policy is likely to be at several levels of detail including, for example, broad organizational policy and policies on specific safety and security topics. Policy states management's commitment to safety and security and typically includes the organization's approach to safety and security management. Organizational policy may address topics such as overall safety and security objectives, reporting of safety and security incidents, what needs to be protected, training and education requirements, consequences of policy violations, and business continuity management. Detailed implementation policy may address topics such as access control, patch management, incident response, evidence retention, etc.

AA 01: Safety and Security Application Area

AP 01.10 Develop and Deploy Safe and Secure Products and Services

Develop and deploy products and services that meet safety and security needs and requirements and operate and dispose of them safely and securely.

Description

Integrate safety and security into all phases of product and service life cycles, including needs, requirements, design, integration, evaluation, implementation, deployment, production, operation, and disposal. Employ established methods to build and operate safe and secure products to assure that needed levels of safety and security are defined and met. This includes the application of laws, standards and regulations and methods such as risk management and independent review, evaluation, and reporting, in concert with the assignment of appropriate responsibility and accountability.

In developing the needs and requirements, determine the acceptable levels of safety and security and use the results of hazard, vulnerability, threat, and risk analyses to specify and maintain the requirements and features for safe and secure products throughout the life cycle. Integrate and harmonize the safety and security requirements with the mission, production, operation, disposal, and other requirements to develop a complete set of product and service requirements. Allocate levels of safety and security and their requirements to derived requirements, design levels, and components in an iterative fashion, as the design evolves. Trace the requirements through the derived requirements, design levels, and components and evaluate the traceability and the components to ensure that the established levels of safety and security are preserved. Design and implement appropriate equipment, training, and procedures for safely and securely developing, deploying, operating, maintaining, and disposing of products and services. Employ established design guidelines and methods that enhance the safety and security of products and services. Transition, deploy, operate, maintain, and dispose of products and services according to the established needs, requirements, and plans.

Implementing Practices

This application practice is implemented by performing the following practices in such a way as to develop and deploy products and services that meet safety and security needs and requirements and operate and dispose of them safely and securely.

<i>iCMM Implementing Practices</i>	<i>CMMI Implementing Practices</i>
<i>PA 01 Needs</i> BP 01.01 Identify customers and stakeholders. BP 01.02 Elicit customer and other stakeholders' needs, expectations, and measures of effectiveness. BP 01.03 Analyze needs and expectations in the context of the intended operational environment. BP 01.04 Establish and maintain a statement of customer and other stakeholder needs and expectations that is understood and agreed upon by the customer and other stakeholders. BP 01.05 Communicate and interact with customers and other stakeholders throughout the life cycle to assure a common understanding of the status and disposition of needs, expectations, and measures of effectiveness.	<i>Requirements Development (RD)</i> RD SP 1.1-2. Elicit stakeholder needs, expectations, constraints, and interfaces for all phases of the product life cycle. RD SP 1.2-1 Transform stakeholder needs, expectations, constraints, and interfaces into customer requirements. RD SP 2.1-1 Establish and maintain product and product-component requirements, which are based on the customer requirements. RD SP 2.2-1 Allocate the requirements for each product component. RD SP 2.3-1 Identify interface requirements. RD SP 3.1-1. Establish and maintain operational concepts and associated scenarios.

AA 01: Safety and Security Application Area

<i>iCMM Implementing Practices</i>	<i>CMMI Implementing Practices</i>
<p><i>PA 02 Requirements</i></p> <p>BP 02.01 Identify functional and performance requirements, and required product or service attributes, including any requirements pertaining to safety, security, human factors, or other specialized areas.</p> <p>BP 02.02 Identify requirements and constraints pertaining to processes used in providing the required product or service, and pertaining to the context or intended operational environment.</p> <p>BP 02.03 Identify key requirements that have a strong influence on cost, schedule, functionality, risk, or performance, or that are critical to customers and other stakeholders.</p> <p>BP 02.04 Derive requirements that may be identified as necessary implications of stated functional, nonfunctional, interface, or other derived requirements.</p> <p>BP 02.05 Identify the requirements associated with external interfaces to the system, product, or service.</p> <p>BP 02.06 Analyze requirements to ensure that they satisfy established quality criteria including unambiguity, completeness, traceability, feasibility, and verifiability.</p> <p>BP 02.07 Record, approve, baseline, and place under change control all requirements, derived requirements, derivation rationale, traceability, and requirements status.</p> <p>BP 02.09 Maintain traceability among requirements and between requirements and plans, work products, and activities, initiating corrective action if inconsistencies are identified.</p> <p><i>PA 03 Design</i></p> <p>BP 03.01 Establish and use a mechanism to capture, prioritize, and resolve product and service design issues.</p> <p>BP 03.02 Evaluate alternatives against established criteria to select the architecture, structure, and elements for the product or service design.</p> <p>BP 03.03 Develop interface specifications for the selected product and service elements.</p> <p>BP 03.04 Allocate product and derived requirements to the design elements and interfaces, and to personnel or processes where appropriate.</p> <p>BP 03.05 Define the dynamic interactions and operational sequences among design elements.</p> <p>BP 03.06 Establish design specifications for each element of the product or service.</p> <p>BP 03.07 Establish and use a strategy for managing issues relating to the use of non-developmental item (NDI) product and service elements.</p> <p>BP 03.08 Establish and maintain a complete description of the product and service design.</p> <p><i>PA 06 Design Implementation</i></p> <p>BP 06.01 Establish the methods, standards, and tools to be used to implement the solution component(s) strategy.</p> <p>BP 06.02 Formulate solution components according to</p>	<p>RD SP 3.2-1. Establish and maintain a definition of required functionality.</p> <p>RD SP 3.4-3 Analyze requirements to balance stakeholder needs and constraints.</p> <p>RD SP 3.5-2 Validate requirements to ensure the resulting product will perform as intended in the user's environment using multiple techniques as appropriate.</p> <p><i>NEW RD PRACTICE PROPOSED:</i></p> <p>RD SP 3.25-1 Determine applicable standards: Determine regulatory and legal requirements, policies, and standards that will be applied to the product and its development, manufacturing, operation and support processes.</p> <p><i>Requirements Management (RM)</i></p> <p>RM SP 1.1-1 Develop an understanding with the requirements providers on the meaning of the requirements.</p> <p>RM SP 1.2-2 Obtain commitment to the requirements from the project participants.</p> <p>RM SP 1.3-1 Manage changes to the requirements as they evolve during the project.</p> <p>RM SP 1.4-2 Maintain bidirectional traceability among the requirements and the project plans and work products.</p> <p>RM SP 1.5-1 Identify inconsistencies between the project plans and work products and the requirements.</p> <p><i>Technical Solution (TS)</i></p> <p>TS SP 1.1-2 Develop detailed alternative solutions and selection criteria.</p> <p>TS SP 1.2-2 Evolve the operational concept, scenarios, and environments to describe the conditions, operating modes, and operating states specific to each product component.</p> <p>TS SP 1.3-1 Select the product-component solutions that best satisfy the criteria established.</p> <p>TS SP 2.1-1 Develop a design for the product or product component.</p> <p>TS SP 2.2-3 Establish and maintain a technical data package.</p> <p>TS SP 2.3-3 Design comprehensive product-component interfaces in terms of established and maintained criteria.</p> <p>TS SP 2.4-3 Evaluate whether the product components should be developed, purchased, or reused based on established criteria.</p> <p>TS SP 3.1-1 Implement the designs of the product components.</p> <p>TS SP 3.2-1 Develop and maintain the end-use documentation.</p> <p><i>Product Integration (PI)</i></p> <p>PI SP 3.2-1 Assemble product components according to the product integration sequence and available</p>

AA 01: Safety and Security Application Area

<i>iCMM Implementing Practices</i>	<i>CMMI Implementing Practices</i>
<p>the specifications. BP 06.03 Develop and maintain the documentation that will be used to operate and maintain the product or service components.</p> <p><i>PA 07 Integration</i> BP 07.04 Assemble or integrate product and service elements in accordance with the integration strategy.</p> <p><i>PA 09 Deployment, Transition, and Disposal</i> BP 09.01 Develop a strategy for deployment, transition, and disposal and perform activities in accordance with the strategy. BP 09.02 Establish the facility and infrastructure environment to receive and operate the product or service. BP 09.03 Verify fielded configuration items reflect the product or service baseline and manage change control. BP 09.04 Demonstrate the ability of the customer/ stakeholder support organization to maintain, modify and support the product or service. BP 09.05 Transfer the product or service to the customer/ stakeholder operation and support organizations. BP 09.06 Deactivate and dispose of the replaced product and/or dispense with replaced service.</p> <p><i>PA 10 Operation and Support</i> BP 10.01 Operate the system, product, or service in its intended environment and in the specified way. BP 10.03 Confirm availability of required resources (personnel and parts) to ensure service levels can be sustained. BP 10.04 Perform preventive maintenance by replacing or servicing products/system elements prior to failure. BP 10.06 Take corrective action when appropriate (e.g., defective part, human error), or initiate corrective action for product or service modification. BP 10.07 Establish a service to answer customer and user questions and help resolve problems they encounter.</p>	<p>procedures.</p> <p><i>PA 09 Deployment, Transition, and Disposal (from iCMM)</i> BP 09.01 Develop a strategy for deployment, transition, and disposal and perform activities in accordance with the strategy. BP 09.02 Establish the facility and infrastructure environment to receive and operate the product or service. BP 09.03 Verify fielded configuration items reflect the product or service baseline and manage change control. BP 09.04 Demonstrate the ability of the customer/ stakeholder support organization to maintain, modify and support the product or service. BP 09.05 Transfer the product or service to the customer/ stakeholder operation and support organizations. BP 09.06 Deactivate and dispose of the replaced product and/or dispense with replaced service.</p> <p><i>PA 10 Operation and Support (from iCMM)</i> BP 10.01 Operate the system, product, or service in its intended environment and in the specified way. BP 10.03 Confirm availability of required resources (personnel and parts) to ensure service levels can be sustained. BP 10.04 Perform preventive maintenance by replacing or servicing products/system elements prior to failure. BP 10.06 Take corrective action when appropriate (e.g., defective part, human error), or initiate corrective action for product or service modification. BP 10.07 Establish a service to answer customer and user questions and help resolve problems they encounter.</p>

Typical Work Products

- safety and security requirements
- requirements specification that includes safety and security requirements
- system requirements specifications (with safety and security annotations)
- traceability of needs, requirements, design, components, and evaluations through all levels of requirements and design
- interface requirements
- required levels of safety and security
- product design documents that meet safety and security requirements
- criteria for design methods
- design checklists for safety and security
- safe and secure style guides

AA 01: Safety and Security Application Area

- technical data package that addresses safety and security
- operating, maintenance, deactivation, and disposal procedures
- system architecture documents
- requirements and design for transition, deployment, deactivation, and disposal

Notes

Risk analysis and management activities and evaluations of work products and the environment are key inputs to the safe and secure product and service development-through-disposal life cycle. Risk analyses relating to hazards, vulnerabilities, threats, technology, environment, and component characteristics drive the requirements and design to achieve the required level of safety and security (see AP 01.08). Levels are established in accordance with selected criteria as described in AP 01.09. These levels determine the methods, standards, tools, and level of rigor to be used during product and service development and evaluation. The required level of safety and security, along with supporting data, provide a sound basis for requirements, design, and subsequent life cycle phases.

Stakeholder needs (mission and safety/security) are elicited, reviewed, and agreed on. Selected references, standards and checklists of possible hazards, vulnerabilities, and threats are valuable in developing a complete and valid set of requirements. Requirements associated with the safety and security functions are reviewed to ensure they are necessary and sufficient with respect to mitigating the targeted hazards and vulnerabilities and that they do not inadvertently introduce unintended or unrecognized hazards or vulnerabilities. Requirements should also be reviewed against quality criteria (e.g., precise, unequivocal, unambiguous, verifiable, up/down traceability among derived requirements, design levels, and implementation). Requirements and controls should reflect mitigation of the risk of harm to individuals, government, society, and tangible assets, as well as damage to business or national security information assets that might result from failures of safety or security. (See AP 01.11 for more information on reviews and evaluation relating to safety and security.)

Safety and security functions and their requirements should be identified separately from functions and requirements that are unrelated to safety and security. In cases where functions include both safety and security related functionality and non-safety and security related functionality and requirements, the method of achieving independence and its justification should be documented. Additional guidelines and methods are available for developing designs that incorporate fault tolerance and fault avoidance; such methods include simplicity, isolation, sneak circuit analysis, and failure mode effects analysis. An appropriate level of rigor should be applied to the review and configuration control of interfaces to other functions to ensure that access and use of non-safety and security functionality poses no risk to safety and security. The same considerations should be applied to functions of different safety/security levels that are to be implemented in the same design.

All the functions, components, and their related requirements necessary to achieve the required safety and security level should be documented. Documentation should include states and modes for which each requirement applies, allocated safety and security levels, throughput and response times, operator interfaces, system interfaces, worst case analyses, start up and shut down sequences, and constraints such as environmental extremes and the electromagnetic environment/limits.

The practices of AP 01.04 should be employed during operation to detect the need for changes and corrective actions. Corrective actions, including component modifications, should only be performed

AA 01: Safety and Security Application Area

when authorization for the action or change has been issued based on an action or modification request that addresses affected hazards and/or vulnerabilities, proposed change, reason for change, and impact analysis.

New requirements or design changes include those resulting from risk mitigation activities throughout the life cycle.

Deactivation and disposal considerations should include appropriate disposal of hazardous materials, reassignment of displaced staff, and destruction or protection of sensitive information.

AA 01: Safety and Security Application Area

AP 01.11 Objectively Evaluate Products

Objectively evaluate products and services to ensure safety and security requirements have been achieved and products and services fulfill their intended use.

Description

Objectively determine whether products or services exhibit the required level of safety and security. Ensure the needed level of objectivity by appropriate means such as the use of independent evaluators. Collect the body of evidence needed to support safety and security claims. Evaluate safety and security claims to determine whether they are warranted based on the demonstrated satisfaction of safety and security requirements.

Define the strategy, procedures, and level of rigor for verifying and validating requirements, designs, products, services, and components, including the depth and breadth of coverage, pass/fail criteria, conditions, and operating modes. Evaluate products, services, requirements, derived requirements, designs, intermediate levels of design, and components to demonstrate compliance with requirements and operational needs, including standards, regulations, and laws, throughout the life cycle. Analyze the results of evaluations and provide recommendations regarding the acceptability of the product or service evaluated. Conduct re-evaluation and update documentation, including assurance cases, when products, services, or the environment changes. Confirm the evaluation environment and tools and calibrations to ensure they meet needed levels of safety and security and are adequate for evaluating products and services.

Implementing Practices

This application practice is implemented by performing the following practices in such a way as to objectively evaluate products and services to ensure safety and security requirements have been achieved and products and services fulfill their intended use.

<i>iCMM Implementing Practices</i>	<i>CMMI Implementing Practices</i>
<p><i>PA 08 Evaluation</i></p> <p>BP 08.01 Establish and maintain a comprehensive strategy and requirements for evaluating products and services throughout their life cycle.</p> <p>BP 08.02 Develop the detailed procedures, methods, and processes to be used in evaluating products and services.</p> <p>BP 08.03 Establish and maintain the tools, facilities, personnel, documentation, and environment needed to perform planned evaluations.</p> <p>BP 08.04 Evaluate incremental work products and services.</p> <p>BP 08.05 Evaluate end-products and services against specified requirements.</p> <p>BP 08.06 Evaluate the capability of end-products and services to fulfill their intended use in representative operational environments.</p> <p>BP 08.07 Analyze results of evaluations and compare them to the needs and requirements to identify and quantify deficiencies, and recommend corrective and preventive actions.</p>	<p><i>Verification (VER)</i></p> <p>VER SP 1.1-1 Select the work products to be verified and the verification methods that will be used for each.</p> <p>VER SP 1.2-2 Establish and maintain the environment needed to support verification.</p> <p>VER SP 1.3-3 Establish and maintain verification procedures and criteria for the selected work products.</p> <p>VER SP 2.1-1 Prepare for peer reviews of selected work products.</p> <p>VER SP 2.2-1 Conduct peer reviews on selected work products and identify issues resulting from the peer review.</p> <p>VER SP 2.3-2 Analyze data about preparation, conduct, and results of the peer reviews.</p> <p>VER SP 3.1-1 Perform verification on the selected work products.</p> <p>VER SP 3.2-2 Analyze the results of all verification activities and identify corrective action.</p> <p><i>Validation (VAL)</i></p> <p>VAL SP 1.1-1 Select products and product components to be validated and the validation methods that will be</p>

AA 01: Safety and Security Application Area

<i>iCMM Implementing Practices</i>	<i>CMMI Implementing Practices</i>
<p><i>PA 19 Work Environment</i> BP 19.04 Maintain the required qualification of work environment components.</p>	<p>used for each. VAL SP 1.2-2 Establish and maintain the environment needed to support validation. VAL SP 1.3-3 Establish and maintain procedures and criteria for validation. VAL SP 2.1-1 Perform validation on the selected products and product components. VAL SP 2.2-1 Analyze the results of the validation activities and identify issues.</p> <p><i>Work Environment (WE)</i> WE SP1.4 Maintain the required qualification of work environment components.</p>

Typical Work Products

- safety or security evaluation strategy
- safety or security evaluation procedures
- safety or security evaluation report
- traceability from requirements to evaluation work products
- independent assessment report
- security test and evaluation plan
- security test and evaluation report
- safety test and evaluation plan
- safety test and evaluation report
- independent verification and validation test
- safety or security peer review results
- reports from auto-code checkers or compilers that use criteria from safe and secure style guides

Notes

Safety and security evaluations are performed in two different contexts. At the overall product or service level, objective evaluations (often by independent agents) are conducted to ascertain the safety and/or security level and/or posture (e.g., residual faults, hazards or vulnerabilities) of a product or service. Such evaluations are sometimes referred to as safety audits, security reviews, safety or security assessments, etc. Safety and security evaluations are also conducted throughout the life cycle to ensure that products and services, development work products, and components meet their safety and security requirements and needs for the intended operational use. The latter parallels classical verification and validation activities for any type of product or service.

Safety and security evaluations are carried out using methods appropriate to the safety and security level of the products and services being evaluated (see AP 01.09 and AP 01.10). When evaluating suppliers and supplier products, the same evaluations, requirements, and standards as for in-house development should be used. If this is not feasible, the level of residual risk should be determined and managed.

Safety and security evaluations should be planned concurrently with development and conducted by personnel and/or organizations with the needed competency and objectivity. “Objectivity” in conducting assurance evaluations means that the evaluations are conducted by persons not involved

AA 01: Safety and Security Application Area

in developing the solutions and who do not have a personal interest (absence of conflict of interest) in the outcome. Independent evaluators should perform evaluations when the required level of safety and security warrants. Selected standards (see AP 01.09) provide guidance on the recommended degree of independence under various conditions. Evaluators should not be pressured to acquiesce on safety or security issues. Outside or independent evaluators are often able to consider the design from a different perspective and identify problems that are not spotted by those involved in the design.

Work products that should undergo safety and security evaluations include requirements, designs, components, interfaces, assemblies, products, services, operating procedures, and assurance claims, as well as their supporting analyses and evidence. Evaluation pass/fail criteria should address input signals, sequences and their values; expected output signals, sequences and their values; and other acceptance criteria, such as memory usage, timing, and tolerances.

Documentation should be established and maintained for evaluation plans, strategy, procedures, failure resolution policies and procedures, and the results of evaluations, including evaluation activities; configurations; environment; functions evaluated; and tools and equipment, including calibration data, versions of requirements, specifications and procedures, discrepancies between expected and actual results, analysis of evaluation results, and recommendations for acceptance, qualified acceptance, or rejection.

The evaluation program should include appropriate levels of integration testing and ensure that, in addition to satisfactory performance of intended functions, no unintended functions are performed. Induced or simulated failures should be considered to demonstrate the acceptable safety and security performance of the equipment and software. It may be possible to reduce costs for safety and security testing through the use of engineering analyses, analogy, laboratory tests, functional mockups, or models and simulations. Where applicable, automatic testing tools and integrated development tools should be used.

AA 01: Safety and Security Application Area

AP 01.12 Establish Safety and Security Assurance Arguments

Establish and maintain safety and security assurance arguments and supporting evidence throughout the life cycle.

Description

An assurance argument is a set of structured assurance claims, supported by evidence and reasoning, that demonstrates how assurance needs have been satisfied. The documentation shows compliance with assurance objectives and provides an argument for the safety and security of the product or service. The arguments and supporting evidence are built and collected throughout the life cycle and are typically derived from multiple sources. These sources may include artifacts generated from several other application practices, as determined in the information management strategy and requirements (see AP 01.03).

Implementing Practices

There are no direct practices in either the iCMM or the CMMI that specifically address the development of an assurance argument, although many practices support the development of supporting evidence. Thus the organization should perform this practice as stated and additionally perform at least the following implementing practices in such a way as to establish and maintain safety and security assurance arguments and supporting evidence throughout the life cycle.

<i>iCMM Implementing Practices</i>	<i>CMMI Implementing Practices</i>
<i>PA 17 Information Management</i> BP 17.03 Collect, receive, and store information according to established strategy and procedures.	<i>PA 17 Information Management (from iCMM)</i> BP 17.03 Collect, receive, and store information according to established strategy and procedures.
<i>PA 08 Evaluation</i> BP 08.07 Analyze results of evaluations and compare them to the needs and requirements to identify and quantify deficiencies, and recommend corrective and preventive actions.	<i>Verification (VER)</i> VER SP 3.2-2 Analyze the results of all verification activities and identify corrective action.
<i>PA 15 Quality Assurance and Management</i> BP 15.04 Record and report the results of quality assurance activities to applicable stakeholders.	<i>Validation (VAL)</i> VAL SP 2.2-1 Analyze the results of the validation activities and identify issues.
	<i>Process and Product Quality Assurance (PPQA)</i> PPQA SP 2.2-1 Establish and maintain records of the quality assurance activities.

Note that additional evidence is likely to be collected as a result of performing other practices depending on the requirements for assurance arguments determined when performing AP01.03. These practices are identified in the *Notes* section on the next page.

Typical Work Products

- high-level safety and/or security assurance argument
- cross references to supporting evidence
- threat or hazard log
- threat or hazard records
- threat or hazard status summaries
- action requests and follow up

AA 01: Safety and Security Application Area

- safety case
- safety analysis report
- security certification and authorization package

Notes

An assurance argument typically consists of two parts – the main part which provides a coherent argument for the safety and security of the product or service and a set of supporting evidence. It can be advantageous to release the argument in stages throughout the project in order to gain early acceptance of the project safety and security approach. Also, for some products and services it may be helpful to produce multiple related documents that make up the overall assurance argument. The argument should be clear, consistent, complete, comprehensible (to all stakeholders), and defensible and should cover all stages of the life cycle. In order to ensure the argument is readable, supporting evidence can be cross-referenced from the main body of the argument.

Examples of assurance argument content include:

- a high level summary of the argument
- justification that the product or service is acceptably safe and secure
- rationale for claiming a specified level of safety and security
- relevant standards and regulatory requirements
- the configuration baseline
- identified hazards and threats and the residual risk of each hazard and threat
- operational and support assumptions

Typically, the supporting evidence will be the safety and security documentation that has been developed throughout the life cycle and may include plans, specifications, assessment and analysis reports, verification reports, and validation reports. Examples of supporting evidence may include:

- safety and security assurance objectives, level of confidence required, and acceptable risk levels (see AP 01.08, AP 01.09 and AP 01.10)
- strategy and plans for meeting assurance objectives (see AP 01.14)
- evidence of risk identification, analysis, mitigation and monitoring activities (see AP 01.06, AP 01.07 and AP 01.08)
- safety and security related requirements (see AP 01.10)
- safety and security related design decisions and features, along with the rationale for these decisions and features (see AP 01.10)
- evidence of assurance activities, including the results of safety and security assessments and evaluations through the life cycle (see AP 01.11), quality assurance activities (see AP 01.16), and evidence collected from the development environment (see AP 01.02) and the operational environment (see AP 01.04)
- recovery and contingency measures (see AP 01.05)
- certification and authorization statements (see AP 01.16)
- safety and security competency records (see AP01.01)

The evidence and processes used to create the argument are analyzed to ensure they address its intent (see AP 01.16).

AA 01: Safety and Security Application Area

The status of hazards or threats provides a good basis for monitoring and controlling progress against safety and security matters. Once a hazard or threat has been identified and documented, it should be tracked to closure. To effectively track a hazard or threat to closure, the status of each must be monitored regularly. The resulting hazard or threat records provide supporting evidence to the safety and security assurance argument (see AP 01.06, AP 01.07, and AP 01.08).

Example information to be logged is:

- a complete description of the hazard or threat
- who identified the hazard or threat and when
- consequences of the hazard or threat and their severity
- causes of the hazard or threat
- assessment of the risk associated with the hazard or threat
- how the hazard or threat will be detected, controlled, or mitigated
- safety and security requirements that are derived from the hazard or threat
- where the safety and security requirements are addressed in the design
- verification requirements that are derived from the safety and security requirements
- verification records or location of verification records
- cross-references to other documents (that may document the above)

An assurance argument can lose its value rapidly following product or service deployment unless it is maintained and improved during operation and maintenance. When maintenance activities are performed on the product or service, the assurance argument should be consulted and updated as necessary. Analysis of anomalies, incidents, and other data during operation may indicate the need for changes in the arguments. The evolving nature of the assurance argument during operation and maintenance may, in turn, require changes to the constraints under which the product or service is operated.

AA 01: Safety and Security Application Area

AP 01.13 Establish Independent Safety and Security Reporting

Establish and maintain independent reporting of safety and security status and issues.

Description

Establish and maintain an organization structure, assigned responsibilities, and resources that provide objective and timely reporting of safety and security status and issues. Establish reporting channels that ensure a level of objectivity or independence appropriate to the needed level of safety and security assurance. Establish and maintain visibility and accountability for all safety and security issues that are reported. Ensure that alerting and notification mechanisms are in place that allow appropriate response time for staff and external entities, e.g., fire departments, emergency rescue, and law enforcement.

Status includes the safety and security level achieved and progress towards meeting safety and security requirements. Issues include changes in hazards, threats and vulnerabilities, accidents, possible security compromises, and related investigations.

Implementing Practices

This application practice is implemented by performing the following practices in such a way as to establish and maintain independent reporting of safety and security status and issues.

<i>iCMM Implementing Practices</i>	<i>CMMI Implementing Practices</i>
<p><i>PA 00 Integrated Enterprise Management</i> BP 00.01 Establish, maintain, and communicate a strategic vision that identifies long-term goals, values, performance expectations, and core activities. BP 00.02 Align the enterprise to operate efficiently and consistently to achieve the vision.</p> <p><i>PA 11 Project Management</i> BP 11.08 Identify individuals or teams that will be assigned the resources and responsibilities for meeting project objectives. BP 11.09 Communicate project plans, direction, corrective actions, and status, and coordinate project activities.</p> <p><i>PA 15 Quality Assurance and Management</i> BP 15.04 Record and report the results of quality assurance activities to applicable stakeholders.</p>	<p><i>Organizational Environment for Integration (OEI)</i> OEI SP1.1 Establish and maintain a shared vision for the organization.</p> <p><i>Integrated Project Management (IPM)</i> IPM SP 4.1-1 Determine the integrated team structure that will best meet the project objectives and constraints.</p> <p><i>Process and Product Quality Assurance (PPQA)</i> PPQA SP 2.1-1 Communicate quality issues and ensure resolution of noncompliance issues with the staff and managers.</p>

Typical Work Products

- organization charts indicating safety and security responsibilities
- safety and security policies that address status and issue reporting
- safety and security policies that address required levels of independence
- safety and security plans and procedures that assign safety and security responsibilities and resources
- issue tracking system
- briefings and other communications to staff on safety and security reporting responsibilities and assignments

AA 01: Safety and Security Application Area

Notes

Top level management commitment to accurate, open, and objective reporting of safety and security status and issues is crucial to achieving needed levels of safety and security in products, services, and the work environment. Effective communication channels will ensure the commitment flows down to managers, supervisors and staff. Realization of the commitment to safety and security is achieved through the establishment of responsibility for issue and status reporting and for accountability of action on the substance of issues and reports. Specific responsibilities are assigned to individuals and groups and broad responsibilities are assigned to all staff. In order to achieve effective results, responsibilities for safety and security reporting must be empowered by the absence of conflict of interest. Additionally, management should strive to eliminate any reluctance of staff to report safety issues due to concerns of personal retribution. In situations where conflict of interest could exist, the reality and perception are eliminated by assigning the safety and security reporting function to an independent entity. The needed level of independence should be determined based on possible consequences and safety and security level requirements.

A climate of objectivity and non-attribution is important for ensuring that staff in a safety or security role are not put under unreasonable pressure to acquiesce on safety or security issues. Often independent persons or organizations are required due to the criticality of the needed safety and security level and/or the pressures of project cost and schedule or staff performance. An additional benefit that may accrue from using independent staff in reviews, verification, validation, or assessment is consideration of designs from a fresh perspective that could reveal problems that might not be spotted by those who are closer to the design.

The effectiveness of those formally assigned to safety and security reporting requires that they have the needed skill and knowledge, access to products and services, access to management, authority, and reasonable scope of assigned coverage.

Planning for independent safety and security reporting (see AP 01.14) should identify responsibilities for safety and security reporting and issues management, required levels of objectivity and/or independence, documentation and preservation of issues and reports, and how reporting and information dissemination will be coordinated throughout an organization (including customers and suppliers). Planning should also establish reporting systems and procedures for investigation and disposition of hazards, accidents, mishaps, and safety and security incidents.

Specialized roles, assignments, and titles are often assigned in connection with responsibilities for safety and security reporting, such as Management Security Forum, Safety and Security Committee, Project Safety Engineer, Project Safety Committee, Security Team, Independent Safety Auditor, accident board, etc.

AA 01: Safety and Security Application Area

AP 0 1.14 Establish a Safety and Security Plan

Establish and maintain a plan to achieve safety and security requirements and objectives.

Description

The safety and security plan establishes the objectives, activities, resources, and responsibilities for safety and security throughout the product or service life cycle, including development, deployment, operation, and disposal.

The plan suits the type of product or service and defines safety and security activities that are integrated and carried out in conjunction with other design, development, production, operation, and quality control functions. It covers safety and security verification, validation, and independent assessment activities, such as audits. Planning includes obtaining commitment to the plan in terms of resource requirements and participant involvement.

Implementing Practices

This application practice is implemented by performing the following practices in such a way as to establish and maintain a plan to achieve safety and security requirements and objectives.

<i>iCMM Implementing Practices</i>	<i>CMMI Implementing Practices</i>
<p><i>PA 00 Integrated Enterprise Management</i> BP 00.04 Establish, integrate, and deploy tactical action plans to accomplish strategic objectives.</p> <p><i>PA 11 Project Management</i> BP 11.01 Define project objectives, scope, and the work products and services that are to be provided by the project. BP 11.02 Define the activities needed to achieve project outputs and the life-cycle approach that will be used. BP 11.03 Estimate and document the work product and task planning parameters that provide a basis for resource estimates. BP 11.04 Estimate the project effort, cost, and other resource requirements. BP 11.05 Develop management and technical schedules for the project. BP 11.06 Establish and maintain a complete set of plans for providing the products and services throughout the project life cycle. BP 11.07 Establish and maintain commitment of affected groups and individuals to project objectives and plans, and commitment of resources as identified in the plan. BP 11.08 Identify individuals or teams that will be assigned the resources and responsibilities for meeting project objectives. BP 11.09 Communicate project plans, direction, corrective actions, and status, and coordinate project activities.</p>	<p><i>Organizational Innovation and Deployment (OID)</i> OID 2.1-1 Establish and maintain the plans for deploying the selected process and technology improvements.</p> <p><i>Quantitative Project Management (QPM)</i> QPM SP 1.1-1 Establish and maintain the project's quality and process-performance objectives.</p> <p><i>Project Planning (PP)</i> PP SP 1.1-1 Establish a top-level work breakdown structure (WBS) to estimate the scope of the project. PP SP 1.2-1 Establish and maintain estimates of the attributes of the work products and tasks. PP SP 1.3-1 Define the project life-cycle phases upon which to scope the planning effort. PP SP 1.4-1 Estimate the project effort and cost for the work products and tasks based on estimation rationale. PP SP 2.1-1 Establish and maintain the project's budget and schedule. PP SP 2.2-1 Identify and analyze project risks. PP SP 2.3-1 Plan for the management of project data. PP SP 2.4-1 Plan for necessary resources to perform the project. PP SP 2.5-1 Plan for knowledge and skills needed to perform the project. PP SP 2.6-1 Plan the involvement of identified stakeholders. PP SP 2.7-1 Establish and maintain the overall project plan content. PP SP 3.1-1 Review all plans that affect the project to understand project commitments.</p>

AA 01: Safety and Security Application Area

<i>PA 13 Risk Management</i> BP 13.01 Establish and maintain an approach for managing risk that is the basis for identifying, assessing, mitigating, and monitoring risks for the life of the project.	PP SP 3.2-1 Reconcile the project plan to reflect available and estimated resources. PP SP 3.3-1 Obtain commitment from relevant stakeholders responsible for performing and supporting plan execution.
<i>PA 16 Configuration Management</i> BP 16.01 Establish roles, responsibilities, and methods for the application of CM activities.	<i>Risk Management (RSKM)</i> RSKM SP 1.3-1 Establish and maintain the strategy to be used for risk management.

Typical Work Products

- safety and/or security strategy
- safety and/or security plan
- independent safety and/or security assessment plan
- skills and experience matrix

Notes

Many standards specify particular methods and techniques that are considered to be suitable for safety and security related work. The methods and techniques may vary according to the complexity and/or safety and security level of the product or service being developed (see AP 01.09). These issues should be considered in safety and security planning and resources should be allocated to provide safety and security assurance commensurate with required levels of safety and security.

A safety and/or security plan generally addresses:

- scope of the work and work products to be developed
- life cycle
- goals and objectives to be measured
- cost, schedule, and resource estimates
- safety and/or security analysis activities, integrated with product or service development, deployment, operation, and disposal activities
- risk assessment procedures and analysis techniques
- risk tracking and resolution procedures, including mitigation, review, and acceptance procedures
- plans for supporting activities such as product and service evaluations, configuration management, quality management, etc.
- roles and responsibilities for identified activities
- stakeholder involvement

Safety and security needs should be considered and reflected in plans throughout the life cycle.

Relevant stakeholder acceptance of the safety and security plans and the product or service should be sought at key points in the life cycle. In order to reduce the risk of major acceptance problems arising late in the life cycle, plans should aim to obtain staged acceptance as the project progresses. The planning should document the key stages of acceptance, what will be delivered for assessment, and who will provide acceptance at each stage.

AA 01: Safety and Security Application Area

Planning includes ensuring commitment to the plan. This entails ensuring allocation of adequate resources and obtaining the commitment of participants and stakeholders.

For safety and security related activities it is particularly important that staff have adequate experience, training, and skills. In certain domains this can also include licensing schemes that ensure staff are licensed before they undertake unsupervised critical work. Planning should address competency requirements in terms of expected qualifications, skills, and years of experience, training requirements where there are shortfalls against the competency requirements, and recruitment requirements where it is not possible to train existing staff to the required competency.

The plan should establish reporting and corrective action procedures for disposition of reported incidents and test failures.

AA 01: Safety and Security Application Area

AP 01.15 Select and Manage Suppliers, Products, and Services

Select and manage suppliers, products, and services using safety and security criteria.

Description

Analyze needs to acquire safety and security related products and services and select suppliers. Establish supplier agreements that identify safety and security requirements, including required levels of safety and security. Ensure that safety and security assurance is delivered with the product or service.

Implementing Practices

This application practice is implemented by performing the following practices in such a way as to select and manage suppliers, products, and services using safety and security criteria.

<i>iCMM Implementing Practices</i>	<i>CMMI Implementing Practices</i>
<p><i>PA 05 Outsourcing</i> BP 05.01 Identify needed solution or process components that may be provided by other/outside organizations. BP 05.02 Identify suppliers that have shown expertise or capability in the identified areas. BP 05.03 Prepare for the solicitation/tasking and the selection of a supplier, including objective review of estimates of cost for the services/products to be outsourced, a clear description of tasking, and inclusion of evaluation criteria in the solicitation/tasking package. BP 05.04 Choose suppliers in accordance with the selection strategy and criteria. BP 05.05 Establish and maintain communication with suppliers emphasizing the needs, expectations, and measures of effectiveness held by the acquirer for the solution or process components that are being acquired.</p> <p><i>PA 12 Supplier Agreement Management</i> BP 12.01 Ensure the supplier adheres to acquirer-approved planning documents. BP 12.02 Review and monitor supplier activities through periodic, formal reviews and informal, technical issue interchanges with the supplier, and by quantitative means to continuously determine agreement outcomes versus plans and requirements. BP 12.03 Ensure agreements comply with current laws, policies and regulations, and incorporate necessary and approved changes into the agreement. BP 12.04 Monitor supplier's quality assurance, configuration management, test, corrective action and risk management systems, plans and process activities, results, and products. BP 12.05 Perform activities to foster a partnership between the acquiring organization and the supplier. BP 12.06 Analyze and direct the performance of agreement activities. BP 12.07 Ensure the agreement is being maintained and followed, and all changes and records are properly</p>	<p><i>Supplier Agreement Management (SAM)</i> SAM SP 1.1-1 Determine the type of acquisition for each product or product component to be acquired. SAM SP 1.2-1 Select suppliers based on an evaluation of their ability to meet the specified requirements and established criteria. SAM SP 1.3-1 Establish and maintain formal agreements with the supplier. SAM SP 2.1-1 Review candidate COTS products to ensure they satisfy the specified requirements that are covered under a supplier agreement. SAM SP 2.2-1 Perform activities with the supplier as specified in the supplier agreement. SAM SP 2.3-1 Ensure that the supplier agreement is satisfied before accepting the acquired product. SAM SP 2.4-1 Transition the acquired products from the supplier to the project.</p> <p><i>Integrated Supplier Management (ISM)</i> ISM SP 1.1-1 Identify and analyze potential sources of products that may be used to satisfy the project's requirements. ISM SP 1.2-1 Use a formal evaluation process to determine which sources of custom-made and off-the-shelf products to use. ISM SP 2.1-1 Monitor and analyze selected processes used by the supplier. ISM SP 2.2-1 For custom-made products, evaluate selected supplier work products. ISM SP 2.3-1 Revise the supplier agreement or relationship, as appropriate, to reflect changes in conditions.</p> <p><i>PA 09 Deployment, Transition, and Disposal(from iCMM)</i> BP 09.05 Transfer the product or service to the customer/stakeholder operation and support organizations.</p>

AA 01: Safety and Security Application Area

<i>iCMM Implementing Practices</i>	<i>CMMI Implementing Practices</i>
processed, controlled and maintained. BP 12.08 Determine whether to accept the supplier's product or service, based on acceptance conditions stipulated in the agreement. <i>PA 09 Deployment, Transition, and Disposal</i> BP 09.05 Transfer the product or service to the customer/stakeholder operation and support organizations.	

Typical Work Products

- supplier selection plan with safety and security criteria
- supplier agreements that include safety and security requirements
- outsourcing plans or agreements that reflect safety and security obligation of providers and suppliers
- subcontract management plan
- product or service requirements (with safety/security annotations)
- minutes of supplier reviews
- audits of supplier records
- records documenting suppliers, including subcontractors, in supply chains contributing to products or services used or delivered

Notes

Ensure that all products and services that will be acquired are assessed to establish whether or not they are safety or security related. In general, the acquirer should assume that all products and services that will be acquired are safety or security related unless it is proven otherwise. Suppliers should be assessed to ensure they have appropriate processes, skills and experience for supplying safety or security related products and services. Suppliers should be selected based on criteria that include ones addressing safety and security.

Establish an agreement with the supplier that includes relevant safety and security requirements. The agreement should cover areas such as the following:

- how the supplier will interact with the acquirer on safety or security matters (e.g., lines of communication for safety or security matters)
- provisions that ensure the supplier satisfies legal obligations associated with safety and security
- the commitment of both the acquirer and the supplier to participate in the ongoing safety and security activities (e.g., through participation in a safety and security working group)
- the need to deliver an assurance argument as part of the safety or security related product or service
- the use of development and evaluation methods appropriate to required levels of safety and security
- allowance for the monitoring activities that are necessary

Procedures should be in place to monitor progress and performance of safety and security related suppliers, e.g., regular progress reviews and/or audits examining safety and security related

AA 01: Safety and Security Application Area

activities. Establish mechanisms for acquirer-supplier collaboration, such as joint working groups to address safety and security issues.

The acquirer should ensure that suitable safety and security assurance is delivered with any product provided as part of the agreement (e.g., in the form of a safety or security assurance argument).

Establish requirements traceability between the acquirer and the supplier. In general, the majority of safety and security requirements flow from the acquirer to the supplier. Assumptions made by either party may need to be vetted to check their validity. Safety and security analyses of the supplier may need to be constructed and used in the context of wider safety and security analyses performed by the acquirer. Other issues requiring traceability include schedules, competencies, and other support practices.

Special consideration should be given where off-the-shelf products are acquired. Example considerations that are important when acquiring off-the-shelf products are:

- transfer of existing safety and security assurance of the product into a suitable form for the acquirer
- the operational history of the product
- ensuring compatibility with the original environment of a product when transferring assurance or using operational histories
- accurate identification of the configuration or version of products
- ensuring any transferred assurance or operational history applies to the version of the product supplied
- identifying and analyzing unspecified functionality of products
- ongoing support of the product
- a safety and security assurance argument for the product
- responsiveness in product updates to meet changing safety or security threats, hazards, and vulnerabilities
- supply chain awareness – those organizations and individuals involved in producing all parts of the product or providing the service, including the parts that are outsourced or sub-contracted.

AA 01: Safety and Security Application Area

AP 01.16 Monitor and Control Activities and Products

Measure, monitor, and review safety and security activities against plans, control products, take corrective action, and improve processes throughout the life cycle.

Description

Measure, monitor, and review development, operation, and service activities against policies, plans, and procedures. Report deviations and initiate corrective actions to ensure adherence to safety and security program requirements throughout the product and service life cycle.

Ensure that proposed changes to policies, procedures, plans, products, and services are subjected to safety and security impact analyses and that approved changes are recorded and reported. Review and audit configuration management procedures and activities to prevent accidental or unauthorized modifications of controlled products. Recommend corrective and preventive actions relating to safety and security.

Establish and pursue quality goals and safety and security process improvement goals based on mission and business objectives. Establish and use measures that reflect the degree of achievement of quality objectives and the effectiveness of safety and security processes and procedures. Use the results of measurements to identify and implement needed improvements.

Implementing Practices

This application practice is implemented by performing the following practices in such a way as to measure, monitor, and review safety and security activities against plans, control products, take corrective action, and improve processes throughout the life cycle.

<i>iCMM Implementing Practices</i>	<i>CMMI Implementing Practices</i>
<p><i>PA 16 Configuration Management</i> BP 16.02 Identify configuration items, interim work products, and work environment items that will be baselined or placed under version control, and baseline them. BP 16.03 Establish and maintain a repository to house work product baselines. BP 16.04 Control changes to baselined work products through tracking, recording, review, and approval processes throughout the life cycle. BP 16.05 Record and report change information about the baselined configuration items. BP 16.06 Conduct configuration audits and inspections to verify integrity of the baselines and check the work products for compliance with the baselines.</p> <p><i>PA 02 Requirements</i> BP 02.08 Analyze all requirements change requests for impact on the product or service and, upon approval, incorporate the approved changes into the requirements baseline. BP 02.07 Record, approve, baseline, and place under change control all requirements, derived</p>	<p><i>Configuration Management (CM)</i> CM SP 1.1-1 Identify the configuration items, components, and related work products that will be placed under configuration management. CM SP 1.2-1 Establish and maintain a configuration management and change management system for controlling work products. CM SP 1.3-1 Create or release baselines for internal use and for delivery to the customer. CM SP 2.1-1 Track change requests for the configuration items. CM SP 2.2-1 Control changes to the configuration items. CM SP 3.1-1 Establish and maintain records describing configuration items. CM SP 3.2-1 Perform configuration audits to maintain integrity of the configuration baselines.</p> <p><i>Requirements Management (RM)</i> RM SP 1.3-1 Manage changes to the requirements as they evolve during the project.</p> <p><i>Process and Product Quality Assurance (PPQA)</i> PPQA SP 1.1-1 Objectively evaluate the designated performed processes against the applicable process</p>

AA 01: Safety and Security Application Area

<i>iCMM Implementing Practices</i>	<i>CMMI Implementing Practices</i>
<p>requirements, derivation rationale, traceability, and requirements status.</p> <p><i>PA 15 Quality Assurance and Management</i> BP 15.01 Establish, document, implement, and maintain a quality management system. BP 15.02 Objectively monitor compliance of performed activities with the established processes throughout the life cycle. BP 15.03 Objectively measure work products and services against the requirements and standards that define them. BP 15.04 Record and report the results of quality assurance activities to applicable stakeholders. BP 15.05 Analyze quality records and measurements to detect the need for corrective action and develop recommendations for quality improvement or corrective and preventive actions. BP 15.06 Initiate activities that address identified quality issues or quality improvement opportunities. BP 15.07 Evaluate the effect of changes after they have been implemented.</p> <p><i>PA 00 Integrated Enterprise Management</i> BP 00.05 Review performance relative to goals and changing needs across the enterprise. BP 00.06 Translate performance review findings into action.</p> <p><i>PA 11 Project Management</i> BP 11.10 Monitor and track project activities and results against plans. BP 11.11 Conduct formal and informal reviews of project performance and analyze variances from plans. BP 11.12 Take corrective actions to address problems.</p> <p><i>PA 18 Measurement and Analysis</i> BP 18.01 Establish measurable objectives from issues and goals and identify the specific measures that will provide the basis for performance analysis. BP 18.02 Collect and verify measurement data and generate results. BP 18.03 Store measurement data and results in a repository. BP 18.04 Analyze data to determine performance against goals. BP 18.05 Report results of measurement and analysis to all affected stakeholders.</p> <p><i>PA 21 Process Improvement</i> BP 21.01 Identify process improvement goals from the organization's business goals.</p>	<p>descriptions, standards, and procedures. PPQA SP 1.2-1 Objectively evaluate the designated work products and services against the applicable process descriptions, standards, and procedures. PPQA SP 2.1-1 Communicate quality issues and ensure resolution of noncompliance issues with the staff and managers. PPQA SP 2.2-1 Establish and maintain records of the quality assurance activities.</p> <p><i>Organizational Innovation and Deployment (OID)</i> OID 2.2-1 Manage the deployment of the selected process and technology improvements. OID 2.3-1 Measure the effects of the deployed process and technology improvements.</p> <p><i>Project Monitoring and Control (PMC)</i> PMC SP 1.1-1 Monitor the actual values of the project planning parameters against the project plan. PMC SP 1.2-1 Monitor commitments against those identified in the project plan. PMC SP 1.3-1 Monitor risks against those identified in the project plan. PMC SP 1.4-1 Monitor the management of project data against the project plan. PMC SP 1.5-1 Monitor stakeholder involvement against the project plan. PMC SP 1.6-1 Periodically review the project's progress, performance, and issues. PMC SP 1.7-1 Review the accomplishments and results of the project at selected project milestones. PMC SP 2.1-1 Collect and analyze the issues and determine the corrective actions necessary to address the issues. PMC SP 2.2-1 Take corrective action on identified issues. PMC SP 2.3-1 Manage corrective actions to closure.</p> <p><i>Measurement and Analysis (MA)</i> MA SP 1.1-1 Establish and maintain measurement objectives that are derived from identified information needs and objectives. MA SP 1.2-1 Specify measures to address the measurement objectives. MA SP 1.3-1 Specify how measurement data will be obtained and stored. MA SP 1.4-1 Specify how measurement data will be analyzed and reported. MA SP 2.1-1 Obtain specified measurement data. MA SP 2.2-1 Analyze and interpret measurement data. MA SP 2.3-1 Manage and store measurement data, measurement specifications, and analysis results. MA SP 2.4-1 Report results of measurement and analysis activities to all relevant stakeholders.</p>

AA 01: Safety and Security Application Area

<i>iCMM Implementing Practices</i>	<i>CMMI Implementing Practices</i>
BP 21.02 Plan improvements to the project/organization's processes based on widespread participation and analysis of the impact of potential improvements on achieving the goals of the organization. BP 21.03 Appraise the processes periodically. BP 21.04 Analyze appraisal results and other sources for improvement and establish an action plan for process improvement. BP 21.05 Implement the process improvement action plan. BP 21.06 Confirm that improvement activities meet goals and desired results. BP 21.07 Sustain and deploy improvement gains across all applicable parts of the organization/project. BP 21.08 Continuously monitor and improve process performance.	<i>Organizational Process Focus (OPF)</i> OPF SP 1.1-1 Establish and maintain the description of the process needs and objectives for the organization. OPF SP 1.2-1 Appraise the processes of the organization periodically and as needed to maintain an understanding of their strengths and weaknesses. OPF SP 1.3-1 Identify improvements to the organization's processes and process assets. OPF SP 2.1-1 Establish and maintain process action plans to address improvements to the organization's processes and process assets. OPF SP 2.2-1 Implement process action plans across the organization. OPF SP 2.3-1 Deploy organizational process assets across the organization. OPF SP 2.4-1 Incorporate process-related work products, measures, and improvement information derived from planning and performing the process into the organizational process assets.

Typical Work Products

- safety and security compliance audits
- schedule variance for safety and security activities
- safety or security non-conformance report
- safety and/or security configuration management audit
- safety and/or security change request
- safety and/or security change impact analysis
- safety and/or security policy, procedure, process, or product change order
- recommendation of safety or security corrective and/or preventive action
- operational error deviation report
- safety trend report
- safety and security process improvement recommendations
- lessons learned
- announcements, bulletins, and/or training that addresses changes in safety or security policies and procedures

Notes

Audit requirements and activities involving checks on operational systems should be carefully planned and coordinated in order to minimize the risk of disruptions to mission operations or business processes. Planning for audits should include coordination with management, agreement and control of scope of audits, ensuring availability of information technology resources for performing checks, monitoring and logging of access, documentation of procedures and responsibilities, and reporting of results.

All proposed product changes, including changes to non-safety and security requirements, design, and components, should undergo safety and security impact analyses. Approved changes that have an impact on safety or security should be returned to the appropriate phase of the life cycle and all subsequent phases repeated for the changes. Information with safety and/or security implications

AA 01: Safety and Security Application Area

should be disseminated widely and should be clear, concise, and easy to read. Information can be disseminated by means of formal reports to management and by safety newsletters, bulletins, and seminars for all staff. Changes in policies and procedures should be supported by appropriate training.

Safety and security programs, systems, policies, and procedures should be checked for compliance with laws, regulations, and standards (see AP 01.09) on an appropriate schedule. Technical compliance checking can be done through examination or audits of operational systems to ensure that hardware and software controls have been correctly implemented. This type of compliance checking may require expert technical assistance. It should be performed manually (supported by appropriate software tools, if necessary) by an experienced system engineer or by an automated software package that generates a technical report for subsequent interpretation by a technical specialist.

AA 01: Safety and Security Application Area

Glossary

Term or Phrase	Definition	Source
Assurance Argument	A set of structured assurance claims, supported by evidence and reasoning, that demonstrate clearly how assurance needs have been satisfied	SSE-CMM
Assurance Claim	An assertion or supporting assertion that a system meets a safety or security need. Claims address both direct threats (e.g., system data are protected from attacks by outsiders) and indirect threats (e.g., system code has minimal flaws)	Adapted from SSE-CMM
Causal Factor	Root cause. An act, omission, condition, or circumstance that either starts or sustains an accident sequence or a security compromise. A causal factor may be related to hardware, software, human, and/or the environment. A given act, omission, condition, or circumstance is a causal factor if correcting, eliminating, or avoiding it would prevent the accident or security compromise or mitigate damage or injury	Adapted from United States Department of Agriculture - Thirty Mile Fire Investigation
Common Cause Failure	Failure, which is the result of one or more events, causing coincident failures of two or more separate channels in a multiple channel system, leading to system failure	IEC 61508
Dependent Failure	Failure whose probability cannot be expressed as the simple product of the unconditional probabilities of the individual events which caused it	IEC 61508
Diagnostic Coverage	Fractional decrease in the probability of dangerous hardware failure resulting from the operation of the automatic diagnostic tests	IEC 61508
Functional Safety Assessment	Investigation, based on evidence, to judge the functional safety achieved by one or more E/E/PE safety-related systems, other technology safety-related systems or external risk reduction facilities	IEC 61508
Hazard	Condition that is a potential source of harm	IEC 61508
Hazard Probability	The aggregate probability of occurrence of the individual events that create a specific hazard	MIL-STD-882C
Integrity	Freedom from flaw or corruption	Synthesized by the Safety and Security Assurance project from multiple sources
Residual Risk	Risk remaining after protective measures have been taken	IEC 61508
Risk	(1) an estimate of the probability of occurrence and the severity of consequences if the loss, harm, or other adverse consequences occur (2) a general statement of the consequences of an adverse event	Synthesis of definitions of risk from: IEC 61508, DEF-STAN-0056, MIL-STD-882C, NIST 800-30, SSE-CMM, and others
Risk Assessment (security)	The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact; part of risk management and synonymous with risk analysis	NIST 800-30

AA 01: Safety and Security Application Area

Term or Phrase	Definition	Source
Safety	Freedom from unacceptable risk of harm to personnel or equipment	Adaptation from IEC 61508
Safety and/or Security Level	An expression of trust that a product or service will perform as expected; designation of one of a possible range of values indicating the extent to which the safety or security risks associated with a product or service have been contained.	Adaptation from ISO 15026
Safety Integrity	Probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time	IEC 61508
Safety Integrity Level	An indicator of the required level of safety integrity	DEF-STAN-0056
Safety Target	A numerical expression of the policy on the tolerability of risks from a system, giving for each identified accident its highest tolerable probability for each group of people who may be harmed by it	DEF-STAN-0056
Security	The combination of confidentiality, integrity, and availability that is intended to protect products, services, and people from harm	Synthesized from NIST 800-30 and other sources
Security Policy	Rules, directives and practices that govern how assets, including sensitive information, are managed, protected and distributed within an organization and its systems	SSE-CMM
Signature Authority	Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk	SSE-CMM
System Safety	The characteristic of a product or service that indicates an acceptable degree of freedom from harm or potential harm	Synthesized from MIL-STD-882C and other sources
Systematic Failure	Failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors	IEC 61508
Threat	An entity with potential to cause harm to an organization, person, product, or service (includes persons, organizations, governments, and environmental phenomena, such as storms)	Synthesized by the Safety and Security Assurance project from multiple sources
Threat Analysis	The examination of threat-sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment	NIST 800-30
Vulnerability	A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy	NIST 800-30

Note:

- (1) Definitions are from the sources that were used to develop the application area, where available.
- (2) Terms that are in the iCMM or CMMI are not included.

Work Environment

Process Area Summary

Purpose

The purpose of the Work Environment process area is to ensure that people have infrastructure and working procedures to perform their work effectively.

Major points addressed

The work environment process area emphasizes maintaining a work environment that meets the needs of stakeholders and whose availability is assured under normal, as well as adverse, conditions. This involves determining work environment needs and requirements, establishing a description of work environment standards adopted for use in the organization, and ensuring that the work environment is established and maintained to meet current and evolving needs. People are trained and qualified to use the work environment, tools and equipment are appropriately qualified and certified, new technology is inserted as appropriate, and work environment continuity is assured.

Goal

- 1. A work environment that meets stakeholder needs and requirements is established and maintained. (*all practices*)**

Practices*

Practice 01 Determine Work Environment Needs

Establish and maintain the needs and requirements to implement, operate, and sustain work environments.

Practice 02 Establish Work Environment Standards

Establish and maintain a description of work environment standards and tailoring guidelines that meet identified needs and requirements.

Practice 03 Establish Work Environment

Establish and maintain a work environment, tailored from the work environment standards, to meet the specific needs.

Practice 04 Maintain the Qualification of Components

Maintain the required qualification of work environment components.

Practice 05 Maintain the Qualification of Personnel

Ensure that personnel have the required competencies and qualifications to access, use, and maintain the work environment.

Practice 06 Maintain Technology Awareness

Monitor, evaluate, and insert, as appropriate, new technology for improving the work environment.

Practice 07 Ensure Work Environment Continuity

Plan and provide for continuity of the work environment.

*(*For iCMM, Work Environment would be PA 19 and practices would be base practices numbered BP 19.01, BP 19.02, etc. For CMMI, practices would be numbered WE SP1.1, WE SP1.2, etc., as specific practices of the Work Environment (WE) process area.)*

Work Environment Process Area

Notes

The work environment is sometimes called the support environment or the infrastructure. It is the work environment for both development and operations and may include facilities, tools, equipment, computing resources, communications systems, techniques, standards, workspace, laboratories, procedures, office equipment, and supplies. The work environment should include appropriate procedures for operation, safety, and security. Work environment stakeholders include workers, organization and enterprise management, and customers. Work environments should be established and maintained according to appropriate standards that address the full life cycle for creation, operation, improvement, sustainment, and disposal.

Relationships between this PA and other PAs

All of the other process areas are employed at the appropriate life cycle phase to establish, operate, and maintain the work environment. The work environment is used by people to perform the activities of other process areas in order to achieve enterprise objectives for products and services. The Risk Management PA is key for assuring the continuity of the work environment and ultimately the continuity of the enterprise.

Work Environment Process Area

Practice 01 Determine Work Environment Needs

Establish and maintain the needs and requirements to implement, operate, and sustain work environments.

Description

Obtain stakeholder needs and determine the work environment requirements appropriate to the business. Consider relevant regulations, laws, policies, and standards when developing needs and requirements. Address an appropriate breadth of needs, including initial cost, cost to sustain, productivity, reliability, availability, performance, safety, and security in determining the work environment requirements. Validate and maintain the work environment requirements to guide current work environments and future migrations in order to stay current with stakeholder needs.

Typical Work Products

- identified work environment regulations and laws
- identified work environment stakeholders
- stakeholder needs
- work environment needs and requirements
- requirements for safety, security, and human factors
- requirements for failure and disaster recovery
- work environment performance and effectiveness measures

Notes

Stakeholders include workers, management, and customers. Retain information on identified stakeholders and specific users that are sources of needs and requirements. Include needs, requirements, and applicable laws and regulations regarding disadvantaged and/or handicapped stakeholders.

Work environment needs and requirements are based on what is needed to develop, maintain, and deliver products and services, including facilities, tools, equipment, computing resources, transportation, utilities, communications systems, techniques, workspace, office equipment, and supplies. Requirements may address a required level of automation, e.g., the level of configuration management automation. Determine or examine the types of products or product lines that the work environment needs to address. Consider needs for both co-located and distributed teams, as well as needs for work environment support services such as hotlines or help desks. Identify any cost or schedule constraints.

Include needs and requirements related to maintaining the safety and security of the work environment. Identify characteristics of the physical environment that could be important for performance including noise, air quality, space, and illumination. Identify measures associated with work environment performance and effectiveness and their target values.

Work Environment Process Area

See requirements-related process areas for further information on determining needs and requirements (PA 01 Needs and PA 02 Requirements in the iCMM; Requirements Development and Requirements Management process areas in CMMI).

Work Environment Process Area

Practice 02 Establish Work Environment Standards

Establish and maintain a description of work environment standards and tailoring guidelines that meet identified needs and requirements.

Description

Establish work environment standards that allow the organization and/or projects to benefit from commonality in tools, training, and maintenance, as well as cost savings from volume purchases. Work environment standards should address the needs of all stakeholders and consider productivity, cost, availability, security, and workplace health, safety, and ergonomic factors. Work environment standards include guidelines for tailoring and/or waivers that allow adaptation of the work environment to meet specific needs.

Typical Work Products

- organizational infrastructure work environment specification
- standard workstation hardware and software
- standard application software
- standard calibration equipment
- standard production equipment
- project specific work environment specifications for similar projects
- tailoring guidelines for specific project applications
- process for requesting and approving tailoring or waivers
- traceability of the work environment specification(s) to established standards

Notes

These standards are those adopted for use in the organization.

Work Environment Process Area

Practice 03 Establish Work Environment

Establish and maintain a work environment, tailored from the work environment standards, to meet the specific needs.

Description

An appropriate work environment is based on requirements and work environment standards; it comprises an infrastructure of facilities, tools and equipment that people need to perform their jobs effectively in support of mission objectives. The work environment and its components are maintained at a level of performance and reliability indicated by the work environment requirements.

Typical Work Products

- office equipment and furniture
- workspace, including individual workspace, conference rooms, meeting spaces, training areas, and laboratories
- human environment controls (temperature, humidity, lighting, noise, and visual distraction)
- equipment environment controls
- communications equipment for personnel, such as telephones, facsimile machines, modems, and electronic mail facilities
- procedures for operation, safety, and security
- computers, workstations, or other computing equipment
- network infrastructure
- equipment and tools, such as office software, decision support software, project management tools, requirements management tools, design tools, configuration management tools, evaluation tools, test and/or evaluation equipment, production tools, and shipping and receiving equipment and tools
- operating and maintenance manuals
- maintenance records
- maintenance and trouble shooting procedures
- user surveys and results
- usage and performance levels
- work environment support services

Notes

The work environment is established upon appropriate authorization, and the total work environment represents the needs of the organization as a whole. An individual project, however, may have unique needs for selected elements of this environment. In this case, tailoring can allow the project to operate more efficiently. For example, project A does not involve signal processing, so signal processing automation tools are tailored out of (i.e., not provided to) this project's automation tool set. Conversely, project B is the only project in the organization that has a need for automated requirements tracing, so the appropriate tools are tailored into (i.e., provided in addition to) this project's automated tool set.

Work Environment Process Area

Work environment components can be developed in house or acquired from external sources. Similarly, maintenance and support of the work environment can be performed internally or outsourced. Perform cost-benefit analysis to support make-buy decisions.

Maintain identification, location, and inventory of work environment assets (tools, equipment, data, and information).

Establish the work environment in time for its use in relevant activities. Collect and analyze data on work environment usage and performance. Monitor and evaluate the effectiveness of the work environment in meeting user needs. Surveying end users is a useful way to determine adequacy of the work environment and to identify potential improvements.

In case of computer/software security incidents, ensure protection of the state of programs and media.

Maintain the work environment, including correcting defects, improving performance, and modifying the environment to keep up with changing needs. Upgrade or add components, as appropriate, after piloting their effectiveness and retire or dispose of components that are no longer needed. Consider all services being supported and attempt to optimize overall performance and maximize integration of tools within the environment.

When disposing of work environment components, ensure that devices containing sensitive information are physically destroyed or that any sensitive data and licensed software have been removed or overwritten prior to disposal.

Provide physical security and protection regarding the work environment and equipment, as required. Provide users with direct access only to services they have been specifically authorized to use.

Work Environment Process Area

Practice 04 Maintain the Qualification of Components

Maintain the required qualification of work environment components.

Description

Work environment components include software, databases, hardware, tools, test equipment, and appropriate documentation. Qualification of software includes configuration status, configuration audit results, build history, validation of database and configuration tables, and appropriate certifications. Hardware and test equipment qualification includes calibration and adjustment records, traceability to calibration standards, and configuration status. The need and frequency of qualification must be determined; qualification processes and records of qualification activities must be maintained to provide confidence in the instrumentation, control, or measurement components. The qualification status of work environment components should be visible to users and the ability to change the qualification (e.g., the calibration) controlled and protected to prevent accidental or intentional changes. Procedures should be in place to identify measurement equipment that is out of calibration and take appropriate action on affected measurements.

Typical Work Products

- list of components requiring periodic calibration and schedule
- calibration parameters for each component requiring calibration
- calibration procedures
- calibration checklist
- calibration records
- instrument accuracy certificates
- safety qualification data
- record of trends or drifts in calibration error
- software qualification test plan/results
- results of software tool vulnerability testing
- corrective action procedures

Notes

Maintaining the qualification of work environment components ensures that their performance meets expectations. Equipment should be correctly maintained to ensure its continued availability and integrity.

Work Environment Process Area

Practice 05 Maintain the Qualification of Personnel

Ensure that personnel have the required competencies and qualifications to access, use, and maintain the work environment.

Description

Personnel using the work environment must be qualified in appropriate areas including authorization to access the work environment, skills to operate and maintain the environment, and knowledge of safety and security features and procedures. The qualifications must be consistent with the standards and needs of the organization.

Typical Work Products

Documented qualifications, training and evaluations for:

- operations
- maintenance
- safety
- security

Notes

The productivity, safety, and security of the work environment depend on personnel qualifications, training, and procedures.

Consider whether supervision is required for new or inexperienced staff.

Inform people about safety and security policy and procedures, correct use of information processing facilities, and procedures for identifying and reporting various types of safety and security incidents.

Qualification of personnel includes qualification of third party users, if applicable.

Generally, requirements related to third party access or internal controls are reflected by the third party contract and/or non-disclosure agreements. In connection with third party access, identify and assess risks; screen applicants, as appropriate; consider offices, computer rooms, filing cabinets, etc., as well as logical access (e.g., databases); consider support staff, cleaning, catering, guards, students, consultants, contractors and other short-term appointments; establish/enforce controls, contract provisions, and non-disclosure agreements, etc.

Work Environment Process Area

Practice 06 Maintain Technology Awareness

Monitor, evaluate, and insert, as appropriate, new technology for improving the work environment.

Description

Seek to improve the effectiveness of the work environment through the application of new technology. Establish and use mechanisms to maintain technology awareness. Evaluate new technology and manage the insertion of appropriate technology that enhances stakeholder benefits. Perform cost/benefit and impact studies for the application of new technology to the work environment, including impacts to enterprise products and services.

Typical Work Products

- subscriptions to technology publications
- disseminated results of attendance at conferences and trade shows
- technology insertion cost benefit analyses
- technology integration and impact studies
- technology insertion plan

Notes

Regularly evaluate the effectiveness of the existing environment and forecast the need for additional, upgraded, or new tools or work environment components. Regularly review and assess external trends that might affect the work environment.

Technology awareness may be maintained through conferences, professional societies, journals, trade shows, or benchmarking. Maintain awareness of recent developments at universities and results from research laboratories.

Work Environment Process Area

Practice 07 Ensure Work Environment Continuity

Plan and provide for continuity of the work environment.

Description

Establish and maintain plans and conduct activities to counteract interruptions to activities and to protect critical assets from the effects of failures or disasters. Failure areas that should be considered for analysis and mitigation actions include equipment, buildings, utilities, systems, software, and key personnel. Safety and security should be considered for all assets. A work environment continuity management process should be implemented to reduce potential disruptions to an acceptable level through a combination of preventative and recovery controls. Continuity plans should be established and maintained to ensure that business and work environment processes can be restored within the required time frames, and the plans should be practiced so that they become an integral part of the work force culture.

Typical Work Products

- list of events and circumstances that constitute a risk to business continuity
- analyses of potential business and work environment continuity risks
- disaster recovery plans, contingency plans, or continuity plans
- resource reserves to respond to disruptive events
- training plans and material for adverse events
- lists of appropriate back-up equipment to be available
- back-up personnel for key personnel
- plans and results of/for testing emergency response systems
- posted procedures for emergencies
- disseminated lists of key contacts and information resources for emergencies

Notes

Disasters may result from natural events (e.g., fire, flood, and storms), intentional events (e.g., war, terrorism, and cyber-attack), or unintentional events (e.g., equipment failures). Consider both external and internal sources.

Plans should address alternate facilities and equipment, regular back-ups, off-site storage, and testing of business continuity plans and procedures. Revise continuity plans, as necessary, based on changing requirements and results of tests and exercises.

Apply risk management practices (see PA 13 Risk Management in the iCMM; Risk Management process area in CMMI) to assess, analyze, and mitigate risks to work environment continuity.

Bibliography and References

The following sources and references were used in the development of this work.

Safety Source Standards

- [DEF STAN 00-56] Defence Standard 00-56, Safety Management Requirements for Defence Systems, Ministry of Defence, United Kingdom, December 1996.
- [IEC 61508] IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems, International Electrotechnical Commission, 1997.
- [MIL-STD-882C] Military Standard System Safety Program Requirements, MIL-STD-882C, United States Department of Defense, January 1993.
- [MIL-STD-882D] Standard Practice for System Safety, MIL-STD-882D, United States Department of Defense, February 2000.

Security Source Standards

- [ISO/IEC 15408:1999 Common Criteria] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 2.1, Common Criteria Project Sponsoring Organizations, 1999.
- [ISO/IEC 17799] ISO/IEC 17799:2000(E): Information technology – Code of practice for information security management, International Organization for Standardization, First edition 2000-12-01.
- [ISO/IEC 21827 SSE-CMM] ISO/IEC 21827:2002: Systems Security Engineering Capability Maturity Model, International Organization for Standardization.

(Systems Security Engineering Capability Maturity Model, Model Description Document Version 3.0, June 2003, Systems Security Engineering Capability Maturity Model (SSE-CMM) Project.)
- [NIST 800-30] Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology, Special Publication 800-30, 2001.

Bibliography and References

Integrated Capability Maturity Models

[CMMI – SE/SW/IPPD] Capability Maturity Model Integration (CMMI), Version 1.1 - CMMI for Systems Engineering, Software Engineering, Integrated Product and Process Development, and Supplier Sourcing (CMMI-SE/SW/IPPD/SS, v1.1) Continuous Representation, CMU/SEI-2002-TR-011, ESC-TR-2002-011, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, March 2002.

[FAA-iCMM v2.0] The Federal Aviation Administration Integrated Capability Maturity Model (FAA-iCMM), Version 2.0, Federal Aviation Administration, September 2001.

Other Safety and Security References

[+SAFE] + SAFE, A Safety Extension to CMMI, SVRC Services, UniQuest Pty Lmt, Queensland, Australia, 2001.

[ISO/IEC 15026] ISO/IEC 15026:1997(E), System and Software Integrity Levels, International Organization for Standardization, 1997.

[NIST 800-61] Computer Security Incident Handling Guide, National Institute of Standards and Technology, Special Publication 800-61, 2004.

[SafSec] SafSec: Integration of Safety and Security, Phase II Final Report, Praxis Critical Systems, United Kingdom, November 2003.

[SCMM] Safety culture maturity model, Offshore Technology Report, The Keil Centre, Edinburgh, 2001.

Work Environment Sources and References (in addition to Safety and Security source standards listed above)

[EIA/IS 731] Systems Engineering Capability EIA/IS 731, EIA Interim Standard, Electronic Industries Association, 1998.

[eSCM] ESourcing Capability Model for IT-enabled Service Providers v1.1, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, 2002.

Bibliography and References

- [FAA-iCMM v1.0] The Federal Aviation Administration Integrated Capability Maturity Model (FAA-iCMM), Version 1.0, Federal Aviation Administration, November 1997.
- [IEEE/EIA 12207] IEEE/EIA 12207.0-1996 Industry Implementation of International Standard ISO/IEC 12207: 1995, Standard for Information Technology – Software life cycle processes, Institute of Electrical and Electronics Engineers, Inc., March 1998.
- [ISO 9001] ISO 9001:2000(E), Quality management systems – Requirements, International Organization for Standardization, Third edition, 2000-12-15.
- [ISO/IEC 15288] ISO/IEC 15288: 2002(E), Systems engineering – System life cycle processes, International Organization for Standardization and International Electrotechnical Commission, First edition, 2002-11-01.
- [ISO/IEC TR 15504] ISO/IEC TR 15504:1998(E) Information technology – Software process assessment, Part 5: An assessment model and indicator guidance; Part 7: Guidelines for software process improvement, International Organization for Standardization and International Electrotechnical Commission, 1998.
- [MBNQA] The Malcolm Baldrige National Quality Award Program 2000, United States Department of Commerce, National Institute of Standards and Technology.
- [P-CMM] People Capability Maturity Model, Version 2.0, CMU/SEI-2001-MM-01, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 2001.

Appendix A: Project History and Approach

Launch Project

This project was launched in May 2002 with a full day kick-off meeting explaining project background and objectives to a broad community of stakeholders, subject matter experts, and potential project participants from across government and industry. In June 2002, several teams were formed to focus on different project activities resulting in the establishment of expert teams for project management, safety, security, model alignment, harmonization, and pilot appraisals.

Select Source Material

Source documents and reference documents were selected for safety and for security by experts within the respective communities of practice. *Source* documents are the documents from which the safety and security practices are derived. Mapping of safety and security practices to source practices is required and coverage of source documents, at an appropriate level of detail, is demonstrated. The approach was to consider only major, essential, widely-recognized documents as source documents, and the number of sources was limited to 3 to 5 for each area. *Reference* documents are documents identified as useful in developing best practice in certain areas, but full coverage and detailed mapping is not required. The following source standards were selected and endorsed by experts from safety and security communities of practice:

For safety:

- *MIL-STD-882C*: System Safety Program Requirements, Military Standard, January 1993.
- *MIL-STD-882D*: Standard Practice for System Safety, Department of Defense, February 2000.
- *IEC 61508*: Functional Safety of Electrical/ Electronic/ Programmable Electronic Systems, International Electrotechnical Commission, 1997.
- *DEF STAN 00-56*: Safety Management Requirements for Defence Systems, Ministry of Defence, December 1996.

For security:

- *ISO/IEC 17799*: Information Technology - Code of practice for information security management, International Organization for Standardization, 2000.
- *ISO/IEC 15408*: Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, v2.1, Common Criteria Project Sponsoring Organizations, 1999.
- *ISO/IEC 21827*: Systems Security Engineering Capability Maturity Model (SSE-CMM), v3.0, SSE-CMM Project, 2003.
- *NIST 800-30*: Risk Management Guide for Information Technology Systems, Special Publication 800-30, National Institute of Standards and Technology, 2001.

Appendix A: Project History and Approach

Synthesize and Harmonize Practices

The safety expert team and the security expert team separately analyzed their respective source documents and aligned them according to common subject matter areas or expected outcomes. Then, for each discipline, practices were synthesized from similar source practices/activities pertaining to common outcomes. In October 2002, the separately derived safety practices and security practices were harmonized into a single set of practices, seeking commonality across the practices, as well as common terminology. Mappings of the synthesized, harmonized practices to the source documents were maintained.

Presentation and First External Review

The harmonized safety and security practices were presented at the 2nd Annual CMMI Technology Conference, held November 2002 in Denver, Colorado. Input received from process improvement experts and from the CMMI Steering Group was incorporated into the initial safety and security package that was distributed for broad review that month. This first external review resulted in over 200 comments from U.S. and international reviewers. By Spring 2003, the team had resolved these comments and revised the harmonized practices accordingly.

Analysis in Relation to the Reference Models

The revised harmonized practices were analyzed in relation to content in the iCMM and CMMI reference models, the needs of users of the safety and security practices, and previous approaches that had been used with both the iCMM and CMMI to address model enhancements. The following issues were debated among the model expert team:

- Do we need new process area(s)?
- Can we just elaborate upon what is already in the models?
- Do we need new practices for existing process areas?
- How can we assure that safety and security practices are visible and distinctly improvable?
- How can we assure safety and security capability can be measured and appraised?

Based on the analysis above, in June 2003 a new construct was proposed for addressing the safety and security practices with respect to the reference models. This construct is called an Application Area (explained in this document). Additionally, the team proposed developing a new Work Environment Process Area.

The team elaborated the safety and security practices within the constructs of a Safety and Security Application Area and a Work Environment Process Area, drawing additional materials from source documents and preparing the next package for external review.

Pilot Appraisals

The first pilot appraisals were carried out in the FAA in the summer of 2003. These appraisals focused on application in a security context. Subsequent pilot appraisals were carried out, the next being performed in part of Lockheed Martin, using the application practices in both a safety and security context, in both the product development

Appendix A: Project History and Approach

environment and the site environment. A final pilot appraisal was performed at Wright Patterson Air Force Base, focusing on security.

Presentations and Second External Review

The Safety and Security Application Area and Work Environment Process Area were presented at the *3rd Annual CMMI Technology Conference* held November 2003 in Denver, Colorado. Feedback from process improvement practitioners was again sought and incorporated into a second package that was distributed for broad external review in January 2004. To ensure awareness of this project across the broad process improvement communities, the safety and security project work was presented at *SEPG 2004* (March 2004 in Orlando), at *European SEPG (ESEPG) 2004* (June 2004 in London), and at numerous other conferences, workshops, and forums.

Final Revisions

The second and subsequent external reviews resulted in receiving over 500 comments from U.S. and international reviewers. The team addressed the comments received, along with lessons learned from pilot appraisals, and incorporated them into this final product.

Publication

This product is being published in three formats:

- An integrated project report, providing the standards-based, harmonized, safety and security application area with information regarding its use with both iCMM and CMMI, plus the work environment process area in a generic format (*Safety and Security Extensions for Integrated Capability Maturity Models*);
- A report directed towards iCMM users, providing the standards-based, harmonized, safety and security application area with information regarding its use with the iCMM, plus the work environment process area in iCMM format (*Safety and Security Extensions for the FAA-iCMM v2.0*); and
- A report directed towards CMMI users, providing the standards-based, harmonized, safety and security application area with information regarding its use with the CMMI along with required iCMM extensions to CMMI, plus the work environment process area in CMMI format (*Safety and Security Extensions for CMMI-SE/SE/IPPD/SS v1.1*).

APPENDIX B: MAPPING TABLES

This appendix contains the following mapping tables:

Table 1: Safety and Security Application Practices Mapped to Sources

- Part 1 – Safety Sources
- Part 2 – Security Sources

Table 2: Safety Sources Mapped to Safety and Security Application Practices

- Part 1 – Defence Standard 00-56, Safety Management Requirements for Defence Systems
- Part 2 – IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems
- Part 3 – Military Standard System Safety Program Requirements, MIL-STD-882C
- Part 4 – Standard Practice for System Safety, MIL-STD-882D

Table 3: Security Sources Mapped to Safety and Security Application Practices

- Part 1 – ISO/IEC 17799 Information technology – Code of practice for information security management
- Part 2 – Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408:1999)
- Part 3 – ISO/IEC 21827: Systems Security Engineering Capability Maturity Model (SSE-CMM)
- Part 4 – NIST 800-30 Risk Management Guide for Information Technology Systems

Table 4: Work Environment Practices Mapped to Sources

- Part 1 – ISO 9001:2000, *EIA/IS 731, CMMI, iCMM v1.0, and MBNQA
- Part 2 – ISO/IEC 15504, ISO/IEC 12207, ISO/IEC 15288, P-CMM, and eSCM
- Part 3 – Safety Sources
- Part 4 – Security Sources

* *Systems Engineering Capability EIA/IS 731*, EIA Interim Standard, Electronic Industries Association, 1998

Permission to use excerpts from this document was granted by Government Electronics & Information Technology Association (GEIA).

**Table 1: Safety and Security Application Practices Mapped to Sources
Part 1 – Safety Sources**

Safety and Security Application Practice	Def Std 0056	MIL-STD-882C	MIL-STD-882D	IEC 61508
AP 01.01 Ensure Safety and Security Competency	5.3.4 Independent Safety Auditor 5.3.5 Quality of staff	4.1.2 Key system safety personnel 4.4.4 Develop procedures and training Task 101 System Safety Program Task 102 System Safety Program Plan Task 206 Operate and Support Hazard Analysis		8.2.8 (Part 1) 8.2.11 (Part 1) 8.2.13 (Part 1) 7.8.2 Requirements (Part 2) 6.2.2 (Part 1) 7.6.2 Requirements (Part 1)
AP 01.02 Establish Qualified Work Environment <i>(See also Work Environment PA Map)</i>	5.5.3 7.3.3 Determination of Design Rules and Techniques	4.2 System safety program objectives 4.3 System safety design requirements 4.4.4 Develop procedures and training Task 102 System Safety Program Plan Task 203 Safety Requirements/ Criteria Analysis Task 206 Operate and Support Hazard Analysis Task 302 Test and Evaluation Safety Task 207 Health Hazard Assessment	4.6 Verification of mishap risk reduction	7.14.2 Requirements (Part 1) 8.2.5 (Part 1) 7.3.2 Requirements (Part 2) 7.4.6 Requirements for proof tests and diagnostic tests (Part 2) 7.4.7 Requirements for the avoidance of failures (Part 2) 7.7.2 Requirements (Part 2) 7.4.4 Requirements for support tools and programming languages (Part 3) 7.5.2 Requirements (Part 3) 7.7.2 Requirements (Part 3) 7.9.2 Requirements (Part 3)
AP 01.03 Ensure Integrity of Safety and Security Information	4.4.2 Mandatory Activities 5.3.4 Independent Safety Auditor 5.6.3 5.8.1 5.8.2 5.8.4 5.8.6 5.8.7 5.8.8 5.8.9 6.2 7.2.2 Preliminary Hazard Listing 7.2.3 Preliminary Hazard	4.2 System safety program objectives Task 102 System Safety Program Plan Task 106 Hazard Tracking and Risk Resolution		5.2.4 (Part 1) 5.2.5 (Part 1) 5.2.6 (Part 1) 5.2.7 (Part 1) 5.2.8 (Part 1) 5.2.10 (Part 1) 6.2.2 (Part 1) 7.2.2 Requirements (Part 1) 7.3.2 Requirements (Part 1) 7.4.2 Requirements (Part 1) 7.6.2 Requirements (Part 1) 7.7.2 Requirements (Part 1) 7.13.2 Requirements (Part 1) 7.14.2 Requirements (Part 1) 7.15.2 Requirements (Part 1)

**Table 1: Safety and Security Application Practices Mapped to Sources
Part 1 – Safety Sources**

Safety and Security Application Practice	Def Std 0056	MIL-STD-882C	MIL-STD-882D	IEC 61508
	Analysis 7.2.4 System Hazard Analysis 7.2.5 System Change Hazard Analysis 7.3.3 Determination of Design Rules and Techniques 7.3.4 Safety Criteria Report 7.4.4 Accident Sequences 7.4.5 Categorization of Accidents 7.4.7 Hazard Probability Targets 7.4.8 Apportionment of Hazard Probability Targets 7.5.5 7.5.6 8.1 8.2 8.3			7.16.2 Requirements (Part 1) 7.17.2 Requirements (Part 1) 7.18.2 Requirements (Part 1) 8.2.2 (Part 1) 7.4.2 General Requirements (Part 2) 7.4.4 Requirements for estimating the probability of hardware failure (Part 2) 7.5.2 Requirements (Part 2) 7.7.2 Requirements (Part 2) 7.8.2 Requirements (Part 2) 7.9.2 Requirements (Part 2) 7.1.2 Requirements (Part 3) 7.4.5 Requirements for detailed design and development (Part 3) 7.4.7 Requirements for software module testing (Part 3) 7.4.8 Requirements for software integration testing (Part 3) 7.5.2 Requirements (Part 3) 7.7.2 Requirements (Part 3) 7.8.2 Requirements (Part 3) 7.9.2 Requirements (Part 3)
AP 01.04 Monitor Operations and Report Incidents	4.4.2 Mandatory Activities 4.5 Safety Verification 4.6 Hazard Log 5.8.3 7.2.5 System Change Hazard Analysis 7.5.7 8.1 8.2 9.4	4.1.1 Management System 4.2 System safety program objectives Task 101 System Safety Program Task 102 System Safety Program Plan Task 206 Operate and Support Hazard Analysis		6.2.2 (Part 1) 7.8.2 Requirements (Part 2)
AP 01.05 Ensure Business		Task 206 Operate and Support Hazard		

**Table 1: Safety and Security Application Practices Mapped to Sources
Part 1 – Safety Sources**

Safety and Security Application Practice	Def Std 0056	MIL-STD-882C	MIL-STD-882D	IEC 61508
Continuity		Analysis Task 207 Health Hazard Assessment		
AP 01.06 Identify Safety and Security Risks	4.2.2 4.4.1 General 4.4.2 Mandatory Activities 4.4.3 Hazard Identification and Refinement 5.7.3 7.1 Introduction 7.2.1 General 7.2.2 Preliminary Hazard Listing	4.1.1 Management System 4.2 System safety program objectives 4.3 System safety design requirements Task 102 System Safety Program Plan Task 201 Preliminary Hazard List Task 203 Safety Requirements/ Criteria Analysis Task 204 Subsystem Hazard Analysis Task 205 System Hazard Analysis Task 206 Operate and Support Hazard Analysis Task 207 Health Hazard Assessment Task 303 Safety Review of Engineering Change Proposals, Specification Change Notices, Software Problem Reports, and Requests for Deviation/ Waiver Task 403 Explosive Hazard Classification and Characteristics Data	4.2 Identification of hazards	7.2.2 Requirements (Part 1) 7.3.2 Requirements (Part 1) 7.4.2 Requirements (Part 1) 7.17.2 Requirements (Part 1) 6.2.2 (Part 1)
AP 01.07 Analyze and Prioritize Risks	7.2.1 General 4.2.2 4.4.3 Hazard Identification and Refinement 4.4.1 General 4.4.2 Mandatory Activities 4.4.4 Risk Estimation 7.1 Introduction 7.2.3 Preliminary Hazard Analysis 7.2.4 System Hazard Analysis 7.2.5 System Change Hazard Analysis 7.3.2 Formulation of the	4.1.1 Management System 4.2 System safety program objectives 4.3 System safety design requirements 4.5 Risk assessment 4.5.1 Hazard severity 4.5.2 Hazard probability 4.5.3 Risk impact Task 102 System Safety Program Plan Task 202 Preliminary Hazard Analysis Task 203 Safety Requirements/ Criteria Analysis Task 204 Subsystem Hazard Analysis Task 205 System Hazard Analysis Task 206 Operate and Support Hazard Analysis	4.3 Assessment of mishap risk	7.4.2 Requirements (Part 1) 7.5.2 Requirements (Part 1) 7.16.2 Requirements (Part 1) 7.17.2 Requirements (Part 1) 6.2.2 (Part 1)

**Table 1: Safety and Security Application Practices Mapped to Sources
Part 1 – Safety Sources**

Safety and Security Application Practice	Def Std 0056	MIL-STD-882C	MIL-STD-882D	IEC 61508
	Safety Analysis Tables 7.3.4 Safety Criteria Report 7.4.1 Introduction 7.4.4 Accident Sequences 7.4.5 Categorization of Accidents 7.4.6 Accident Probability Targets 7.4.7 Hazard Probability Targets	Task 207 Health Hazard Assessment Task 303 Safety Review of Engineering Change Proposals, Specification Change Notices, Software Problem Reports, and Requests for Deviation/ Waiver		
AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan	4.4.1 General 5.9 Design Documentation 7.1 Introduction 7.2.3 Preliminary Hazard Analysis 7.3.4 Safety Criteria Report 7.4.1 Introduction 7.4.2 Safety Integrity 7.4.3 Claim limits 7.4.8 Apportionment of Hazard Probability Targets 7.5.2 7.5.3 7.5.5	4.1.1 Management System 4.2 System safety program objectives 4.3 System safety design requirements 4.4.1 Design for minimum risk 4.4.2 Incorporate safety devices 4.4.3 Provide warning devices 4.4.4 Develop procedures and training 4.6 Action on identified hazards Task 202 Preliminary Hazard Analysis Task 203 Safety Requirements/ Criteria Analysis Task 204 Subsystem Hazard Analysis Task 205 System Hazard Analysis Task 206 Operate and Support Hazard Analysis Task 207 Health Hazard Assessment	4.4 Identification of mishap risk mitigation measures 4.5 Reduction of mishap risk to an acceptable level 4.8 Tracking of hazards, their closures, and residual mishap risk	7.4.2 Requirements (Part 1) 7.5.2 Requirements (Part 1) 7.6.2 Requirements (Part 1)
AP 01.09 Determine Regulatory Requirements, Laws and Standards	7.3.1 Introduction 7.3.2 Formulation of the Safety Analysis Tables 7.3.3 Determination of Design Rules and Techniques 7.4.2 Safety Integrity 7.4.3 Claim limits 7.4.6 Accident Probability	4.3 System safety design requirements Task 102 System Safety Program Plan Task 203 Safety Requirements/ Criteria Analysis		5.2.4 (Part 1) 7.1.4 Requirements (Part 1) 7.2.2 Requirements (Part 1) 7.4.2 Requirements (Part 1) 7.5.2 Requirements (Part 1) 7.15.2 Requirements (Part 1) 8.2.12 (Part 1) 7.2.3 E/E/PES safety requirements (Part 2)

**Table 1: Safety and Security Application Practices Mapped to Sources
Part 1 – Safety Sources**

Safety and Security Application Practice	Def Std 0056	MIL-STD-882C	MIL-STD-882D	IEC 61508
	Targets 7.4.7 Hazard Probability Targets Targets 7.4.8 Apportionment of Hazard Probability Targets			7.4.2 General Requirements (Part 2) 7.4.5 Architectural constraints on hardware safety integrity (Part 2) 7.4.7 Requirements for the avoidance of failures (Part 2) 7.6.2 Requirements (Part 2) 7.7.2 Requirements (Part 2) 7.1.2 Requirements (Part 3) 7.2.2 Requirements (Part 3) 7.4.2 General Requirements (Part 3) 7.4.3 Requirements for software (Part 3)architecture 7.4.4 Requirements for support tools and programming languages (Part 3)
AP 01.10 Develop and Deploy Safe and Secure Products and Services	4.3.2 4.4.1 General 4.4.5 Safety Compliance Assessment 5.9 Design Documentation 6.1 7.2.3 Preliminary Hazard Analysis 7.4.2 Safety Integrity 7.4.3 Claim limits 7.4.8 Apportionment of Hazard Probability Targets	4.2 System safety program objectives 4.3 System safety design requirements 4.4 System safety precedence 4.4.1 Design for minimum risk 4.4.2 Incorporate safety devices 4.4.3 Provide warning devices 4.4.4 Develop procedures and training Task 102 System Safety Program Plan Task 202 Preliminary Hazard Analysis Task 203 Safety Requirements/ Criteria Analysis Task 204 Subsystem Hazard Analysis Task 205 System Hazard Analysis Task 206 Operate and Support Hazard Analysis Task 207 Health Hazard Assessment Task 303 Safety Review of Engineering	4.4 Identification of mishap risk mitigation measures 5 Detailed requirements	5.2.1 (Part 1) 5.2.3 (Part 1) 6.2.2 (Part 1) 7.5.2 Requirements (Part 1) 7.6.2 Requirements (Part 1) 7.13.2 Requirements (Part 1) 7.15.2 Requirements (Part 1) 7.16.2 Requirements (Part 1) 7.17.2 Requirements (Part 1) 7.2.2 General Requirements (Part 2) 7.2.3 E/E/PES safety requirements (Part 2) 7.4.2 General Requirements (Part 2) 7.4.3 Requirements for the control of random hardware

**Table 1: Safety and Security Application Practices Mapped to Sources
Part 1 – Safety Sources**

Safety and Security Application Practice	Def Std 0056	MIL-STD-882C	MIL-STD-882D	IEC 61508
		Change Proposals, Specification Change Notices, Software Problem Reports, and Requests for Deviation/ Waiver Task 404 Explosive Ordnance Disposal Source Data		faults (Part 2) 7.4.4 Requirements for estimating the probability of hardware failure (Part 2) 7.4.5 Architectural constraints on hardware safety integrity (Part 2) 7.4.6 Requirements for proof tests and diagnostic tests (Part 2) 7.4.7 Requirements for the avoidance of failures (Part 2) 7.4.8 Requirements for the control of systematic faults (Part 2) 7.4.9 Requirements for E/E/PES Implementation (Part 2) 7.5.2 Requirements (Part 2) 7.8.2 Requirements (Part 2) 7.2.2 Requirements (Part 3) 7.4.2 General Requirements (Part 3) 7.4.3 Requirements for software (Part 3)architecture 7.4.5 Requirements for detailed design and development (Part 3) 7.4.6 Requirements for code implementation (Part 3) 7.8.2 Requirements (Part 3) 7.6.2 Requirements (Part 2)
AP 01.11 Objectively Evaluate Products	4.2.2 4.4.1 General 4.4.2 Mandatory Activities 4.4.5 Safety Compliance Assessment 4.5 Safety Verification	Task 102 System Safety Program Plan Task 204 Subsystem Hazard Analysis Task 205 System Hazard Analysis Task 206 Operate and Support Hazard Analysis Task 301 Safety Assessment	4.6 Verification of mishap risk reduction	7.6.2 Requirements (Part 2) 5.2.3 (Part 1) 6.2.2 (Part 1) 7.1.4 Requirements (Part 1) 7.8.2 Requirements (Part 1) 7.14.2 Requirements (Part 1)

**Table 1: Safety and Security Application Practices Mapped to Sources
Part 1 – Safety Sources**

Safety and Security Application Practice	Def Std 0056	MIL-STD-882C	MIL-STD-882D	IEC 61508
	5.3.4 Independent Safety Auditor 5.4.1 5.7.1 5.7.3 5.9 Design Documentation 7.1 Introduction 7.5.1 7.5.2 7.5.5 7.5.6 7.5.7 9.1 9.2 9.4	Task 302 Test and Evaluation Safety Task 401 Safety Verification Task 402 Safety Compliance Assessment Task 403 Explosive Hazard Classification and Characteristics Data Task 403 Explosive Hazard Classification and Characteristics Data Task 404 Explosive Ordnance Disposal Source Data Task 207 Health Hazard Assessment		7.15.2 Requirements (Part 1) 7.18.2 Requirements (Part 1) 8.2.1 (Part 1) 8.2.3 (Part 1) 8.2.4 (Part 1) 8.2.5 (Part 1) 8.2.6 (Part 1) 8.2.7 (Part 1) 8.2.8 (Part 1) 8.2.10 (Part 1) 8.2.12 (Part 1) 8.2.13 (Part 1) 8.2.14 (Part 1) 7.3.2 Requirements (Part 2) 7.4.2 General Requirements (Part 2) 7.4.4 Requirements for estimating the probability of hardware failure (Part 2) 7.4.7 Requirements for the avoidance of failures (Part 2) 7.5.2 Requirements (Part 2) 7.7.2 Requirements (Part 2) 7.8.2 Requirements (Part 2) 7.9.2 Requirements (Part 2) 6.2.2 (Part 3) 7.3.2 Requirements (Part 3) 7.4.4 Requirements for support tools and programming languages (Part 3) 7.4.5 Requirements for detailed design and development (Part 3) 7.4.6 Requirements for code implementation (Part 3) 7.4.7 Requirements for software module testing (Part 3)

**Table 1: Safety and Security Application Practices Mapped to Sources
Part 1 – Safety Sources**

Safety and Security Application Practice	Def Std 0056	MIL-STD-882C	MIL-STD-882D	IEC 61508
				7.4.8 Requirements for software integration testing (Part 3) 7.5.2 Requirements (Part 3) 7.7.2 Requirements(Part 3) 7.8.2 Requirements (Part 3) 7.9.2 Requirements (Part 3) 5.2.1 (Part 1)
AP 01.12 Establish Safety and Security Assurance Arguments	4.2.1 7.2.2 Preliminary Hazard Listing 4.2.2 4.4.1 General 4.6 Hazard Log 4.7 Safety Case 5.3.4 Independent Safety Auditor 5.4.2 5.7.3 5.8.1 5.8.2 5.8.3 5.8.4 5.8.6 5.8.7 5.8.8 5.8.9 6.2 7.2.3 Preliminary Hazard Analysis 7.2.4 System Hazard Analysis 7.2.5 System Change Hazard Analysis 7.3.2 Formulation of the Safety Analysis Tables	4.2 System safety program objectives 4.6.1 Residual risk Task 106 Hazard Tracking and Risk Resolution Task 301 Safety Assessment Task 302 Test and Evaluation Safety Task 402 Safety Compliance Assessment	4.6 Verification of mishap risk reduction 4.7 Review of hazards and acceptance of residual mishap risk by the appropriate authority	5.2.3 (Part 1) 6.2.2 (Part 1) 7.2.2 Requirements (Part 1) 7.3.2 Requirements (Part 1) 7.4.2 Requirements (Part 1) 7.4.8 Requirements for the control of systematic faults (Part 2) 7.6.2 Requirements (Part 1) 7.13.2 Requirements (Part 1) 7.14.2 Requirements (Part 1) 7.16.2 Requirements (Part 1) 7.17.2 Requirements (Part 1) 7.18.2 Requirements (Part 1) 7.4.2 General Requirements (Part 2) 7.4.9 Requirements for E/E/PES Implementation (Part 2) 7.7.2 Requirements (Part 2) 7.9.2 Requirements (Part 2) 7.3.2 Requirements (Part 3) 7.4.3 Requirements for software (Part 3)architecture 7.8.2 Requirements (Part 3) 7.9.2 Requirements (Part 3)

**Table 1: Safety and Security Application Practices Mapped to Sources
Part 1 – Safety Sources**

Safety and Security Application Practice	Def Std 0056	MIL-STD-882C	MIL-STD-882D	IEC 61508
	7.3.3 Determination of Design Rules and Techniques 7.3.4 Safety Criteria Report 7.4.4 Accident Sequences 7.4.5 Categorization of Accidents 7.4.7 Hazard Probability Targets 7.4.8 Apportionment of Hazard Probability Targets 7.5.5 7.5.6 7.5.7 8.3			
AP 01.13 Establish Independent Safety and Security Reporting	4.3.3 5.2.2 5.3.4 Independent Safety Auditor	Task 101 System Safety Program Task 102 System Safety Program Plan		8.2.8 (Part 1) 8.2.12 (Part 1) 8.2.13 (Part 1) 8.2.14 (Part 1)
AP 01.14 Establish a Safety and Security Plan	4.2.2 4.3.1 4.3.2 4.3.3 5.2.1 5.2.2 5.2.3 5.2.4 5.3.1 Project Manager 5.3.2 Project Safety Engineer 5.3.3 Project Safety Committee 5.3.4 Independent Safety Auditor 5.4.3	4.1 System safety program 4.1.1 Management System 4.1.4 Conflicting requirements 4.4 System safety precedence Task 101 System Safety Program Task 102 System Safety Program Plan Task 103 Integration/ Management of Associate contractors, subcontractors, and architect and engineering firms Task 105 System safety group/system working group support	4.1 Documentation of the system safety approach 4.7 Review of hazards and acceptance of residual mishap risk by the appropriate authority	6.2.1 (Part 1) 6.2.4 (Part 1) 7.1.4 Requirements (Part 1) 7.7.2 Requirements (Part 1) 7.8.2 Requirements (Part 1) 7.9.2 Requirements (Part 1) 7.15.2 Requirements (Part 1) 7.16.2 Requirements (Part 1) 7.17.2 Requirements (Part 1) 7.18.2 Requirements (Part 1) 8.2.1 (Part 1) 8.2.7 (Part 1) 8.2.8 (Part 1) 8.2.9 (Part 1) 7.1.3 Requirements (Part 2) 7.2.2 General Requirements

**Table 1: Safety and Security Application Practices Mapped to Sources
Part 1 – Safety Sources**

Safety and Security Application Practice	Def Std 0056	MIL-STD-882C	MIL-STD-882D	IEC 61508
	5.5.2 5.6.1 5.7.4 5.7.5 5.8.5 7.1 Introduction 7.3.2 Formulation of the Safety Analysis Tables 7.4.3 Claim limits 7.5.4 8.1 8.3 9.2 9.3 10.1 10.2			(Part 2) 7.3.2 Requirements (Part 2) 7.4.7 Requirements for the avoidance of failures (Part 2) 7.7.2 Requirements (Part 2) 7.8.2 Requirements (Part 2) 7.9.2 Requirements (Part 2) 6.2.1 (Part 3) 6.2.2 (Part 3) 7.1.2 Requirements (Part 3) 7.3.2 Requirements (Part 3) 7.4.2 General Requirements (Part 3) 7.4.3 Requirements for software (Part 3)architecture 7.4.5 Requirements for detailed design and development (Part 3) 7.4.8 Requirements for software integration testing (Part 3) 7.5.2 Requirements (Part 3) 7.7.2 Requirements (Part 3) 7.8.2 Requirements (Part 3) 7.9.2 Requirements (Part 3) 5.2.2 (Part 1)
AP 01.15 Select and Manage Suppliers, Products and Services	5.2.2 5.7.1 5.7.2 5.7.3 5.7.4 5.7.5 9.2	Task 102 System Safety Program Plan Task 103 Integration/ Management of Associate contractors, subcontractors, and architect and engineering firms	5 Detailed requirements	6.2.5 (Part 1) 7.4.2 General Requirements (Part 2) 7.4.7 Requirements for the avoidance of failures (Part 2) 7.7.2 Requirements (Part 2) 6.2.2 (Part 3) 7.4.2 General Requirements (Part 3) 7.4.3 Requirements for software (Part 3)architecture

**Table 1: Safety and Security Application Practices Mapped to Sources
Part 1 – Safety Sources**

Safety and Security Application Practice	Def Std 0056	MIL-STD-882C	MIL-STD-882D	IEC 61508
				7.4.5 Requirements for detailed design and development (Part 3) 7.7.2 Requirements (Part 3)
AP 01.16 Monitor and Control Activities and Products	4.2.2 4.4.5 Safety Compliance Assessment 5.3.4 Independent Safety Auditor 5.4.1 5.4.2 5.5.1 5.5.2 5.5.3 5.6.2 5.6.3 5.7.3 5.7.5 7.2.5 System Change Hazard Analysis 7.5.2 7.5.7 8.1 8.2	4.1 System safety program 4.1.1 Management System 4.1.3 Compliance 4.1.4 Conflicting requirements 4.2 System safety program objectives Task 102 System Safety Program Plan Task 104 System safety program reviews/audits Task 107 System Safety Progress Summary Task 203 Safety Requirements/ Criteria Analysis Task 303 Safety Review of Engineering Change Proposals, Specification Change Notices, Software Problem Reports, and Requests for Deviation/ Waiver Task 402 Safety Compliance Assessment	4.7 Review of hazards and acceptance of residual mishap risk by the appropriate authority	5.2.9 (Part 1) 5.2.10 (Part 1) 5.2.11 (Part 1) 6.2.2 (Part 1) 6.2.3 (Part 1) 6.2.5 (Part 1) 7.1.3 Requirements (Part 2) 7.1.4 Requirements (Part 1) 7.13.2 Requirements (Part 1) 7.15.2 Requirements (Part 1) 7.16.2 Requirements (Part 1) 7.17.2 Requirements (Part 1) 7.5.2 Requirements (Part 2) 7.7.2 Requirements (Part 2) 6.2.3 7.1.2 Requirements (Part 3) 7.4.3 Requirements for software (Part 3) architecture 7.4.7 Requirements for software module testing (Part 3) 7.4.8 Requirements for software integration testing (Part 3) 7.5.2 Requirements (Part 3) 7.7.2 Requirements (Part 3) 7.8.2 Requirements (Part 3)

**Table 1: Safety and Security Application Practices Mapped to Sources
Part 2 - Security Sources**

Safety and Security Application Practice	ISO/IEC 17799	ISO/IEC 15408 Common Criteria	ISO/IEC 21827 SSE-CMM	NIST 800-30
AP 01.01 Ensure Safety and Security Competency	4.1.3 Allocation of information security responsibilities 4.1.5 Specialist information security advice 6.2 <i>User training</i> 6.2.1 Information security education and training 9.3 <i>User responsibilities</i> 9.3.1 Password use 9.3.2 Unattended user equipment		BP.01.03 Manage security awareness, training, and education programs for all users and administrators. BP.09.01 Work with designers, developers, and users to ensure that appropriate parties have a common understanding of security input needs. BP.09.05 Provide security related guidance to the other engineering groups. BP.09.06 Provide security related guidance to operational system users and administrators. BP.21.01 Identify training needs BP.21.02 Select mode of knowledge or skill acquisition BP.21.03 Assure availability of skill and knowledge BP.21.04 Prepare training materials BP.21.05 Train personnel BP.21.06 Assess training effectiveness BP.21.07 Maintain training records BP.21.08 Maintain training materials	
AP 01.02 Establish Qualified Work Environment <i>(See also Work Environment PA Map)</i>	4.1.4 Authorization process for information processing facilities 4.2 <i>Security of third party access</i> 4.2.1 Identification of risks from third party access 4.2.2 Security requirements in third party contracts 5.1.1 Inventory of assets 6.1 <i>Security in job definition and resourcing</i> 6.1.2 Personnel screening and policy 6.2 <i>User training</i> 6.2.1 Information security education and training 6.3.2 Reporting security weaknesses 6.3.3 Reporting software malfunctions 7.1 <i>Secure areas</i> 7.1.1 Physical security perimeter	ACM_AUT Automation ALC_DVS Development security ALC_FLR Flaw remediation ALC_LCD Life cycle definition ALC_TAT Tools and techniques AMA_CAT TOE Component categorization report	BP.01.03 Manage security awareness, training, and education programs for all users and administrators. BP.01.04 Manage periodic maintenance and administration of security services and control mechanisms. BP.02.02 Identify and characterize the system assets that support the key operational capabilities or the security objectives of the system. BP.09.05 Provide security related guidance to the other engineering groups. BP.09.06 Provide security related guidance to operational system users and administrators. BP.13.01 Establish configuration management methodology BP.13.05 Communicate configuration status	3.1.2 Information-Gathering Techniques 4.4.3 Operational Security Controls

**Table 1: Safety and Security Application Practices Mapped to Sources
Part 2 - Security Sources**

Safety and Security Application Practice	ISO/IEC 17799	ISO/IEC 15408 Common Criteria	ISO/IEC 21827 SSE-CMM	NIST 800-30
	<p>7.1.2 Physical entry controls 7.1.3 Securing offices, rooms and facilities 7.1.4. Working in secure areas 7.1.5 Isolated delivery and loading areas 7.2 <i>Equipment security</i> 7.2.1 Equipment siting and protection 7.2.2 Power supplies 7.2.3 Cabling security 7.2.4 Equipment maintenance 7.2.5 Security of equipment off-premises 7.2.6 Secure disposal or re-use of equipment 7.3 <i>General controls</i> 7.3.1 Clear desk and clear screen policy 7.3.2 Removal of property 8.1 <i>Operational procedures and responsibilities</i> 8.1.1 Documented operating procedures 8.1.2 Operational change control 8.1.4 Segregation of duties 8.1.5 Separation of development and operational facilities 8.2.1 Capacity planning 8.4 <i>Housekeeping</i> 8.4.1 Information back-up 8.5 <i>Network management</i> 8.5.1 Network controls 8.7.4 Security of electronic mail 8.7.5 Security of electronic office systems 9.1.1 Access Control Policy 9.2 <i>User access management</i> 9.2.1 User registration 9.2.2 Privilege management 9.2.3 User password management 9.2.4 Review of user access rights 9.3 <i>User responsibilities</i> 9.3.1 Password use 9.3.2 Unattended user equipment 9.4 <i>Network access control</i></p>		<p>BP.19.01 Define product evolution BP.19.02 Identify new product technologies BP.19.03 Adapt development processes BP.19.04 Ensure critical components availability BP.19.05 Insert product technology BP.20.01 Maintain technical awareness BP.20.02 Determine support requirements BP.20.03 Obtain engineering support environment BP.20.04 Tailor engineering support environment BP.20.05 Insert new technology BP.20.06 Maintain environment BP.20.07 Monitor engineering support environment</p>	

**Table 1: Safety and Security Application Practices Mapped to Sources
Part 2 - Security Sources**

Safety and Security Application Practice	ISO/IEC 17799	ISO/IEC 15408 Common Criteria	ISO/IEC 21827 SSE-CMM	NIST 800-30
	9.4.2 Enforced path 9.4.5 Remote diagnostic port protection 9.4.9 Security of network services 9.6.2 Sensitive system isolation 9.7.2 Monitoring system use 9.7.3 Clock synchronization 9.8 <i>Mobile computing and teleworking</i> 9.8.1 Mobile computing 9.8.2 Teleworking 10.4 <i>Security of system files</i> 10.4.1 Control of operational software 10.4.2 Protection of system test data 10.4.3 Access control to program source library 10.5 <i>Security in development and support processes</i> 11.1 <i>Aspects of business continuity management</i> 11.1.1 Business continuity management process 11.1.2 Business continuity and impact analysis 11.1.3 Writing and implementing continuity plans 11.1.4 Business continuity planning framework 11.1.5 Testing, maintaining and re-assessing business continuity plans 12.1.5 Prevention of misuse of information processing facilities 12.3 <i>System audit considerations</i> 12.3.2 Protection of system audit tools			
AP 01.03 Ensure Integrity of Safety and Security Information	4.1.6 Co-operation between organizations 5.1 <i>Accountability for assets</i> 5.2 <i>Information classification</i> 5.2.1 Classification guidelines 5.2.2 Information labeling and handling 6.1.3 Confidentiality agreements 6.1.4 Terms and conditions of employment	ALC_FLR Flaw remediation	BP.01.04 Manage periodic maintenance and administration of security services and control mechanisms. BP.06.03 Identify and control security assurance evidence. BP.08.07 Ensure that the artifacts related to security monitoring are suitably protected.	

**Table 1: Safety and Security Application Practices Mapped to Sources
Part 2 - Security Sources**

Safety and Security Application Practice	ISO/IEC 17799	ISO/IEC 15408 Common Criteria	ISO/IEC 21827 SSE-CMM	NIST 800-30
	6.3.4 Learning from incidents 8.6 <i>Media handling and security</i> 8.6.1 Management of removable computer media 8.6.2 Disposal of media 8.6.3 Information handling procedures 8.6.4 Security of system documentation 8.7 <i>Exchanges of information and software</i> 8.7.1 Information and software exchange agreements 8.7.2 Security of media in transit 8.7.3 Electronic commerce security 8.7.6 Publicly available systems 8.7.7 Other forms of information exchange 9.1 <i>Business requirement for access control</i> 9.1.1 Access control policy 9.6.1 Information access restriction 12.1.2 Intellectual property rights 12.1.3 Safeguarding of organizational records 12.1.4 Data protection and privacy of personal information			
AP 01.04 Monitor Operations and Report Incidents	6.3 <i>Responding to security incidents and malfunctions</i> 6.3.1 Reporting security incidents 6.3.2 Reporting security weaknesses 6.3.3 Reporting software malfunctions 6.3.4 Learning from incidents 8.1 <i>Operational procedures and responsibilities</i> 8.1.3 Incident management procedures 8.4 Housekeeping 8.4.2 Operator logs 8.4.3 Fault logging 9.7 <i>Monitoring system access and use</i> 9.7.1 Event logging 9.7.2 Monitoring system use 9.7.3 Clock synchronization	ALC_FLR Flaw remediation ALC_LCD Life cycle definition	BP.02.06 Monitor ongoing changes in the impacts. BP.03.06 Monitor ongoing changes in the risk spectrum and changes to their characteristics. BP.04.06 Monitor ongoing changes in the threat spectrum and changes to their characteristics. BP.05.05 Monitor ongoing changes in the applicable vulnerabilities and changes to their characteristics. BP.08.01 Analyze event records to determine the cause of an event, how it proceeded, and likely future events. BP.08.02 Monitor changes in threats, vulnerabilities, impacts, risks, and the environment. BP.08.03 Identify security relevant incidents.	3.3.2 System Security Testing

**Table 1: Safety and Security Application Practices Mapped to Sources
Part 2 - Security Sources**

Safety and Security Application Practice	ISO/IEC 17799	ISO/IEC 15408 Common Criteria	ISO/IEC 21827 SSE-CMM	NIST 800-30
			BP.08.04 Monitor the performance and functional effectiveness of security safeguards. BP.08.05 Review the security posture of the system to identify necessary changes.	
AP 01.05 Ensure Business Continuity	7.2 <i>Equipment security</i> 7.2.1 Equipment siting and protection 7.2.2 Power supplies 7.2.3 Cabling security 8.4.1 Information back-up 8.6 <i>Media handling and security</i> 10.5.2 Technical review of operating system changes 11.1 Aspects of business continuity management 11.1.1 Business continuity management process 11.1.2 Business continuity and impact analysis 11.1.3 Writing and implementing continuity plans 11.1.4 Business continuity planning framework 11.1.5 Testing, maintaining and re-assessing business continuity plans	AMA_AMP Assurance maintenance plan AMA_CAT TOE Component categorization report	BP.08.06 Manage the response to security relevant incidents.	
AP 01.06 Identify Safety and Security Risks	4.2.1 Identification of risks from third party access 8.3 <i>Protection against malicious software</i> 8.3.1 Controls against malicious software 10.2.2 Control of internal processing	AVA_CCA Covert channel analysis AVA_MSU Misuse	BP.02.01 Identify, analyze, and prioritize operational, business, or mission capabilities leveraged by the system. BP.02.02 Identify and characterize the system assets that support the key operational capabilities or the security objectives of the system. BP.04.01 Identify applicable threats arising from a natural source. BP.04.02 Identify applicable threats arising from man-made sources, either accidental or deliberate. BP.04.03 Identify appropriate units of measure, and applicable ranges, in a specified	3.1.1 System-Related Information 3.1.2 Information-Gathering Techniques 3.2.1 Threat-Source Identification 3.2.2 Motivation and Threat Actions 3.3 <i>STEP 3: VULNERABILITY IDENTIFICATION</i> 3.3.1 Vulnerability Sources

**Table 1: Safety and Security Application Practices Mapped to Sources
Part 2 - Security Sources**

Safety and Security Application Practice	ISO/IEC 17799	ISO/IEC 15408 Common Criteria	ISO/IEC 21827 SSE-CMM	NIST 800-30
			<p>environment. BP.04.04 Assess capability and motivation of threat agent for threats arising from man-made sources. BP.05.01 Select the methods, techniques, and criteria by which security system vulnerabilities in a defined environment are identified and characterized. BP.05.02 Identify system security vulnerabilities. BP.05.03 Gather data related to the properties of the vulnerabilities. BP.10.03 Identify the purpose of the system in order to determine the security context. BP.10.04 Capture a high-level security oriented view of the system operation. BP.14.02 Identify risks</p>	<p>3.3.2 System Security Testing 3.3.3 Development of Security Requirements Checklist</p>
AP 01.07 Analyze and Prioritize Risks	<p>8.3 <i>Protection against malicious software</i> 8.3.1 Controls against malicious software 10.1.1 Security requirements analysis and specification 10.3.1 Policy on the use of cryptographic controls 10.3.2 Encryption</p>	<p>AVA_SOF Strength of TOE security functions AVA_VLA Vulnerability analysis</p>	<p>BP.02.01 Identify, analyze, and prioritize operational, business, or mission capabilities leveraged by the system. BP.02.02 Identify and characterize the system assets that support the key operational capabilities or the security objectives of the system. BP.02.03 Select the impact metric to be used for this assessment, BP.02.04 Identify the relationship between the selected metrics for this assessment and metric conversion factors if required, BP.02.05 Identify and characterize impacts. BP.03.01 Select the methods, techniques, and criteria by which security risks, for the system in a defined environment are analyzed, assessed, and compared. BP.03.02 Identify threat/vulnerability/impact triples (exposures). BP.03.03 Assess the risk associated with the occurrence of an exposure. BP.03.05 Order risks by priority.</p>	<p>3.2.1 Threat-Source Identification 3.4.1 Control Methods 3.4.2 Control Categories 3.4.3 Control Analysis Technique 3.5 <i>STEP 5: LIKELIHOOD DETERMINATION</i> 3.6 <i>STEP 6: IMPACT ANALYSIS</i> 3.7.1 Risk-Level Matrix 3.7.2 Description of Risk Level 3.9 <i>STEP 9: RESULTS DOCUMENTATION</i></p>

**Table 1: Safety and Security Application Practices Mapped to Sources
Part 2 - Security Sources**

Safety and Security Application Practice	ISO/IEC 17799	ISO/IEC 15408 Common Criteria	ISO/IEC 21827 SSE-CMM	NIST 800-30
			BP.04.04 Assess capability and motivation of threat agent for threats arising from man-made sources. BP.04.05 Assess the likelihood of an occurrence of a threat event. BP.05.03 Gather data related to the properties of the vulnerabilities. BP.05.04 Assess the system vulnerability and aggregate vulnerabilities that result from specific vulnerabilities and combinations of specific vulnerabilities. BP.14.03 Assess risks	
AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan	4.1.6 Co-operation between organizations 8.2.1 Capacity planning 8.3 <i>Protection against malicious software</i> 8.3.1 Controls against malicious software 9.4.3 User authentication for external connections 9.4.4 Node authentication 10.1.1 Security requirements analysis and specification 10.3.2 Encryption 10.5.4 Covert channels and Trojan code		BP.08.06 Manage the response to security relevant incidents. BP.14.05 Execute risk mitigation BP.14.06 Track risk mitigation	<i>4.4 CONTROL CATEGORIES</i> 4.4.1 Technical Security Controls 4.4.2 Management Security Controls 4.4.3 Operational Security Controls <i>4.5 COST-BENEFIT ANALYSIS</i> <i>4.6 RESIDUAL RISK</i>
AP 01.09 Determine Regulatory Requirements, Laws and Standards	<i>3.1 Information security policy</i> 3.1.1 Information security policy document 4.1.3 Allocation of information security responsibilities 4.1.6 Co-operation between organizations 6.1 Security in job definition and resourcing 6.3.5 Disciplinary process 7.3.1 Clear desk and clear screen policy 8.7 <i>Exchanges of information and software</i> 8.7.1 Information and software exchange agreements 8.7.4 Security of electronic mail 8.7.5 Security of electronic office systems 9.1.1 Access control policy 9.4.1 Policy on use of network services	ADV_FSP Functional specification ADV_INT TSF internals ADV_SPM Security policy modeling ALC_TAT Tools and techniques	BP.03.01 Select the methods, techniques, and criteria by which security risks, for the system in a defined environment are analyzed, assessed, and compared. BP.05.01 Select the methods, techniques, and criteria by which security system vulnerabilities in a defined environment are identified and characterized. BP.09.02 Determine the security constraints and considerations needed to make informed engineering choices. BP.10.02 Identify the laws, policies, standards, external influences and constraints that govern the system. BP.10.05 Capture high-level goals that define	3.1.1 System-Related Information 3.1.2 Information-Gathering Techniques 3.3.3 Development of Security Requirements Checklist

**Table 1: Safety and Security Application Practices Mapped to Sources
Part 2 - Security Sources**

Safety and Security Application Practice	ISO/IEC 17799	ISO/IEC 15408 Common Criteria	ISO/IEC 21827 SSE-CMM	NIST 800-30
	<p>9.6 <i>Application access control</i></p> <p>9.6.1 Information access restriction</p> <p>9.8.1 Mobile computing</p> <p>9.8.2 Teleworking</p> <p>10.3.1 Policy on the use of cryptographic controls</p> <p>10.3.2 Encryption</p> <p>10.3.3 Digital signatures</p> <p>10.3.5 Key management</p> <p>12. Compliance</p> <p>12.1 <i>Compliance with legal requirements</i></p> <p>12.1.1 Identification of applicable legislation</p> <p>12.1.2 Intellectual property rights</p> <p>12.1.4 Data protection and privacy of personal information</p> <p>12.1.6 Regulation of cryptographic controls</p> <p>12.1.7 Collection of evidence</p>		<p>the security of the system.</p>	
<p>AP 01.10 Develop and Deploy Safe and Secure Products and Services</p>	<p>8.2 <i>System planning and acceptance</i></p> <p>9.2 <i>User access management</i></p> <p>9.2.1 User registration</p> <p>9.2.2 Privilege management</p> <p>9.2.3 User password management</p> <p>9.4 <i>Network access control</i></p> <p>9.4.2 Enforced path</p> <p>9.4.3 User authentication for external connections</p> <p>9.4.4 Node authentication</p> <p>9.4.5 Remote diagnostic port protection</p> <p>9.4.6 Segregation in networks</p> <p>9.4.7 Network connection control</p> <p>9.4.8 Network routing control</p> <p>9.5 <i>Operating system access control</i></p> <p>9.5.1 Automatic terminal identification</p> <p>9.5.2 Terminal log-on procedures</p> <p>9.5.3 User identification and authentication</p> <p>9.5.4 Password management system</p> <p>9.5.5 Use of system utilities</p> <p>9.5.6 Duress alarm to safeguard users</p>	<p>ADO_DEL Delivery</p> <p>ADO_IGS Installation, generation and start-up</p> <p>ADV_HLD High-level design</p> <p>ADV_IMP Implementation representation</p> <p>ADV_LLD Low-level design</p> <p>AGD_ADM Administrator Guidance</p> <p>AGD_USR User Guidance</p> <p>ALC_LCD Life cycle definition</p> <p>ALC_TAT Tools and techniques</p>	<p>BP.06.01 Identify the security assurance objectives.</p> <p>BP.09.01 Work with designers, developers, and users to ensure that appropriate parties have a common understanding of security input needs.</p> <p>BP.09.02 Determine the security constraints and considerations needed to make informed engineering choices.</p> <p>BP.09.03 Identify alternative solutions to security related engineering problems.</p> <p>BP.09.04 Analyze and prioritize engineering alternatives using security constraints and considerations.</p> <p>BP.10.01 Gain an understanding of the customer's security needs.</p> <p>BP.10.03 Identify the purpose of the system in order to determine the security context.</p> <p>BP.10.04 Capture a high-level security oriented view of the system operation.</p> <p>BP.10.05 Capture high-level goals that define</p>	<p>3.3.3 Development of Security Requirements Checklist</p>

**Table 1: Safety and Security Application Practices Mapped to Sources
Part 2 - Security Sources**

Safety and Security Application Practice	ISO/IEC 17799	ISO/IEC 15408 Common Criteria	ISO/IEC 21827 SSE-CMM	NIST 800-30
	9.5.7 Terminal time-out 9.5.8 Limitation of connection time 9.6 <i>Application access control</i> 9.6.1 Information access restriction 10.1 <i>Security requirements of system</i> 10.1.1 Security requirements analysis and specification 10.2 <i>Security in application systems</i> 10.2.1 Input data validation 10.2.2 Control of internal processing 10.2.3 Message authentication 10.2.4 Output data validation 10.3 <i>Cryptographic controls</i> 10.3.2 Encryption 10.3.3 Digital signatures 10.3.5 Key management		the security of the system. BP.10.06 Define a consistent set of statements which define the protection to be implemented in the system. BP.10.07 Obtain agreement that the specified security meets the customer's needs. BP.16.08 Establish technical parameters BP.19.01 Define product evolution BP.19.02 Identify new product technologies	
AP 01.11 Objectively Evaluate Products	3.1.2 Review and evaluation 8.2.2 System acceptance 10.2.1 Input data validation 10.2.4 Output data validation 10.4.1 Control of operational software 10.4.2 Protection of system test data 10.5.2 Technical review of operating system changes 10.5.3 Restrictions on changes to software packages 12. Compliance 12.1 <i>Compliance with legal requirements</i> 12.2.2 Technical compliance checking	ADV_RCR Representation correspondence ATE_COV Coverage ATE_DPT Depth ATE_FUN Functional tests ATE_IND Independent testing	BP.06.04 Perform analysis of security assurance evidence. BP.08.05 Review the security posture of the system to identify necessary changes. BP.08.06 Manage the response to security relevant incidents. BP.11.01 Identify the solution to be verified and validated. BP.11.02 Define the approach and level of rigor for verifying and validating each solution. BP.11.03 Verify that the solution implements the requirements associated with the previous level of abstraction. BP.11.04 Validate the solution by showing that it satisfies the needs associated with the previous level of abstraction, ultimately meeting the customer's operational security needs. BP.11.05 Capture the verification and validation results for the other engineering groups. BP.14.04 Review risk assessment	3.3.2 System Security Testing

**Table 1: Safety and Security Application Practices Mapped to Sources
Part 2 - Security Sources**

Safety and Security Application Practice	ISO/IEC 17799	ISO/IEC 15408 Common Criteria	ISO/IEC 21827 SSE-CMM	NIST 800-30
AP 01.12 Establish Safety and Security Assurance Arguments	10.3.4 Non-repudiation services 12.1.7 Collection of evidence	AMA_EVD Evidence of assurance maintenance AMA_SIA Security impact analysis	BP.06.04 Perform analysis of security assurance evidence. BP.06.05 Provide a security assurance argument that demonstrates the customer's security needs are met.	<i>5.1 GOOD SECURITY PRACTICE</i> <i>5.2 KEYS FOR SUCCESS</i>
AP 01.13 Establish Independent Safety and Security Reporting	4.1.1 Management information security forum 4.1.3 Allocation of information security responsibilities	ALC_LCD Life cycle definition ATE_IND Independent testing	BP.01.01 Establish responsibilities and accountability for security controls and communicate them to everyone in the organization. BP.16.06 Define project interface	<i>4.3 APPROACH FOR CONTROL IMPLEMENTATION</i>
AP 01.14 Establish a Safety and Security Plan	<i>4.1 Information security infrastructure</i> 4.1.1 Management information security forum 4.1.2 Information security co-ordination 4.1.3 Allocation of information security responsibilities 6.1.1 Including security in job responsibility <i>8.2 System planning and acceptance</i>	ALC_LCD Life cycle definition AMA_AMP Assurance maintenance plan AMA_CAT TOE Component categorization report	BP.01.01 Establish responsibilities and accountability for security controls and communicate them to everyone in the organization. BP.06.02 Define a security assurance strategy to address all assurance objectives. BP.07.01 Define security engineering coordination objectives and relationships. BP.07.02 Identify coordination mechanisms for security engineering. BP.07.03 Facilitate security engineering coordination. BP.07.04 Use the identified mechanisms to coordinate decisions and recommendations related to security. BP.11.01 Identify the solution to be verified and validated. BP.13.01 Establish configuration management methodology BP.13.02 Identify configuration units BP.14.01 Develop risk management approach BP.16.01 Identify critical resources BP.16.02 Estimate project scope BP.16.03 Develop cost estimates BP.16.04 Determine project's process BP.16.05 Identify technical activities BP.16.06 Define project interface BP.16.07 Develop project schedules	<i>4.3 APPROACH FOR CONTROL IMPLEMENTATION</i> <i>5.1 GOOD SECURITY PRACTICE</i> <i>5.2 KEYS FOR SUCCESS</i>

**Table 1: Safety and Security Application Practices Mapped to Sources
Part 2 - Security Sources**

Safety and Security Application Practice	ISO/IEC 17799	ISO/IEC 15408 Common Criteria	ISO/IEC 21827 SSE-CMM	NIST 800-30
			BP.16.09 Develop technical management plan BP.16.10 Review and approve project plans BP.19.04 Ensure critical components availability	
AP 01.15 Select and Manage Suppliers, Products and Services	4.2 <i>Security of third party access</i> 4.2.1 Identification of risks from third party access 4.2.2 Security requirements in third party contracts 4.3 <i>Outsourcing</i> 4.3.1 Security requirements in outsourcing contracts 6.1 <i>Security in job definition and resourcing</i> 8.1.6 External facilities management 10.4.1 Control of operational software 10.5.5 Outsourced software development		BP.16.06 Define project interface BP.16.09 Develop technical management plan BP.22.01 Identify systems components or services BP.22.02 Identify competent suppliers or vendors BP.22.03 Choose suppliers or vendors BP.22.04 Provide expectations BP.22.05 Maintain communications	
AP 01.16 Monitor and Control Activities and Products	4.1.4 Authorization process for information processing facilities 4.1.7 Independent review of information security 6.3.5 Disciplinary process 8.1.2 Operational change control 9.2.4 Review of user access rights 10.4.1 Control of operational software 10.4.3 Access control to program source library 10.5 <i>Security in development and support processes</i> 10.5.1 Change control procedures 10.5.2 Technical review of operating system changes 12.1 <i>Compliance with legal requirements</i> 12.1.6 Regulation of cryptographic controls 12.2 <i>Review of security policy and technical compliance</i> 12.2.1 Compliance with security policy 12.2.2 Technical compliance checking 12.3.1 System audit controls	ACM_CAP Capabilities ACM_SCP Scope ALC_FLR Flaw remediation	BP.01.02 Manage the configuration of system security controls. BP.07.03 Facilitate security engineering coordination. BP.07.04 Use the identified mechanisms to coordinate decisions and recommendations related to security. BP.08.06 Manage the response to security relevant incidents. BP.12.01 Monitor conformance to the defined process BP.12.02 Measure work product quality BP.12.03 Measure quality of the process BP.12.04 Analyze quality measurements BP.12.05 Obtain participation BP.12.06 Initiate quality improvement activities BP.12.07 Detect need for corrective actions BP.13.01 Establish configuration management methodology BP.13.02 Identify configuration units BP.13.03 Maintain work product baselines	

**Table 1: Safety and Security Application Practices Mapped to Sources
Part 2 - Security Sources**

Safety and Security Application Practice	ISO/IEC 17799	ISO/IEC 15408 Common Criteria	ISO/IEC 21827 SSE-CMM	NIST 800-30
			BP.13.04 Control changes BP.13.05 Communicate configuration status BP.15.01 Direct technical effort BP.15.02 Track project resources BP.15.03 Track technical parameters BP.15.04 Review project performance BP.15.05 Analyze project issues BP.15.06 Take corrective action BP.17.01 Establish process goals BP.17.02 Collect process assets BP.17.03 Develop organization's security engineering process BP.17.04 Define tailoring guidelines BP.18.01 Appraise the process BP.18.02 Plan process improvements BP.18.03 Change the standard process BP.18.04 Communicate process improvements BP.19.03 Adapt development processes	

Table 2: Safety Sources Mapped to Safety and Security Application Practices
Part 1 - Defence Standard 00-56, Safety Management Requirements for Defence Systems

DEF STAN 0056	Safety and Security Application Practice
4 General Principles	
<i>4.2 Introduction</i>	
4.2.1	AP 01.12 Establish Safety and Security Assurance Arguments
4.2.2	AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks AP 01.11 Objectively Evaluate Products AP 01.12 Establish Safety and Security Assurance Arguments AP 01.14 Establish a Safety and Security Plan AP 01.16 Monitor and Control Activities and Products
<i>4.3 Safety Management</i>	
4.3.1	AP 01.14 Establish a Safety and Security Plan
4.3.2	AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.14 Establish a Safety and Security Plan
4.3.3	AP 01.13 Establish Independent Safety and Security Reporting AP 01.14 Establish a Safety and Security Plan
<i>4.4 System Safety Analysis</i>	
4.4.1 General	AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.11 Objectively Evaluate Products AP 01.12 Establish Safety and Security Assurance Arguments
4.4.2 Mandatory Activities	AP 01.04 Monitor Operations and Report Incidents AP 01.03 Ensure Integrity of Safety and Security Information AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks AP 01.11 Objectively Evaluate Products
4.4.3 Hazard Identification and Refinement	AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks
4.4.4 Risk Estimation	AP 01.07 Analyze and Prioritize Risks
4.4.5 Safety Compliance Assessment	AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.11 Objectively Evaluate Products AP 01.16 Monitor and Control Activities and Products
<i>4.5 Safety Verification</i>	AP 01.04 Monitor Operations and Report Incidents AP 01.11 Objectively Evaluate Products
<i>4.6 Hazard Log</i>	AP 01.04 Monitor Operations and Report Incidents AP 01.12 Establish Safety and Security Assurance Arguments
<i>4.7 Safety Case</i>	AP 01.12 Establish Safety and Security Assurance Arguments
5 Management and Associated Documentation	
<i>5.1 General</i>	
<i>5.2 Safety Programme Plan</i>	
5.2.1	AP 01.14 Establish a Safety and Security Plan
5.2.2	AP 01.13 Establish Independent Safety and Security Reporting AP 01.14 Establish a Safety and Security Plan AP 01.15 Select and Manage Suppliers, Products and Services
5.2.3	AP 01.14 Establish a Safety and Security Plan
5.2.4	AP 01.14 Establish a Safety and Security Plan
<i>5.3 Key Appointments</i>	

Table 2: Safety Sources Mapped to Safety and Security Application Practices
Part 1 - Defence Standard 00-56, Safety Management Requirements for Defence Systems

DEF STAN 0056	Safety and Security Application Practice
5.3.1 Project Manager	AP 01.14 Establish a Safety and Security Plan
5.3.2 Project Safety Engineer	AP 01.14 Establish a Safety and Security Plan
5.3.3 Project Safety Committee	AP 01.14 Establish a Safety and Security Plan
5.3.4 Independent Safety Auditor	AP 01.01 Ensure Safety and Security Competency AP 01.03 Ensure Integrity of Safety and Security Information AP 01.11 Objectively Evaluate Products AP 01.12 Establish Safety and Security Assurance Arguments AP 01.13 Establish Independent Safety and Security Reporting AP 01.14 Establish a Safety and Security Plan AP 01.16 Monitor and Control Activities and Products
5.3.5 Quality of staff	AP 01.01 Ensure Safety and Security Competency
<i>5.4 Safety Review</i>	
5.4.1	AP 01.11 Objectively Evaluate Products AP 01.16 Monitor and Control Activities and Products
5.4.2	AP 01.12 Establish Safety and Security Assurance Arguments AP 01.16 Monitor and Control Activities and Products
5.4.3	AP 01.14 Establish a Safety and Security Plan
<i>5.5 Quality Assurance</i>	
5.5.1	AP 01.16 Monitor and Control Activities and Products
5.5.2	AP 01.14 Establish a Safety and Security Plan AP 01.16 Monitor and Control Activities and Products
5.5.3	AP 01.02 Establish Qualified Work Environment AP 01.16 Monitor and Control Activities and Products
<i>5.6 Configuration Management</i>	
5.6.1	AP 01.14 Establish a Safety and Security Plan
5.6.2	AP 01.16 Monitor and Control Activities and Products
5.6.3	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.16 Monitor and Control Activities and Products
<i>5.7 Monitoring and Control of Sub-contractors</i>	
5.7.1	AP 01.11 Objectively Evaluate Products AP 01.15 Select and Manage Suppliers, Products and Services
5.7.2	AP 01.15 Select and Manage Suppliers, Products and Services
5.7.3	AP 01.06 Identify Safety and Security Risks AP 01.11 Objectively Evaluate Products AP 01.12 Establish Safety and Security Assurance Arguments AP 01.15 Select and Manage Suppliers, Products and Services AP 01.16 Monitor and Control Activities and Products
5.7.4	AP 01.14 Establish a Safety and Security Plan AP 01.15 Select and Manage Suppliers, Products and Services
5.7.5	AP 01.14 Establish a Safety and Security Plan AP 01.15 Select and Manage Suppliers, Products and Services AP 01.16 Monitor and Control Activities and Products
<i>5.8 Hazard Log</i>	
5.8.1	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.12 Establish Safety and Security Assurance Arguments
5.8.2	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.12 Establish Safety and Security Assurance Arguments
5.8.3	AP 01.04 Monitor Operations and Report Incidents

Table 2: Safety Sources Mapped to Safety and Security Application Practices
Part 1 - Defence Standard 00-56, Safety Management Requirements for Defence Systems

DEF STAN 0056	Safety and Security Application Practice
	AP 01.12 Establish Safety and Security Assurance Arguments
5.8.4	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.12 Establish Safety and Security Assurance Arguments
5.8.5	AP 01.14 Establish a Safety and Security Plan
5.8.6	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.12 Establish Safety and Security Assurance Arguments
5.8.7	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.12 Establish Safety and Security Assurance Arguments
5.8.8	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.12 Establish Safety and Security Assurance Arguments
5.8.9	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.12 Establish Safety and Security Assurance Arguments
<i>5.9 Design Documentation</i>	AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.11 Objectively Evaluate Products
6 Safety Requirements	
6.1	AP 01.10 Develop and Deploy Safe and Secure Products and Services
6.2	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.12 Establish Safety and Security Assurance Arguments
7 System Safety Analysis	
<i>7.1 Introduction</i>	AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan AP 01.11 Objectively Evaluate Products AP 01.14 Establish a Safety and Security Plan
<i>7.2 Hazard Identification</i>	
7.2.1 General	AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks
7.2.2 Preliminary Hazard Listing	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.06 Identify Safety and Security Risks AP 01.12 Establish Safety and Security Assurance Arguments
7.2.3 Preliminary Hazard Analysis	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.07 Analyze and Prioritize Risks AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan AP 01.12 Establish Safety and Security Assurance Arguments AP 01.10 Develop and Deploy Safe and Secure Products and Services
7.2.4 System Hazard Analysis	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.07 Analyze and Prioritize Risks AP 01.12 Establish Safety and Security Assurance Arguments
7.2.5 System Change Hazard Analysis	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.04 Monitor Operations and Report Incidents AP 01.07 Analyze and Prioritize Risks AP 01.12 Establish Safety and Security Assurance Arguments AP 01.16 Monitor and Control Activities and Products
<i>7.3 Safety Criteria Definition</i>	
7.3.1 Introduction	AP 01.09 Determine Regulatory Requirements, Laws and Standards
7.3.2 Formulation of the Safety Analysis Tables	AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.07 Analyze and Prioritize Risks AP 01.14 Establish a Safety and Security Plan AP 01.12 Establish Safety and Security Assurance Arguments
7.3.3 Determination of Design Rules	AP 01.03 Ensure Integrity of Safety and Security Information

Table 2: Safety Sources Mapped to Safety and Security Application Practices
Part 1 - Defence Standard 00-56, Safety Management Requirements for Defence Systems

DEF STAN 0056	Safety and Security Application Practice
and Techniques	AP 01.02 Establish Qualified Work Environment AP 01.12 Establish Safety and Security Assurance Arguments AP 01.09 Determine Regulatory Requirements, Laws and Standards
7.3.4 Safety Criteria Report	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.07 Analyze and Prioritize Risks AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan AP 01.12 Establish Safety and Security Assurance Arguments
<i>7.4 Risk Estimation</i>	
7.4.1 Introduction	AP 01.07 Analyze and Prioritize Risks AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan
7.4.2 Safety Integrity	AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan AP 01.10 Develop and Deploy Safe and Secure Products and Services
7.4.3 Claim limits	AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.14 Establish a Safety and Security Plan
7.4.4 Accident Sequences	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.07 Analyze and Prioritize Risks AP 01.12 Establish Safety and Security Assurance Arguments
7.4.5 Categorization of Accidents	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.07 Analyze and Prioritize Risks AP 01.12 Establish Safety and Security Assurance Arguments
7.4.6 Accident Probability Targets	AP 01.07 Analyze and Prioritize Risks AP 01.09 Determine Regulatory Requirements, Laws and Standards
7.4.7 Hazard Probability Targets	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.07 Analyze and Prioritize Risks AP 01.12 Establish Safety and Security Assurance Arguments AP 01.09 Determine Regulatory Requirements, Laws and Standards
7.4.8 Apportionment of Hazard Probability Targets	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.12 Establish Safety and Security Assurance Arguments AP 01.09 Determine Regulatory Requirements, Laws and Standards
<i>7.5 Safety Compliance Assessment</i>	
7.5.1	AP 01.11 Objectively Evaluate Products
7.5.2	AP 01.11 Objectively Evaluate Products AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan AP 01.16 Monitor and Control Activities and Products
7.5.3	AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan
7.5.4	AP 01.14 Establish a Safety and Security Plan
7.5.5	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan AP 01.11 Objectively Evaluate Products AP 01.12 Establish Safety and Security Assurance Arguments
7.5.6	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.11 Objectively Evaluate Products AP 01.12 Establish Safety and Security Assurance Arguments
7.5.7	AP 01.04 Monitor Operations and Report Incidents AP 01.11 Objectively Evaluate Products AP 01.12 Establish Safety and Security Assurance Arguments AP 01.16 Monitor and Control Activities and Products
8 Data Management	

Table 2: Safety Sources Mapped to Safety and Security Application Practices
Part 1 - Defence Standard 00-56, Safety Management Requirements for Defence Systems

DEF STAN 0056	Safety and Security Application Practice
8.1	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.04 Monitor Operations and Report Incidents AP 01.14 Establish a Safety and Security Plan AP 01.16 Monitor and Control Activities and Products
8.2	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.04 Monitor Operations and Report Incidents AP 01.16 Monitor and Control Activities and Products
8.3	AP 01.14 Establish a Safety and Security Plan AP 01.03 Ensure Integrity of Safety and Security Information AP 01.12 Establish Safety and Security Assurance Arguments
9 Test Programme	
9.1	AP 01.11 Objectively Evaluate Products
9.2	AP 01.11 Objectively Evaluate Products AP 01.14 Establish a Safety and Security Plan AP 01.15 Select and Manage Suppliers, Products and Services
9.3	AP 01.14 Establish a Safety and Security Plan
9.4	AP 01.04 Monitor Operations and Report Incidents AP 01.11 Objectively Evaluate Products
10 Work Programme	
10.1	AP 01.14 Establish a Safety and Security Plan
10.2	AP 01.14 Establish a Safety and Security Plan

Table 2: Safety Sources Mapped to Safety and Security Application Practices
Part - 2 IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC 61508	Safety and Security Application Practices
5 Documentation	
<i>5.2 Requirements</i>	
5.2.1 (Part 1)	AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.11 Objectively Evaluate Products
5.2.2 (Part 1)	AP 01.14 Establish a Safety and Security Plan
5.2.3 (Part 1)	AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.11 Objectively Evaluate Products AP 01.12 Establish Safety and Security Assurance Arguments
5.2.4 (Part 1)	AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.03 Insure Integrity of Safety and Security Information
5.2.5 (Part 1)	AP 01.03 Insure Integrity of Safety and Security Information
5.2.6 (Part 1)	AP 01.03 Insure Integrity of Safety and Security Information
5.2.7 (Part 1)	AP 01.03 Insure Integrity of Safety and Security Information
5.2.8 (Part 1)	AP 01.03 Insure Integrity of Safety and Security Information
5.2.9 (Part 1)	AP 01.16 Monitor and Control Activities and Products
5.2.10 (Part 1)	AP 01.03 Insure Integrity of Safety and Security Information AP 01.16 Monitor and Control Activities and Products
5.2.11 (Part 1)	AP 01.16 Monitor and Control Activities and Products
6. Management of functional safety	
<i>6.2 Requirements (Part 1)</i>	
6.2.1 (Part 1)	AP 01.14 Establish a Safety and Security Plan
6.2.2 (Part 1)	AP 01.01 Ensure Safety and Security Competency AP 01.04 Monitor Operations and Report Incidents AP 01.03 Insure Integrity of Safety and Security Information AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.11 Objectively Evaluate Products AP 01.12 Establish Safety and Security Assurance Arguments AP 01.16 Monitor and Control Activities and Products
6.2.3 (Part 1)	AP 01.16 Monitor and Control Activities and Products
6.2.4 (Part 1)	AP 01.14 Establish a Safety and Security Plan
6.2.5 (Part 1)	AP 01.15 Select and Manage Suppliers, Products and Services AP 01.16 Monitor and Control Activities and Products
7 Overall safety lifecycle requirements	
<i>7.1 General</i>	
7.1.4 Requirements (Part 1)	AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.14 Establish a Safety and Security Plan AP 01.16 Monitor and Control Activities and Products AP 01.11 Objectively Evaluate Products
<i>7.2 Concept</i>	
7.2.2 Requirements (Part 1)	AP 01.03 Insure Integrity of Safety and Security Information AP 01.06 Identify Safety and Security Risks AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.12 Establish Safety and Security Assurance Arguments
<i>7.3 Overall Scope Definition</i>	
7.3.2 Requirements (Part 1)	AP 01.03 Insure Integrity of Safety and Security Information AP 01.06 Identify Safety and Security Risks AP 01.12 Establish Safety and Security Assurance Arguments
<i>7.4 Hazard and risk analysis</i>	

Table 2: Safety Sources Mapped to Safety and Security Application Practices
Part - 2 IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC 61508	Safety and Security Application Practices
7.4.1 Objectives	
7.4.2 Requirements (Part 1)	AP 01.03 Insure Integrity of Safety and Security Information AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.12 Establish Safety and Security Assurance Arguments
7.5 Overall Safety Requirements	
7.5.2 Requirements (Part 1)	AP 01.07 Analyze and Prioritize Risks AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.10 Develop and Deploy Safe and Secure Products and Services
7.6 Safety Requirements Allocation	
7.6.2 Requirements (Part 1)	AP 01.01 Ensure Safety and Security Competency AP 01.03 Insure Integrity of Safety and Security Information AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.12 Establish Safety and Security Assurance Arguments
7.7 Overall operation and maintenance planning	
7.7.2 Requirements (Part 1)	AP 01.03 Insure Integrity of Safety and Security Information AP 01.14 Establish a Safety and Security Plan
7.8 Overall safety validation planning	
7.8.2 Requirements (Part 1)	AP 01.11 Objectively Evaluate Products AP 01.14 Establish a Safety and Security Plan
7.9 Overall installation and commissioning plan	
7.9.2 Requirements (Part 1)	AP 01.14 Establish a Safety and Security Plan
7.10 Realisation: E/E/PES	
7.10.2 Requirements (see parts 2 and 3)	
7.11 Realisation: other technology	
7.11.2 Requirements (not covered in the standard)	
7.12 Realisation: external risk reduction facilities	
7.12.2 Requirements (not covered in the standard)	
7.13 Overall installation and commissioning	
7.13.2 Requirements (Part 1)	AP 01.03 Insure Integrity of Safety and Security Information AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.12 Establish Safety and Security Assurance Arguments AP 01.16 Monitor and Control Activities and Products
7.14 Overall Safety Validation	
7.14.2 Requirements (Part 1)	AP 01.02 Establish Qualified Work Environment AP 01.03 Insure Integrity of Safety and Security Information AP 01.11 Objectively Evaluate Products AP 01.12 Establish Safety and Security Assurance Arguments
7.15 Overall operation, maintenance and repair	

Table 2: Safety Sources Mapped to Safety and Security Application Practices
Part - 2 IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC 61508	Safety and Security Application Practices
7.15.2 Requirements (Part 1)	AP 01.03 Insure Integrity of Safety and Security Information AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.11 Objectively Evaluate Products AP 01.14 Establish a Safety and Security Plan AP 01.16 Monitor and Control Activities and Products
<i>7.16 Overall modification and retrofit</i>	
7.16.2 Requirements (Part 1)	AP 01.03 Insure Integrity of Safety and Security Information AP 01.07 Analyze and Prioritize Risks AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.12 Establish Safety and Security Assurance Arguments AP 01.14 Establish a Safety and Security Plan AP 01.16 Monitor and Control Activities and Products
<i>7.17 Decommissioning or disposal</i>	
7.17.2 Requirements (Part 1)	AP 01.03 Insure Integrity of Safety and Security Information AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks AP 01.16 Monitor and Control Activities and Products AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.12 Establish Safety and Security Assurance Arguments AP 01.14 Establish a Safety and Security Plan
<i>7.18 Verification</i>	Verification
7.18.2 Requirements (Part 1)	AP 01.03 Insure Integrity of Safety and Security Information AP 01.11 Objectively Evaluate Products AP 01.12 Establish Safety and Security Assurance Arguments AP 01.14 Establish a Safety and Security Plan
8 Functional safety assessment	
<i>8.2 Requirements</i>	
8.2.1 (Part 1)	AP 01.11 Objectively Evaluate Products AP 01.14 Establish a Safety and Security Plan
8.2.2 (Part 1)	AP 01.03 Insure Integrity of Safety and Security Information
8.2.3 (Part 1)	AP 01.11 Objectively Evaluate Products
8.2.4 (Part 1)	AP 01.11 Objectively Evaluate Products
8.2.5 (Part 1)	AP 01.02 Establish Qualified Work Environment Establish Qualified Work Environment AP 01.11 Objectively Evaluate Products
8.2.6 (Part 1)	AP 01.11 Objectively Evaluate Products
8.2.7 (Part 1)	AP 01.11 Objectively Evaluate Products AP 01.14 Establish a Safety and Security Plan
8.2.8 (Part 1)	AP 01.01 Ensure Safety and Security Competency AP 01.11 Objectively Evaluate Products AP 01.13 Establish Independent Safety and Security Reporting AP 01.14 Establish a Safety and Security Plan
8.2.9 (Part 1)	AP 01.14 Establish a Safety and Security Plan
8.2.10 (Part 1)	AP 01.11 Objectively Evaluate Products
8.2.11 (Part 1)	AP 01.01 Ensure Safety and Security Competency
8.2.12 (Part 1)	AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.11 Objectively Evaluate Products AP 01.13 Establish Independent Safety and Security Reporting
8.2.13 (Part 1)	AP 01.01 Ensure Safety and Security Competency

Table 2: Safety Sources Mapped to Safety and Security Application Practices
Part - 2 IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC 61508	Safety and Security Application Practices
	AP 01.11 Objectively Evaluate Products AP 01.13 Establish Independent Safety and Security Reporting
8.2.14 (Part 1)	AP 01.11 Objectively Evaluate Products AP 01.13 Establish Independent Safety and Security Reporting
EC61508 Pt 2	Safety and Security Application Practices
7 E/E/EPS safety lifecycle requirements	
<i>7.1 General</i>	
7.1.3 Requirements (Part 2)	AP 01.14 Establish a Safety and Security Plan AP 01.16 Monitor and Control Activities and Products
<i>7.2 E/E/EPS safety requirements specification</i>	
7.2.2 General Requirements (Part 2)	AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.14 Establish a Safety and Security Plan
7.2.3 E/E/PES safety requirements (Part 2)	AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.10 Develop and Deploy Safe and Secure Products and Services
7.3 E/E/PES safety validation planning	
7.3.2 Requirements (Part 2)	AP 01.02 Establish Qualified Work Environment AP 01.11 Objectively Evaluate Products AP 01.14 Establish a Safety and Security Plan
<i>7.4 E/E/PES design and development</i>	
7.4.2 General Requirements (Part 2)	AP 01.03 Insure Integrity of Safety and Security Information AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.11 Objectively Evaluate Products AP 01.12 Establish Safety and Security Assurance Arguments AP 01.15 Select and Manage Suppliers, Products and Services
7.4.3 Requirements for the control of random hardware faults (Part 2)	AP 01.10 Develop and Deploy Safe and Secure Products and Services
7.4.4 Requirements for estimating the probability of hardware failure (Part 2)	AP 01.03 Insure Integrity of Safety and Security Information AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.11 Objectively Evaluate Products
7.4.5 Architectural constraints on hardware safety integrity (Part 2)	AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.10 Develop and Deploy Safe and Secure Products and Services
7.4.6 Requirements for proof tests and diagnostic tests (Part 2)	AP 01.02 Establish Qualified Work Environment AP 01.10 Develop and Deploy Safe and Secure Products and Services
7.4.7 Requirements for the avoidance of failures (Part 2)	AP 01.02 Establish Qualified Work Environment AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.11 Objectively Evaluate Products AP 01.14 Establish a Safety and Security Plan AP 01.15 Select and Manage Suppliers, Products and Services
7.4.8 Requirements for control of systematic faults (Part 2)	AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.12 Establish Safety and Security Assurance Arguments
7.4.9 Requirements for E/E/PES Implementation (Part 2)	AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.12 Establish Safety and Security Assurance Arguments
<i>7.5 E/E/PES integration</i>	
7.5.2 Requirements (Part 2)	AP 01.03 Insure Integrity of Safety and Security Information

Table 2: Safety Sources Mapped to Safety and Security Application Practices
Part - 2 IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC 61508	Safety and Security Application Practices
	AP 01.11 Objectively Evaluate Products AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.16 Monitor and Control Activities and Products
<i>7.6 E/E/PES operation and maintenance procedures</i>	
7.6.2 Requirements (Part 2)	AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.11 Objectively Evaluate Products
<i>7.7 E/E/EPS safety validation</i>	
7.7.2 Requirements (Part 2)	AP 01.02 Establish Qualified Work Environment AP 01.03 Insure Integrity of Safety and Security Information AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.11 Objectively Evaluate Products AP 01.12 Establish Safety and Security Assurance Arguments AP 01.14 Establish a Safety and Security Plan AP 01.15 Select and Manage Suppliers, Products and Services AP 01.16 Monitor and Control Activities and Products
<i>7.8 E/E/PES modification</i>	
7.8.2 Requirements (Part 2)	AP 01.01 Ensure Safety and Security Competency AP 01.03 Insure Integrity of Safety and Security Information AP 01.04 Monitor Operations and Report Incidents AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.11 Objectively Evaluate Products AP 01.14 Establish a Safety and Security Plan
<i>7.9 E/E/PES verification</i>	
7.9.2 Requirements (Part 2)	AP 01.03 Insure Integrity of Safety and Security Information AP 01.11 Objectively Evaluate Products AP 01.12 Establish Safety and Security Assurance Arguments AP 01.14 Establish a Safety and Security Plan
8 Functional safety assessment (see Part 1)	
IEC61508 Part 3	Safety and Security Application Practices
6 Software quality management system	
<i>6.2 Requirements</i>	
6.2.1 (Part 3)	AP 01.14 Establish a Safety and Security Plan
6.2.2 (Part 3)	AP 01.11 Objectively Evaluate Products AP 01.14 Establish a Safety and Security Plan AP 01.15 Select and Manage Suppliers, Products and Services
6.2.3	AP 01.16 Monitor and Control Activities and Products
7 Software safety lifecycle requirements	
<i>7.1 General</i>	
7.1.2 Requirements (Part 3)	AP 01.03 Insure Integrity of Safety and Security Information AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.14 Establish a Safety and Security Plan AP 01.16 Monitor and Control Activities and Products
<i>7.2 Software safety requirements specification</i>	
7.2.2 Requirements (Part 3)	AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.10 Develop and Deploy Safe and Secure Products and Services
<i>7.3 Software safety validation planning</i>	

Table 2: Safety Sources Mapped to Safety and Security Application Practices
Part - 2 IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC 61508	Safety and Security Application Practices
7.3.2 Requirements (Part 3)	AP 01.11 Objectively Evaluate Products AP 01.12 Establish Safety and Security Assurance Arguments AP 01.14 Establish a Safety and Security Plan
<i>7.4 Software design and development</i>	
7.4.2 General Requirements (Part 3)	AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.14 Establish a Safety and Security Plan AP 01.15 Select and Manage Suppliers, Products and Services
7.4.3 Requirements for software architecture (Part 3)	AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.12 Establish Safety and Security Assurance Arguments AP 01.14 Establish a Safety and Security Plan AP 01.15 Select and Manage Suppliers, Products and Services AP 01.16 Monitor and Control Activities and Products
7.4.4 Requirements for support tools and programming languages (Part 3)	AP 01.02 Establish Qualified Work Environment AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.11 Objectively Evaluate Products
7.4.5 Requirements for detailed design and development (Part 3)	AP 01.03 Insure Integrity of Safety and Security Information AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.11 Objectively Evaluate Products AP 01.14 Establish a Safety and Security Plan AP 01.15 Select and Manage Suppliers, Products and Services
7.4.6 Requirements for code implementation (Part 3)	AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.11 Objectively Evaluate Products
7.4.7 Requirements for software module testing (Part 3)	AP 01.03 Insure Integrity of Safety and Security Information AP 01.11 Objectively Evaluate Products AP 01.16 Monitor and Control Activities and Products
7.4.8 Requirements for software integration testing (Part 3)	AP 01.03 Insure Integrity of Safety and Security Information AP 01.11 Objectively Evaluate Products AP 01.14 Establish a Safety and Security Plan AP 01.16 Monitor and Control Activities and Products
<i>7.5 Programmable electronics integration (hardware and software)</i>	
7.5.2 Requirements (Part 3)	AP 01.02 Establish Qualified Work Environment AP 01.03 Insure Integrity of Safety and Security Information AP 01.11 Objectively Evaluate Products AP 01.14 Establish a Safety and Security Plan AP 01.16 Monitor and Control Activities and Products
<i>7.6 Software operation and modification procedures</i>	
7.6.2 Requirements (see 7.6 of part 2 and 7.8 of part 3.)	
<i>7.7 Software safety validation</i>	
7.7.2 Requirements(Part 3)	AP 01.02 Establish Qualified Work Environment AP 01.03 Insure Integrity of Safety and Security Information AP 01.11 Objectively Evaluate Products AP 01.14 Establish a Safety and Security Plan AP 01.15 Select and Manage Suppliers, Products and Services AP 01.16 Monitor and Control Activities and Products
<i>7.8 Software modification</i>	
7.8.2 Requirements (Part 3)	AP 01.03 Insure Integrity of Safety and Security Information AP 01.10 Develop and Deploy Safe and Secure Products and Services

Table 2: Safety Sources Mapped to Safety and Security Application Practices
Part - 2 IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC 61508	Safety and Security Application Practices
	AP 01.11 Objectively Evaluate Products AP 01.12 Establish Safety and Security Assurance Arguments AP 01.14 Establish a Safety and Security Plan AP 01.16 Monitor and Control Activities and Products
<i>7.9 Software verification</i>	
7.9.2 Requirements (Part 3)	AP 01.02 Establish Qualified Work Environment AP 01.03 Insure Integrity of Safety and Security Information AP 01.11 Objectively Evaluate Products AP 01.12 Establish Safety and Security Assurance Arguments AP 01.14 Establish a Safety and Security Plan
8 Functional safety assessment (see Part 1)	

Table 2: Safety Sources Mapped to Safety and Security Application Practices
Part 3 – Military Standard System Safety Program Requirements, MIL-STD-882C

MIL-STD-882C	Safety and Security Application Practices
4 General Requirements	
<i>4.1 System safety program</i>	AP 01.14 Establish a Safety and Security Plan AP 01.16 Monitor and Control Activities and Products
4.1.1 Management System	AP 01.04 Monitor Operations and Report Incidents AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan AP 01.14 Establish a Safety and Security Plan AP 01.16 Monitor and Control Activities and Products
4.1.2 Key system safety personnel	AP 01.01 Ensure Safety and Security Competency
4.1.3 Compliance	AP 01.16 Monitor and Control Activities and Products
4.1.4 Conflicting requirements	AP 01.14 Establish a Safety and Security Plan AP 01.16 Monitor and Control Activities and Products
<i>4.2 System safety program objectives</i>	AP 01.02 Establish Qualified Work Environment AP 01.03 Ensure Integrity of Safety and Security Information AP 01.04 Monitor Operations and Report Incidents AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.12 Establish Safety and Security Assurance Arguments AP 01.16 Monitor and Control Activities and Products
<i>4.3 System safety design requirements</i>	AP 01.02 Establish Qualified Work Environment AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan
<i>4.4 System safety precedence</i>	AP 01.14 Establish a Safety and Security Plan AP 01.10 Develop and Deploy Safe and Secure Products and Services
4.4.1 Design for minimum risk	AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan AP 01.10 Develop and Deploy Safe and Secure Products and Services
4.4.2 Incorporate safety devices	AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan AP 01.10 Develop and Deploy Safe and Secure Products and Services
4.4.3 Provide warning devices	AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan AP 01.10 Develop and Deploy Safe and Secure Products and Services
4.4.4 Develop procedures and training	AP 01.01 Ensure Safety and Security Competency AP 01.02 Establish Qualified Work Environment AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan AP 01.10 Develop and Deploy Safe and Secure Products and Services
<i>4.5 Risk assessment</i>	AP 01.07 Analyze and Prioritize Risks
4.5.1 Hazard severity	AP 01.07 Analyze and Prioritize Risks
4.5.2 Hazard probability	AP 01.07 Analyze and Prioritize Risks
4.5.3 Risk impact	AP 01.07 Analyze and Prioritize Risks
4.6 Action on identified hazards	AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan
4.6.1 Residual risk	AP 01.12 Establish Safety and Security Assurance Arguments
5. Detailed Requirements	
Task 101 System Safety Program	AP 01.01 Ensure Safety and Security Competency AP 01.04 Monitor Operations and Report Incidents AP 01.13 Establish Independent Safety and Security Reporting AP 01.14 Establish a Safety and Security Plan

Table 2: Safety Sources Mapped to Safety and Security Application Practices
Part 3 – Military Standard System Safety Program Requirements, MIL-STD-882C

MIL-STD-882C	Safety and Security Application Practices
Task 102 System Safety Program Plan	AP 01.01 Ensure Safety and Security Competency AP 01.02 Establish Qualified Work Environment AP 01.03 Ensure Integrity of Safety and Security Information AP 01.04 Monitor Operations and Report Incidents AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.11 Objectively Evaluate Products AP 01.13 Establish Independent Safety and Security Reporting AP 01.14 Establish a Safety and Security Plan AP 01.15 Select and Manage Suppliers, Products and Services AP 01.16 Monitor and Control Activities and Products AP 01.10 Develop and Deploy Safe and Secure Products and Services
Task 103 Integration/ Management of Associate contractors, subcontractors, and architect and engineering firms	AP 01.14 Establish a Safety and Security Plan AP 01.15 Select and Manage Suppliers, Products and Services
Task 104 System safety program reviews/audits	AP 01.16 Monitor and Control Activities and Products
Task 105 System safety group/system working group support	AP 01.14 Establish a Safety and Security Plan
Task 106 Hazard Tracking and Risk Resolution	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.12 Establish Safety and Security Assurance Arguments
Task 107 System Safety Progress Summary	AP 01.16 Monitor and Control Activities and Products
Task 201 Preliminary Hazard List	AP 01.06 Identify Safety and Security Risks
Task 202 Preliminary Hazard Analysis	AP 01.07 Analyze and Prioritize Risks AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan AP 01.10 Develop and Deploy Safe and Secure Products and Services
Task 203 Safety Requirements/ Criteria Analysis	AP 01.02 Establish Qualified Work Environment AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.16 Monitor and Control Activities and Products
Task 204 Subsystem Hazard Analysis	AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.11 Objectively Evaluate Products
Task 205 System Hazard Analysis	AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.11 Objectively Evaluate Products
Task 206 Operate and Support Hazard Analysis	AP 01.01 Ensure Safety and Security Competency AP 01.02 Establish Qualified Work Environment AP 01.04 Monitor Operations and Report Incidents AP 01.05 Ensure Business Continuity AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks

Table 2: Safety Sources Mapped to Safety and Security Application Practices
Part 3 – Military Standard System Safety Program Requirements, MIL-STD-882C

MIL-STD-882C	Safety and Security Application Practices
	AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.11 Objectively Evaluate Products
Task 207 Health Hazard Assessment	AP 01.02 Establish Qualified Work Environment AP 01.05 Ensure Business Continuity AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.11 Objectively Evaluate Products
Task 301 Safety Assessment	AP 01.11 Objectively Evaluate Products AP 01.12 Establish Safety and Security Assurance Argument
Task 302 Test and Evaluation Safety	AP 01.02 Establish Qualified Work Environment AP 01.11 Objectively Evaluate Products AP 01.12 Establish Safety and Security Assurance Argument
Task 303 Safety Review of Engineering Change Proposals, Specification Change Notices, Software Problem Reports, and Requests for Deviation/ Waiver	AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.16 Monitor and Control Activities and Products
Task 401 Safety Verification	AP 01.11 Objectively Evaluate Products
Task 402 Safety Compliance Assessment	AP 01.11 Objectively Evaluate Products AP 01.12 Establish Safety and Security Assurance Arguments AP 01.16 Monitor and Control Activities and Products
Task 403 Explosive Hazard Classification and Characteristics Data	AP 01.11 Objectively Evaluate Products AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks
Task 404 Explosive Ordnance Disposal Source Data	AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.11 Objectively Evaluate Products

Table 2: Safety Sources Mapped to Safety and Security Application Practices
Part 4 – Standard Practice for System Safety, MIL-STD-882D

MIL-STD-882D	Safety and Security Application Practice
4 General Requirements	
4.1 Documentation of the system safety approach	AP 01.14 Establish a Safety and Security Plan
4.2 Identification of hazards	AP 01.06 Identify Safety and Security Risks
4.3 Assessment of mishap risk	AP 01.07 Analyze and Prioritize Risks
4.4 Identification of mishap risk mitigation measures	AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan AP 01.10 Develop and Deploy Safe and Secure Products and Services
4.5 Reduction of mishap risk to an acceptable level	AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan
4.6 Verification of mishap risk reduction	AP 01.02 Establish Qualified Work Environment AP 01.11 Objectively Evaluate Products AP 01.12 Establish Safety and Security Assurance Arguments
4.7 Review of hazards and acceptance of residual mishap risk by the appropriate authority	AP 01.12 Establish Safety and Security Assurance Arguments AP 01.14 Establish a Safety and Security Plan AP 01.16 Monitor and Control Activities and Products
4.8 Tracking of hazards, their closures, and residual mishap risk	AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan
5 Detailed requirements	AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.15 Select and Manage Suppliers, Products and Services

Table 3: Security Sources Mapped to Safety and Security Application Practices
Part 1 - ISO/IEC 17799 Information technology - Code of practice for information security management

ISO/IEC 17799	Safety and Security Application Practice
3. Security policy	
<i>3.1 Information security policy</i>	AP 01.09 Determine Regulatory Requirements, Laws and Standards
3.1.1 Information security policy document	AP 01.09 Determine Regulatory Requirements, Laws and Standards
3.1.2 Review and evaluation	AP 01.11 Objectively Evaluate Products
4. Organizational security	
<i>4.1 Information security infrastructure</i>	AP 01.14 Establish a Safety and Security Plan
4.1.1 Management information security forum	AP 01.13 Establish Independent Safety and Security Reporting AP 01.14 Establish a Safety and Security Plan
4.1.2 Information security co-ordination	AP 01.14 Establish a Safety and Security Plan
4.1.3 Allocation of information security responsibilities	AP 01.01 Ensure Safety and Security Competency AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.13 Establish Independent Safety and Security Reporting AP 01.14 Establish a Safety and Security Plan
4.1.4 Authorization process for information processing facilities	AP 01.02 Establish Qualified Work Environment AP 01.16 Monitor and Control Activities and Products
4.1.5 Specialist information security advice	AP 01.01 Ensure Safety and Security Competency
4.1.6 Co-operation between organizations	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan AP 01.09 Determine Regulatory Requirements, Laws and Standards
4.1.7 Independent review of information security	AP 01.16 Monitor and Control Activities and Products
<i>4.2 Security of third party access</i>	AP 01.02 Establish Qualified Work Environment AP 01.15 Select and Manage Suppliers, Products and Services
4.2.1 Identification of risks from third party access	AP 01.02 Establish Qualified Work Environment AP 01.06 Identify Safety and Security Risks AP 01.15 Select and Manage Suppliers, Products and Services
4.2.2 Security requirements in third party contracts	AP 01.02 Establish Qualified Work Environment AP 01.15 Select and Manage Suppliers, Products and Services
<i>4.3 Outsourcing</i>	AP 01.15 Select and Manage Suppliers, Products and Services
4.3.1 Security requirements in outsourcing contracts	AP 01.15 Select and Manage Suppliers, Products and Services
5. Asset classification and control	
<i>5.1 Accountability for assets</i>	AP 01.03 Ensure Integrity of Safety and Security Information
5.1.1 Inventory of assets	AP 01.02 Establish Qualified Work Environment
<i>5.2 Information classification</i>	AP 01.03 Ensure Integrity of Safety and Security Information
5.2.1 Classification guidelines	AP 01.03 Ensure Integrity of Safety and Security Information
5.2.2 Information labeling and handling	AP 01.03 Ensure Integrity of Safety and Security Information
6. Personnel security	
<i>6.1 Security in job definition and resourcing</i>	AP 01.02 Establish Qualified Work Environment AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.15 Select and Manage Suppliers, Products and Services
6.1.1 Including security in job responsibility	AP 01.14 Establish a Safety and Security Plan
6.1.2 Personnel screening and policy	AP 01.02 Establish Qualified Work Environment
6.1.3 Confidentiality agreements	AP 01.03 Ensure Integrity of Safety and Security Information
6.1.4 Terms and conditions of	AP 01.03 Ensure Integrity of Safety and Security Information

Table 3: Security Sources Mapped to Safety and Security Application Practices
Part 1 - ISO/IEC 17799 Information technology - Code of practice for information security management

ISO/IEC 17799	Safety and Security Application Practice
employment	
6.2 <i>User training</i>	AP 01.01 Ensure Safety and Security Competency AP 01.02 Establish Qualified Work Environment
6.2.1 Information security education and training	AP 01.01 Ensure Safety and Security Competency AP 01.02 Establish Qualified Work Environment
6.3 <i>Responding to security incidents and malfunctions</i>	AP 01.04 Monitor Operations and Report Incidents
6.3.1 Reporting security incidents	AP 01.04 Monitor Operations and Report Incidents
6.3.2 Reporting security weaknesses	AP 01.02 Establish Qualified Work Environment AP 01.04 Monitor Operations and Report Incidents
6.3.3 Reporting software malfunctions	AP 01.02 Establish Qualified Work Environment AP 01.04 Monitor Operations and Report Incidents
6.3.4 Learning from incidents	AP 01.03 Control Information AP 01.04 Monitor Operations and Report Incidents
6.3.5 Disciplinary process	AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.16 Monitor and Control Activities and Products
7. Physical and environmental security	
7.1 <i>Secure areas</i>	AP 01.02 Establish Qualified Work Environment
7.1.1 Physical security perimeter	AP 01.02 Establish Qualified Work Environment
7.1.2 Physical entry controls	AP 01.02 Establish Qualified Work Environment
7.1.3 Securing offices, rooms and facilities	AP 01.02 Establish Qualified Work Environment
7.1.4. Working in secure areas	AP 01.02 Establish Qualified Work Environment
7.1.5 Isolated delivery and loading areas	AP 01.02 Establish Qualified Work Environment
7.2 <i>Equipment security</i>	AP 01.02 Establish Qualified Work Environment AP 01.05 Ensure Business Continuity
7.2.1 Equipment siting and protection	AP 01.02 Establish Qualified Work Environment AP 01.05 Ensure Business Continuity
7.2.2 Power supplies	AP 01.02 Establish Qualified Work Environment AP 01.05 Ensure Business Continuity
7.2.3 Cabling security	AP 01.02 Establish Qualified Work Environment AP 01.05 Ensure Business Continuity
7.2.4 Equipment maintenance	AP 01.02 Establish Qualified Work Environment
7.2.5 Security of equipment off-premises	AP 01.02 Establish Qualified Work Environment
7.2.6 Secure disposal or re-use of equipment	AP 01.02 Establish Qualified Work Environment
7.3 <i>General controls</i>	AP 01.02 Establish Qualified Work Environment
7.3.1 Clear desk and clear screen policy	AP 01.02 Establish Qualified Work Environment AP 01.09 Determine Regulatory Requirements, Laws and Standards
7.3.2 Removal of property	AP 01.02 Establish Qualified Work Environment
8. Communications and operations management	
8.1 <i>Operational procedures and responsibilities</i>	AP 01.02 Establish Qualified Work Environment AP 01.04 Monitor Operations and Report Incidents
8.1.1 Documented operating procedures	AP 01.02 Establish Qualified Work Environment
8.1.2 Operational change control	AP 01.02 Establish Qualified Work Environment AP 01.16 Monitor and Control Activities and Products
8.1.3 Incident management procedures	AP 01.04 Monitor Operations and Report Incidents
8.1.4 Segregation of duties	AP 01.02 Establish Qualified Work Environment

Table 3: Security Sources Mapped to Safety and Security Application Practices
Part 1 - ISO/IEC 17799 Information technology - Code of practice for information security management

ISO/IEC 17799	Safety and Security Application Practice
8.1.5 Separation of development and operational facilities	AP 01.02 Establish Qualified Work Environment
8.1.6 External facilities management	AP 01.15 Select and Manage Suppliers, Products and Services
8.2 <i>System planning and acceptance</i>	AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.14 Establish a Safety and Security Plan
8.2.1 Capacity planning	AP 01.02 Establish Qualified Work Environment AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan
8.2.2 System acceptance	AP 01.11 Objectively Evaluate Products
8.3 <i>Protection against malicious software</i>	AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan
8.3.1 Controls against malicious software	AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan
8.4 <i>Housekeeping</i>	AP 01.02 Establish Qualified Work Environment AP 01.04 Monitor Operations and Report Incidents
8.4.1 Information back-up	AP 01.02 Establish Qualified Work Environment AP 01.05 Ensure Business Continuity
8.4.2 Operator logs	AP 01.04 Monitor Operations and Report Incidents
8.4.3 Fault logging	AP 01.04 Monitor Operations and Report Incidents
8.5 <i>Network management</i>	AP 01.02 Establish Qualified Work Environment
8.5.1 Network controls	AP 01.02 Establish Qualified Work Environment
8.6 <i>Media handling and security</i>	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.05 Ensure Business Continuity
8.6.1 Management of removable computer media	AP 01.03 Ensure Integrity of Safety and Security Information
8.6.2 Disposal of media	AP 01.03 Ensure Integrity of Safety and Security Information
8.6.3 Information handling procedures	AP 01.03 Ensure Integrity of Safety and Security Information
8.6.4 Security of system documentation	AP 01.03 Ensure Integrity of Safety and Security Information
8.7 <i>Exchanges of information and software</i>	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.09 Determine Regulatory Requirements, Laws and Standards
8.7.1 Information and software exchange agreements	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.09 Determine Regulatory Requirements, Laws and Standards
8.7.2 Security of media in transit	AP 01.03 Ensure Integrity of Safety and Security Information
8.7.3 Electronic commerce security	AP 01.03 Ensure Integrity of Safety and Security Information
8.7.4 Security of electronic mail	AP 01.02 Establish Qualified Work Environment AP 01.09 Determine Regulatory Requirements, Laws and Standards
8.7.5 Security of electronic office systems	AP 01.02 Establish Qualified Work Environment AP 01.09 Determine Regulatory Requirements, Laws and Standards
8.7.6 Publicly available systems	AP 01.03 Ensure Integrity of Safety and Security Information
8.7.7 Other forms of information exchange	AP 01.03 Ensure Integrity of Safety and Security Information
9. Access control	
9.1 <i>Business requirement for access control</i>	AP 01.03 Ensure Integrity of Safety and Security Information
9.1.1 Access control policy	AP 01.02 Establish Qualified Work Environment AP 01.03 Ensure Integrity of Safety and Security Information AP 01.09 Determine Regulatory Requirements, Laws and Standards
9.2 <i>User access management</i>	AP 01.02 Establish Qualified Work Environment AP 01.10 Develop and Deploy Safe and Secure Products and Services

Table 3: Security Sources Mapped to Safety and Security Application Practices
Part 1 - ISO/IEC 17799 Information technology - Code of practice for information security management

ISO/IEC 17799	Safety and Security Application Practice
9.2.1 User registration	AP 01.02 Establish Qualified Work Environment AP 01.10 Develop and Deploy Safe and Secure Products and Services
9.2.2 Privilege management	AP 01.02 Establish Qualified Work Environment AP 01.10 Develop and Deploy Safe and Secure Products and Services
9.2.3 User password management	AP 01.02 Establish Qualified Work Environment AP 01.10 Develop and Deploy Safe and Secure Products and Services
9.2.4 Review of user access rights	AP 01.02 Establish Qualified Work Environment AP 01.16 Monitor and Control Activities and Products
<i>9.3 User responsibilities</i>	AP 01.01 Ensure Safety and Security Competency AP 01.02 Establish Qualified Work Environment
9.3.1 Password use	AP 01.01 Ensure Safety and Security Competency AP 01.02 Establish Qualified Work Environment
9.3.2 Unattended user equipment	AP 01.01 Ensure Safety and Security Competency AP 01.02 Establish Qualified Work Environment
<i>9.4 Network access control</i>	AP 01.02 Establish Qualified Work Environment AP 01.10 Develop and Deploy Safe and Secure Products and Services
9.4.1 Policy on use of network services	AP 01.09 Determine Regulatory Requirements, Laws and Standards
9.4.2 Enforced path	AP 01.02 Establish Qualified Work Environment AP 01.10 Develop and Deploy Safe and Secure Products and Services
9.4.3 User authentication for external connections	AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan AP 01.10 Develop and Deploy Safe and Secure Products and Services
9.4.4 Node authentication	AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan AP 01.10 Develop and Deploy Safe and Secure Products and Services
9.4.5 Remote diagnostic port protection	AP 01.02 Establish Qualified Work Environment AP 01.10 Develop and Deploy Safe and Secure Products and Services
9.4.6 Segregation in networks	AP 01.10 Develop and Deploy Safe and Secure Products and Services
9.4.7 Network connection control	AP 01.10 Develop and Deploy Safe and Secure Products and Services
9.4.8 Network routing control	AP 01.10 Develop and Deploy Safe and Secure Products and Services
9.4.9 Security of network services	AP 01.02 Establish Qualified Work Environment
<i>9.5 Operating system access control</i>	AP 01.10 Develop and Deploy Safe and Secure Products and Services
9.5.1 Automatic terminal identification	AP 01.10 Develop and Deploy Safe and Secure Products and Services
9.5.2 Terminal log-on procedures	AP 01.10 Develop and Deploy Safe and Secure Products and Services
9.5.3 User identification and authentication	AP 01.10 Develop and Deploy Safe and Secure Products and Services
9.5.4 Password management system	AP 01.10 Develop and Deploy Safe and Secure Products and Services
9.5.5 Use of system utilities	AP 01.10 Develop and Deploy Safe and Secure Products and Services
9.5.6 Duress alarm to safeguard users	AP 01.10 Develop and Deploy Safe and Secure Products and Services
9.5.7 Terminal time-out	AP 01.10 Develop and Deploy Safe and Secure Products and Services
9.5.8 Limitation of connection time	AP 01.10 Develop and Deploy Safe and Secure Products and Services
<i>9.6 Application access control</i>	AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.10 Develop and Deploy Safe and Secure Products and Services
9.6.1 Information access restriction	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.10 Develop and Deploy Safe and Secure Products and Services
9.6.2 Sensitive system isolation	AP 01.02 Establish Qualified Work Environment
<i>9.7 Monitoring system access and use</i>	AP 01.04 Monitor Operations and Report Incidents
9.7.1 Event logging	AP 01.04 Monitor Operations and Report Incidents

Table 3: Security Sources Mapped to Safety and Security Application Practices
Part 1 - ISO/IEC 17799 Information technology - Code of practice for information security management

ISO/IEC 17799	Safety and Security Application Practice
9.7.2 Monitoring system use	AP 01.02 Establish Qualified Work Environment AP 01.04 Monitor Operations and Report Incidents
9.7.3 Clock synchronization	AP 01.02 Establish Qualified Work Environment AP 01.04 Monitor Operations and Report Incidents
<i>9.8 Mobile computing and teleworking</i>	AP 01.02 Establish Qualified Work Environment
9.8.1 Mobile computing	AP 01.02 Establish Qualified Work Environment AP 01.09 Determine Regulatory Requirements, Laws and Standards
9.8.2 Teleworking	AP 01.02 Establish Qualified Work Environment AP 01.09 Determine Regulatory Requirements, Laws and Standards
10. Systems development and maintenance	
<i>10.1 Security requirements of systems</i>	AP 01.10 Develop and Deploy Safe and Secure Products and Services
10.1.1 Security requirements analysis and specification	AP 01.07 Analyze and Prioritize Risks AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan AP 01.10 Develop and Deploy Safe and Secure Products and Services
<i>10.2 Security in application systems</i>	AP 01.10 Develop and Deploy Safe and Secure Products and Services
10.2.1 Input data validation	AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.11 Objectively Evaluate Products
10.2.2 Control of internal processing	AP 01.06 Identify Safety and Security Risks AP 01.10 Develop and Deploy Safe and Secure Products and Services
10.2.3 Message authentication	AP 01.10 Develop and Deploy Safe and Secure Products and Services
10.2.4 Output data validation	AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.11 Objectively Evaluate Products
<i>10.3 Cryptographic controls</i>	AP 01.10 Develop and Deploy Safe and Secure Products and Services
10.3.1 Policy on the use of cryptographic controls	AP 01.07 Analyze and Prioritize Risks AP 01.09 Determine Regulatory Requirements, Laws and Standards
10.3.2 Encryption	AP 01.07 Analyze and Prioritize Risks AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.10 Develop and Deploy Safe and Secure Products and Services
10.3.3 Digital signatures	AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.10 Develop and Deploy Safe and Secure Products and Services
10.3.4 Non-repudiation services	AP 01.12 Establish Safety and Security Assurance Arguments
10.3.5 Key management	AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.10 Develop and Deploy Safe and Secure Products and Services
<i>10.4 Security of system files</i>	AP 01.02 Establish Qualified Work Environment
10.4.1 Control of operational software	AP 01.02 Establish Qualified Work Environment AP 01.11 Objectively Evaluate Products AP 01.15 Select and Manage Suppliers, Products and Services AP 01.16 Monitor and Control Activities and Products
10.4.2 Protection of system test data	AP 01.02 Establish Qualified Work Environment AP 01.11 Objectively Evaluate Products
10.4.3 Access control to program source library	AP 01.02 Establish Qualified Work Environment AP 01.16 Monitor and Control Activities and Products
<i>10.5 Security in development and support processes</i>	AP 01.02 Establish Qualified Work Environment AP 01.16 Monitor and Control Activities and Products
10.5.1 Change control procedures	AP 01.16 Monitor and Control Activities and Products
10.5.2 Technical review of operating system changes	AP 01.05 Ensure Business Continuity AP 01.11 Objectively Evaluate Products AP 01.16 Monitor and Control Activities and Products
10.5.3 Restrictions on changes to	AP 01.11 Objectively Evaluate Products

Table 3: Security Sources Mapped to Safety and Security Application Practices
Part 1 - ISO/IEC 17799 Information technology - Code of practice for information security management

ISO/IEC 17799	Safety and Security Application Practice
software packages	
10.5.4 Covert channels and Trojan code	AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan
10.5.5 Outsourced software development	AP 01.15 Select and Manage Suppliers, Products and Services
11. Business Continuity Management	
<i>11.1 Aspects of business continuity management</i>	AP 01.02 Establish Qualified Work Environment AP 01.05 Ensure Business Continuity
11.1.1 Business continuity management process	AP 01.02 Establish Qualified Work Environment AP 01.05 Ensure Business Continuity
11.1.2 Business continuity and impact analysis	AP 01.02 Establish Qualified Work Environment AP 01.05 Ensure Business Continuity
11.1.3 Writing and implementing continuity plans	AP 01.02 Establish Qualified Work Environment AP 01.05 Ensure Business Continuity
11.1.4 Business continuity planning framework	AP 01.02 Establish Qualified Work Environment AP 01.05 Ensure Business Continuity
11.1.5 Testing, maintaining and re-assessing business continuity plans	AP 01.02 Establish Qualified Work Environment AP 01.05 Ensure Business Continuity
12. Compliance	AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.11 Objectively Evaluate Products
<i>12.1 Compliance with legal requirements</i>	AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.11 Objectively Evaluate Products AP 01.16 Monitor and Control Activities and Products
12.1.1 Identification of applicable legislation	AP 01.09 Determine Regulatory Requirements, Laws and Standards
12.1.2 Intellectual property rights	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.09 Determine Regulatory Requirements, Laws and Standards
12.1.3 Safeguarding of organizational records	AP 01.03 Ensure Integrity of Safety and Security Information
12.1.4 Data protection and privacy of personal information	AP 01.03 Ensure Integrity of Safety and Security Information AP 01.09 Determine Regulatory Requirements, Laws and Standards
12.1.5 Prevention of misuse of information processing facilities	AP 01.02 Establish Qualified Work Environment
12.1.6 Regulation of cryptographic controls	AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.16 Monitor and Control Activities and Products
12.1.7 Collection of evidence	AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.12 Establish Safety and Security Assurance Arguments
<i>12.2 Review of security policy and technical compliance</i>	AP 01.16 Monitor and Control Activities and Products
12.2.1 Compliance with security policy	AP 01.16 Monitor and Control Activities and Products
12.2.2 Technical compliance checking	AP 01.11 Objectively Evaluate Products AP 01.16 Monitor and Control Activities and Products
<i>12.3 System audit considerations</i>	AP 01.02 Establish Qualified Work Environment
12.3.1 System audit controls	AP 01.16 Monitor and Control Activities and Products
12.3.2 Protection of system audit tools	AP 01.02 Establish Qualified Work Environment

Table 3: Security Sources Mapped to Safety and Security Application Practices
Part 2 – Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408:1999)

ISO/IEC 15408:1999	Safety and Security Application Practice
Class ACM: Configuration management	
ACM_AUT Automation	AP 01.02 Establish Qualified Work Environment
ACM_CAP Capabilities	AP 01.16 Monitor and Control Activities and Products
ACM_SCP Scope	AP 01.16 Monitor and Control Activities and Products
Class ADO: Delivery and operation	
ADO_DEL Delivery	AP 01.10 Develop and Deploy Safe and Secure Products and Services
ADO_IGS Installation, generation and start-up	AP 01.10 Develop and Deploy Safe and Secure Products and Services
Class ADV: Development	
ADV_FSP Functional specification	AP 01.09 Determine Regulatory Requirements, Laws and Standards
ADV_HLD High-level design	AP 01.10 Develop and Deploy Safe and Secure Products and Services
ADV_IMP Implementation representation	AP 01.10 Develop and Deploy Safe and Secure Products and Services
ADV_INT TSF internals	AP 01.09 Determine Regulatory Requirements, Laws and Standards
ADV_LLD Low-level design	AP 01.10 Develop and Deploy Safe and Secure Products and Services
ADV_RCR Representation correspondence	AP 01.11 Objectively Evaluate Products
ADV_SPM Security policy modeling	AP 01.09 Determine Regulatory Requirements, Laws and Standards
Class AGD: Guidance documents	
<i>AGD_ADM Administrator Guidance</i>	AP 01.10 Develop and Deploy Safe and Secure Products and Services
AGD_USR User Guidance	AP 01.10 Develop and Deploy Safe and Secure Products and Services
Class ALC: Life cycle support	
ALC_DVS Development security	AP 01.02 Establish Qualified Work Environment
ALC_FLR Flaw remediation	AP 01.02 Establish Qualified Work Environment AP 01.03 Control Information AP 01.04 Monitor Incidents AP 01.16 Monitor and Control Activities and Products
ALC_LCD Life cycle definition	AP 01.02 Establish Qualified Work Environment AP 01.04 Monitor Incidents AP 01.10 Develop and Deploy Safe and Secure Products and Services AP 01.13 Establish Independent Safety and Security Reporting AP 01.14 Establish a Safety and Security Plan
ALC_TAT Tools and techniques	AP 01.02 Establish Qualified Work Environment AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.10 Develop and Deploy Safe and Secure Products and Services
Class ATE: Tests	
ATE_COV Coverage	AP 01.11 Objectively Evaluate Products
ATE_DPT Depth	AP 01.11 Objectively Evaluate Products
ATE_FUN Functional tests	AP 01.11 Objectively Evaluate Products
ATE_IND Independent testing	AP 01.11 Objectively Evaluate Products AP 01.13 Establish Independent Safety and Security Reporting

Table 3: Security Sources Mapped to Safety and Security Application Practices
Part 2 – Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408:1999)

ISO/IEC 15408:1999	Safety and Security Application Practice
Class AVA: Vulnerability assessment	
AVA_CCA Covert channel analysis	AP 01.06 Identify Safety and Security Risks
AVA_MSU Misuse	AP 01.06 Identify Safety and Security Risks
AVA_SOF Strength of TOE security functions	AP 01.07 Analyze and Prioritize Risks
AVA_VLA Vulnerability analysis	AP 01.07 Analyze and Prioritize Risks
Class AMA: Maintenance of Assurance	
AMA_AMP Assurance maintenance plan	AP 01.05 Ensure Business Continuity AP 01.14 Establish a Safety and Security Plan
AMA_CAT TOE Component categorization report	AP 01.02 Establish Qualified Work Environment AP 01.05 Ensure Business Continuity AP 01.14 Establish a Safety and Security Plan
AMA_EVD Evidence of assurance maintenance	AP 01.12 Establish Safety and Security Assurance Argument
AMA_SIA Security impact analysis	AP 01.12 Establish Safety and Security Assurance Argument

Table 3: Security Sources Mapped to Safety and Security Application Practices
Part 3 – ISO/IEC 21827: Systems Security Engineering Capability Maturity Model (SSE-CMM)

SSE-CMM	Safety and Security Application Practice
PA01: Administer Security Controls	
BP.01.01 Establish responsibilities and accountability for security controls and communicate them to everyone in the organization.	AP 01.13 Establish Independent Safety and Security Reporting AP 01.14 Establish a Safety and Security Plan
BP.01.02 Manage the configuration of system security controls.	AP 01.16 Monitor and Control Activities and Products
BP.01.03 Manage security awareness, training, and education programs for all users and administrators.	AP 01.01 Ensure Safety and Security Competency AP 01.02 Establish Qualified Work Environment
BP.01.04 Manage periodic maintenance and administration of security services and control mechanisms.	AP 01.02 Establish Qualified Work Environment AP 01.03 Ensure Integrity of Safety and Security Information
PA02: Assess Impact	
BP.02.01 Identify, analyze, and prioritize operational, business, or mission capabilities leveraged by the system.	AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks
BP.02.02 Identify and characterize the system assets that support the key operational capabilities or the security objectives of the system.	AP 01.02 Establish Qualified Work Environment AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks
BP.02.03 Select the impact metric to be used for this assessment,	AP 01.07 Analyze and Prioritize Risks
BP.02.04 Identify the relationship between the selected metrics for this assessment and metric conversion factors if required,	AP 01.07 Analyze and Prioritize Risks
BP.02.05 Identify and characterize impacts.	AP 01.07 Analyze and Prioritize Risks
BP.02.06 Monitor ongoing changes in the impacts.	AP 01.04 Monitor Operations and Report Incidents
PA03: Assess Security Risk	
BP.03.01 Select the methods, techniques, and criteria by which security risks, for the system in a defined environment are analyzed, assessed, and compared.	AP 01.07 Analyze and Prioritize Risks AP 01.09. Identify regulatory requirements, laws and standards
BP.03.02 Identify threat/vulnerability/impact triples (exposures).	AP 01.07 Analyze and Prioritize Risks
BP.03.03 Assess the risk associated with the occurrence of an exposure.	AP 01.07 Analyze and Prioritize Risks
BP.03.04 Assess the total uncertainty associated with the risk for the exposure.	AP 01.07 Analyze and Prioritize Risks
BP.03.05 Order risks by priority.	AP 01.07 Analyze and Prioritize Risks
BP.03.06 Monitor ongoing changes in the risk spectrum and changes to their characteristics.	AP 01.04 Monitor Operations and Report Incidents
PA04: Assess Threat	
BP.04.01 Identify applicable threats arising from a natural source.	AP 01.06 Identify Safety and Security Risks
BP.04.02 Identify applicable threats arising from man-made sources, either accidental or deliberate.	AP 01.06 Identify Safety and Security Risks
BP.04.03 Identify appropriate units of	AP 01.06 Identify Safety and Security Risks

Table 3: Security Sources Mapped to Safety and Security Application Practices
Part 3 – ISO/IEC 21827: Systems Security Engineering Capability Maturity Model (SSE-CMM)

SSE-CMM	Safety and Security Application Practice
measure, and applicable ranges, in a specified environment.	
BP.04.04 Assess capability and motivation of threat agent for threats arising from man-made sources.	AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks
BP.04.05 Assess the likelihood of an occurrence of a threat event.	AP 01.07 Analyze and Prioritize Risks
BP.04.06 Monitor ongoing changes in the threat spectrum and changes to their characteristics.	AP 01.04 Monitor Operations and Report Incidents
PA05: Assess Vulnerability	
BP.05.01 Select the methods, techniques, and criteria by which security system vulnerabilities in a defined environment are identified and characterized.	AP 01.06 Identify Safety and Security Risks AP 01.09 Determine Regulatory Requirements, Laws and Standards
BP.05.02 Identify system security vulnerabilities.	AP 01.06 Identify Safety and Security Risks
BP.05.03 Gather data related to the properties of the vulnerabilities.	AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks
BP.05.04 Assess the system vulnerability and aggregate vulnerabilities that result from specific vulnerabilities and combinations of specific vulnerabilities.	AP 01.07 Analyze and Prioritize Risks
BP.05.05 Monitor ongoing changes in the applicable vulnerabilities and changes to their characteristics.	AP 01.04 Monitor Operations and Report Incidents
PA06: Build Assurance Argument	
BP.06.01 Identify the security assurance objectives.	AP 01.10 Develop and Deploy Safe and Secure Products and Services
BP.06.02 Define a security assurance strategy to address all assurance objectives.	AP 01.14 Establish a Safety and Security Plan
BP.06.03 Identify and control security assurance evidence.	AP 01.03 Control Information
BP.06.04 Perform analysis of security assurance evidence.	AP 01.11 Objectively Evaluate Products AP 01.12 Establish Safety and Security Assurance Argument AP 01.16 Monitor and Control Activities and Products
BP.06.05 Provide a security assurance argument that demonstrates the customer's security needs are met.	AP 01.12 Establish Safety and Security Assurance Argument
PA07: Coordinate Security	
BP.07.01 Define security engineering coordination objectives and relationships.	AP 01.14 Establish a Safety and Security Plan
BP.07.02 Identify coordination mechanisms for security engineering.	AP 01.14 Establish a Safety and Security Plan
BP.07.03 Facilitate security engineering coordination.	AP 01.14 Establish a Safety and Security Plan AP 01.16 Monitor and Control Activities and Products
BP.07.04 Use the identified mechanisms to coordinate decisions and recommendations related to security.	AP 01.14 Establish a Safety and Security Plan AP 01.16 Monitor and Control Activities and Products
PA08: Monitor Security Posture	
BP.08.01 Analyze event records to determine the cause of an event, how it proceeded, and likely future events.	AP 01.04 Monitor Operations and Report Incidents
BP.08.02 Monitor changes in threats,	AP 01.04 Monitor Operations and Report Incidents

Table 3: Security Sources Mapped to Safety and Security Application Practices
Part 3 – ISO/IEC 21827: Systems Security Engineering Capability Maturity Model (SSE-CMM)

SSE-CMM	Safety and Security Application Practice
vulnerabilities, impacts, risks, and the environment.	
BP.08.03 Identify security relevant incidents.	AP 01.04 Monitor Operations and Report Incidents
BP.08.04 Monitor the performance and functional effectiveness of security safeguards.	AP 01.04 Monitor Operations and Report Incidents
BP.08.05 Review the security posture of the system to identify necessary changes.	AP 01.04 Monitor Operations and Report Incidents AP 01.11 Objectively Evaluate Products
BP.08.06 Manage the response to security relevant incidents.	AP 01.05 Ensure Business Continuity AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan AP 01.11 Objectively Evaluate Products AP 01.16 Monitor and Control Activities and Products
BP.08.07 Ensure that the artifacts related to security monitoring are suitably protected.	AP 01.03 Control Information
PA09: Provide Security Input	
BP.09.01 Work with designers, developers, and users to ensure that appropriate parties have a common understanding of security input needs.	AP 01.01 Ensure Safety and Security Competency AP 01.10 Develop and Deploy Safe and Secure Products and Services
BP.09.02 Determine the security constraints and considerations needed to make informed engineering choices.	AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.10 Develop and Deploy Safe and Secure Products and Services
BP.09.03 Identify alternative solutions to security related engineering problems.	AP 01.10 Develop and Deploy Safe and Secure Products and Services
BP.09.04 Analyze and prioritize engineering alternatives using security constraints and considerations.	AP 01.10 Develop and Deploy Safe and Secure Products and Services
BP.09.05 Provide security related guidance to the other engineering groups.	AP 01.01 Ensure Safety and Security Competency AP 01.02 Establish Qualified Work Environment
BP.09.06 Provide security related guidance to operational system users and administrators.	AP 01.01 Ensure Safety and Security Competency AP 01.02 Establish Qualified Work Environment
PA10: Specify Security Needs	
BP.10.01 Gain an understanding of the customer's security needs.	AP 01.10 Develop and Deploy Safe and Secure Products and Services
BP.10.02 Identify the laws, policies, standards, external influences and constraints that govern the system.	AP 01.09 Determine Regulatory Requirements, Laws and Standards
BP.10.03 Identify the purpose of the system in order to determine the security context.	AP 01.06 Identify Safety and Security Risks AP 01.10 Develop and Deploy Safe and Secure Products and Services
BP.10.04 Capture a high-level security oriented view of the system operation.	AP 01.06 Identify Safety and Security Risks AP 01.10 Develop and Deploy Safe and Secure Products and Services
BP.10.05 Capture high-level goals that define the security of the system.	AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.10 Develop and Deploy Safe and Secure Products and Services
BP.10.06 Define a consistent set of statements which define the protection to be implemented in the system.	AP 01.10 Develop and Deploy Safe and Secure Products and Services

Table 3: Security Sources Mapped to Safety and Security Application Practices
Part 3 – ISO/IEC 21827: Systems Security Engineering Capability Maturity Model (SSE-CMM)

SSE-CMM	Safety and Security Application Practice
BP.10.07 Obtain agreement that the specified security meets the customer's needs.	AP 01.10 Develop and Deploy Safe and Secure Products and Services
PA11: Verify and Validate Security	
BP.11.01 Identify the solution to be verified and validated.	AP 01.11 Objectively Evaluate Products AP 01.14 Establish a Safety and Security Plan
BP.11.02 Define the approach and level of rigor for verifying and validating each solution.	AP 01.11 Objectively Evaluate Products
BP.11.03 Verify that the solution implements the requirements associated with the previous level of abstraction.	AP 01.11 Objectively Evaluate Products
BP.11.04 Validate the solution by showing that it satisfies the needs associated with the previous level of abstraction, ultimately meeting the customer's operational security needs.	AP 01.11 Objectively Evaluate Products
BP.11.05 Capture the verification and validation results for the other engineering groups.	AP 01.11 Objectively Evaluate Products
PA12: Ensure Quality	
BP.12.01 Monitor conformance to the defined process	AP 01.16 Monitor and Control Activities and Products
BP.12.02 Measure work product quality	AP 01.16 Monitor and Control Activities and Products
BP.12.03 Measure quality of the process	AP 01.16 Monitor and Control Activities and Products
BP.12.04 Analyze quality measurements	AP 01.16 Monitor and Control Activities and Products
BP.12.05 Obtain participation	AP 01.16 Monitor and Control Activities and Products
BP.12.06 Initiate quality improvement activities	AP 01.16 Monitor and Control Activities and Products
BP.12.07 Detect need for corrective actions	AP 01.16 Monitor and Control Activities and Products
PA13 Manage Configurations	
BP.13.01 Establish configuration management methodology	AP 01.02 Establish Qualified Work Environment AP 01.14 Establish a Safety and Security Plan AP 01.16 Monitor and Control Activities and Products
BP.13.02 Identify configuration units	AP 01.14 Establish a Safety and Security Plan AP 01.16 Monitor and Control Activities and Products
BP.13.03 Maintain work product baselines	AP 01.16 Monitor and Control Activities and Products
BP.13.04 Control changes	AP 01.16 Monitor and Control Activities and Products
BP.13.05 Communicate configuration status	AP 01.02 Establish Qualified Work Environment AP 01.16 Monitor and Control Activities and Products
PA14 Manage Project Risk	
BP.14.01 Develop risk management approach	AP 01.14 Establish a Safety and Security Plan
BP.14.02 Identify risks	AP 01.06 Identify Safety and Security Risks
BP.14.03 Assess risks	AP 01.07 Analyze and Prioritize Risks
BP.14.04 Review risk assessment	AP 01.11 Objectively Evaluate Products
BP.14.05 Execute risk mitigation	AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan
BP.14.06 Track risk mitigation	AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan
PA15: Monitor and Control Technical Effort	
BP.15.01 Direct technical effort	AP 01.16 Monitor and Control Activities and Products

Table 3: Security Sources Mapped to Safety and Security Application Practices
Part 3 – ISO/IEC 21827: Systems Security Engineering Capability Maturity Model (SSE-CMM)

SSE-CMM	Safety and Security Application Practice
BP.15.02 Track project resources	AP 01.16 Monitor and Control Activities and Products
BP.15.03 Track technical parameters	AP 01.16 Monitor and Control Activities and Products
BP.15.04 Review project performance	AP 01.16 Monitor and Control Activities and Products
BP.15.05 Analyze project issues	AP 01.16 Monitor and Control Activities and Products
BP.15.06 Take corrective action	AP 01.16 Monitor and Control Activities and Products
PA16: Plan Technical Effort	
BP.16.01 Identify critical resources	AP 01.14 Establish a Safety and Security Plan
BP.16.02 Estimate project scope	AP 01.14 Establish a Safety and Security Plan
BP.16.03 Develop cost estimates	AP 01.14 Establish a Safety and Security Plan
BP.16.04 Determine project's process	AP 01.14 Establish a Safety and Security Plan
BP.16.05 Identify technical activities	AP 01.14 Establish a Safety and Security Plan
BP.16.06 Define project interface	AP 01.13 Establish Independent Safety and Security Reporting AP 01.14 Establish a Safety and Security Plan AP 01.15 Select and Manage Suppliers, Products and Services
BP.16.07 Develop project schedules	AP 01.14 Establish a Safety and Security Plan
BP.16.08 Establish technical parameters	AP 01.10 Develop and Deploy Safe and Secure Products and Services
BP.16.09 Develop technical management plan	AP 01.14 Establish a Safety and Security Plan AP 01.15 Select and Manage Suppliers, Products and Services
BP.16.10 Review and approve project plans	AP 01.14 Establish a Safety and Security Plan
PA17: Define Organization's Security Engineering Process	
BP.17.01 Establish process goals	AP 01.16 Monitor and Control Activities and Products
BP.17.02 Collect process assets	AP 01.16 Monitor and Control Activities and Products
BP.17.03 Develop organization's security engineering process	AP 01.16 Monitor and Control Activities and Products
BP.17.04 Define tailoring guidelines	AP 01.16 Monitor and Control Activities and Products
PA18: Improve Organization's Security Engineering Processes	
BP.18.01 Appraise the process	AP 01.16 Monitor and Control Activities and Products
BP.18.02 Plan process improvements	AP 01.16 Monitor and Control Activities and Products
BP.18.03 Change the standard process	AP 01.16 Monitor and Control Activities and Products
BP.18.04 Communicate process improvements	AP 01.16 Monitor and Control Activities and Products
PA19: Manage Product Line Evolution	
BP.19.01 Define product evolution	AP 01.02 Establish Qualified Work Environment AP 01.10 Develop and Deploy Safe and Secure Products and Services
BP.19.02 Identify new product technologies	AP 01.02 Establish Qualified Work Environment AP 01.10 Develop and Deploy Safe and Secure Products and Services
BP.19.03 Adapt development processes	AP 01.02 Establish Qualified Work Environment AP 01.16 Monitor and Control Activities and Products
BP.19.04 Ensure critical components availability	AP 01.02 Establish Qualified Work Environment AP 01.14 Establish a Safety and Security Plan
BP.19.05 Insert product technology	AP 01.02 Establish Qualified Work Environment
PA20: Manage Systems Engineering Support Environment	
BP.20.01 Maintain technical awareness	AP 01.02 Establish Qualified Work Environment
BP.20.02 Determine support requirements	AP 01.02 Establish Qualified Work Environment

Table 3: Security Sources Mapped to Safety and Security Application Practices
Part 3 – ISO/IEC 21827: Systems Security Engineering Capability Maturity Model (SSE-CMM)

SSE-CMM	Safety and Security Application Practice
BP.20.03 Obtain engineering support environment	AP 01.02 Establish Qualified Work Environment
BP.20.04 Tailor engineering support environment	AP 01.02 Establish Qualified Work Environment
BP.20.05 Insert new technology	AP 01.02 Establish Qualified Work Environment
BP.20.06 Maintain environment	AP 01.02 Establish Qualified Work Environment
BP.20.07 Monitor engineering support environment	AP 01.02 Establish Qualified Work Environment
PA21: Provide Ongoing Skills and Knowledge	
BP.21.01 Identify training needs	AP 01.01 Ensure Safety and Security Competency
BP.21.02 Select mode of knowledge or skill acquisition	AP 01.01 Ensure Safety and Security Competency
BP.21.03 Assure availability of skill and knowledge	AP 01.01 Ensure Safety and Security Competency
BP.21.04 Prepare training materials	AP 01.01 Ensure Safety and Security Competency
BP.21.05 Train personnel	AP 01.01 Ensure Safety and Security Competency
BP.21.06 Assess training effectiveness	AP 01.01 Ensure Safety and Security Competency
BP.21.07 Maintain training records	AP 01.01 Ensure Safety and Security Competency
BP.21.08 Maintain training materials	AP 01.01 Ensure Safety and Security Competency
PA22: Coordinate with Suppliers	
BP.22.01 Identify systems components or services	AP 01.15 Select and Manage Suppliers, Products and Services
BP.22.02 Identify competent suppliers or vendors	AP 01.15 Select and Manage Suppliers, Products and Services
BP.22.03 Choose suppliers or vendors	AP 01.15 Select and Manage Suppliers, Products and Services
BP.22.04 Provide expectations	AP 01.15 Select and Manage Suppliers, Products and Services
BP.22.05 Maintain communications	AP 01.15 Select and Manage Suppliers, Products and Services

Table 3: Security Sources Mapped to Safety and Security Application Practices
Part 4 – NIST 800-30 Risk Management Guide for Information Technology Systems

NIST 800-30	Safety and Security Application Practice
3. RISK ASSESSMENT	
<i>3.1 STEP 1: SYSTEM CHARACTERIZATION</i>	
3.1.1 System-Related Information	AP 01.06 Identify Safety and Security Risks AP 01.09 Determine regulatory, requirements, laws, and standards
3.1.2 Information-Gathering Techniques	AP 01.02 Establish Qualified Work Environment AP 01.06 Identify Safety and Security Risks AP 01.09 Determine regulatory, requirements, laws, and standards
<i>3.2 STEP 2: THREAT IDENTIFICATION</i>	
3.2.1 Threat-Source Identification	AP 01.06 Identify Safety and Security Risks AP 01.07 Analyze and Prioritize Risks
3.2.2 Motivation and Threat Actions	AP 01.06 Identify Safety and Security Risks
<i>3.3 STEP 3: VULNERABILITY IDENTIFICATION</i>	AP 01.06 Identify Safety and Security Risks
3.3.1 Vulnerability Sources	AP 01.06 Identify Safety and Security Risks
3.3.2 System Security Testing	AP 01.04 Monitor Operations and Report Incidents AP 01.06 Identify Safety and Security Risks AP 01.11 Objectively Evaluate Products
3.3.3 Development of Security Requirements Checklist	AP 01.06 Identify Safety and Security Risks AP 01.09 Determine Regulatory Requirements, Laws and Standards AP 01.10. Develop and Deploy Safe and Secure Products and Services
<i>3.4 STEP 4: CONTROL ANALYSIS</i>	
3.4.1 Control Methods	AP 01.07 Analyze and Prioritize Risks
3.4.2 Control Categories	AP 01.07 Analyze and Prioritize Risks
3.4.3 Control Analysis Technique	AP 01.07 Analyze and Prioritize Risks
<i>3.5 STEP 5: LIKELIHOOD DETERMINATION</i>	AP 01.07 Analyze and Prioritize Risks
<i>3.6 STEP 6: IMPACT ANALYSIS</i>	AP 01.07 Analyze and Prioritize Risks
<i>3.7 STEP 7: RISK DETERMINATION</i>	
3.7.1 Risk-Level Matrix	AP 01.07 Analyze and Prioritize Risks
3.7.2 Description of Risk Level	AP 01.07 Analyze and Prioritize Risks
<i>3.8 STEP 8: CONTROL RECOMMENDATIONS</i>	AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan
<i>3.9 STEP 9: RESULTS DOCUMENTATION</i>	AP 01.07 Analyze and Prioritize Risks
4. RISK MITIGATION	
<i>4.1 RISK MITIGATION OPTIONS</i>	AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan
<i>4.2 RISK MITIGATION STRATEGY</i>	AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan
<i>4.3 APPROACH FOR CONTROL IMPLEMENTATION</i>	AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan AP 01.13 Establish Independent Safety and Security Reporting AP 01.14 Establish a Safety and Security Plan
<i>4.4 CONTROL CATEGORIES</i>	AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan
4.4.1 Technical Security Controls	AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan
4.4.2 Management Security Controls	AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan
4.4.3 Operational Security Controls	AP 01.02 Establish Qualified Work Environment AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan
<i>4.5 COST-BENEFIT ANALYSIS</i>	AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan
<i>4.6 RESIDUAL RISK</i>	AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan

Table 3: Security Sources Mapped to Safety and Security Application Practices
Part 4 – NIST 800-30 Risk Management Guide for Information Technology Systems

NIST 800-30	Safety and Security Application Practice
5. EVALUATION AND ASSESSMENT	
<i>5.1 GOOD SECURITY PRACTICE</i>	AP 01.12 Establish Safety and Security Argument AP 01.14 Establish a Safety and Security Plan
<i>5.2 KEYS FOR SUCCESS</i>	AP 01.12 Establish Safety and Security Argument AP 01.14 Establish a Safety and Security Plan

Table 4: Work Environment Practices Mapped to Sources
Part 1 – ISO 9001:2000, EIA/IS 731, CMMI, FAA-iCMM, and MBNQA

Work Environment Practice	ISO9001-2000	EIA/IS 731 (Focus Area: 3.4 Manage Systems Engineering Support Environment)	CMMI-SE/SW/IPPD v1.1; FAA-iCMM v1.0	MBNQA
Practice 01 Determine Work Environment Needs	6.3 Infrastructure 6.4 Work Environment	SP 3.4-1-2 Determine requirements for the support environment based on program specific needs. SP 3.4-1-3a Include the needs of each program as part of a documented set of requirements for the support environment. SP 3.4-1-3b Include the business goals of the organization in determining the documented requirements for the support environment.		
Practice 02 Establish Work Environment Standards		SP 3.4-2-3a Establish an organizational standard system engineering support environment.		
Practice 03 Establish Work Environment	6.3 Infrastructure 6.4 Work Environment	SP 3.4-2-3a Establish an organizational standard system engineering support environment. SP 3.4-2-1 Deploy a Systems Engineering Support Environment that supports program needs. SP 3.4-2-3b Tailor the Systems Engineering Support Environment to individual program needs. SP 3.4-2-2b Perform cost-benefit analysis for commercial off-the-shelf versus in-house developed environments. SP 3.4-2-2a Pilot new tools prior to including them in the systems engineering support environment. SP 3.4-2-1 Deploy a Systems Engineering Support Environment that supports program needs. SP 3.4-2-3b Tailor the Systems Engineering Support Environment to individual program needs. SP 3.4-2-5 Maximize integration of tools within the environment. SP 3.4-3-3a Collect data on the systems engineering support environment usage and performance. SP 3.4-3-3b Retire support tools or facilities which no longer support the organization's requirements. SP 3.4-3-1 Maintain the support environment to continuously support the program. SP 3.4-3-3c Upgrade or add support tools or facilities which enhance the ability to meet the organization's requirements SP 3.4-3-3d Seek periodic evaluation of the adequacy of the	<i>CMMI, Organizational Environment for Integration:</i> SP 1.2-1. Establish and maintain an integrated work environment that supports IPPD by enabling collaboration and concurrent development.	5.3a Work Environment - Address and improve workplace health, safety, and ergonomic factors 6.1a Design Process -3 New technology is incorporated into products/ services and into production/ delivery systems and processes, as appropriate. - 6-coordinate and test design and production/ delivery processes to ensure capability for trouble-free and timely introduction of products/services

Table 4: Work Environment Practices Mapped to Sources
Part 1 – ISO 9001:2000, EIA/IS 731, CMMI, FAA-iCMM, and MBNQA

Work Environment Practice	ISO9001-2000	EIA/IS 731 (Focus Area: 3.4 Manage Systems Engineering Support Environment)	CMMI-SE/SW/IPPD v1.1; FAA-iCMM v1.0	MBNQA
		systems engineering support environment from users. SP 3.4-3-4a Base support environment management decisions on the analysis of usage and performance data. SP 3.4-3-5 Establish goals for improvements to systems engineering processes through the use of the systems engineering environment.		
Practice 04 Maintain the Qualification of Components	7.6 Control of monitoring and measuring devices			
Practice 05 Maintain the Qualification of Personnel				
Practice 06 Maintain Technology Awareness		SP 3.3-1-3a Support participation by the organization in technical consortia, societies, and collaborations. SP 3.3-1-3c Establish a mechanism for maintaining awareness and disseminating knowledge of the state-of-the-art technology. SP 3.4-1-3c Regularly review and assess external trends that might affect the support environment for potential impact.	<i>iCMM v1.0, PA10 Product Evolution:</i> BP 10.02 Identify new product technologies or enabling infrastructure that will help the organization acquire, develop, and apply technology for competitive advantage. BP 10.05 Insert new technology into product development, marketing, and manufacturing.	
Practice 07 Assure Work Environment Continuity				

Table 4: Work Environment Practices Mapped to Sources
Part 2 – ISO/IEC 15504, ISO/IEC 12207, ISO/IEC 15288, P-CMM, eSCM

Work Environment Practice	ISO/IEC 15504 (ORG.4 Infrastructure)	IEEE/EIA 12207 (7.2 Infrastructure)	ISO/IEC 15288	P-CMM	eSCM
Practice 01 Determine Work Environment Needs	ORG.4.BP1 : Identify software engineering environment requirements. ORG.4.BP3 : Provide support for those who utilize the software engineering environment.	7.2.1.1 7.2.2.1	5.3.3 Investment Management Process 5.3.3.3 5.3.5 Resource Management Process 5.3.5.3 a) 5.4.2 Project Planning Process 5.4.2.3	<i>P-CMM Work Environment Practice 1</i> The physical environment and resources required to perform committed work are identified in each unit.	
Practice 02 Establish Work Environment Standards		7.2.1.1			
Practice 03 Establish Work Environment	ORG.4.BP2 : Provide a software engineering environment ORG.4.BP3 : Provide support for individuals using the software engineering infrastructure. ORG.4.BP4 : Maintain software engineering environment. ORG.4.BP5 : Provide a workspace conducive to productive performance. ORG.4.BP7 : Provide remote access facility.	7.2.1.2 7.2.2.2. 7.2.3.1	5.3.5 Resource Management Process 5.3.5.3 a) 5.3.5.3 b) 5.4.3 Project Assessment Process 5.4.3.3 5.5.6 Integration Process 5.5.6.3 5.5.11 Maintenance Process 5.5.11.3 5.5.12 Disposal Process 5.5.12.3	<i>P-CMM Work Environment Practice 2</i> The physical environment required to perform assigned work is provided. <i>Practice 3</i> Individual workspaces provide an adequate personal environment for performing assigned work responsibilities. <i>Practice 4</i> The resources needed to accomplish committed work are made available in a timely manner. <i>Practice 5</i> Improvements are made to the work environment that improve work performance. <i>Practice 6</i> Environmental factors that degrade or endanger the health or safety of the workforce are identified and corrected. <i>Practice 7</i> Physical factors that degrade the effectiveness of the	eSCM org_over_7_3 Establish and implement procedures to capture and analyze performance measures. eSCM ppl_over_7_2 Establish and maintain a work environment that enables personnel to work effectively. eSCM tech_over_2_2 Establish and implement procedures to manage the security of the technology infrastructure. eSCM tech_exe_2_3 Optimize the overall performance of the technology infrastructure needed to deliver all services. eSCM: ppl_over_7_2 Establish and maintain a work environment that enables personnel to work

Table 4: Work Environment Practices Mapped to Sources
Part 2 – ISO/IEC 15504, ISO/IEC 12207, ISO/IEC 15288, P-CMM, eSCM

Work Environment Practice	ISO/IEC 15504 (ORG.4 Infrastructure)	IEEE/EIA 12207 (7.2 Infrastructure)	ISO/IEC 15288	P-CMM	eSCM
				work environment are identified and addressed. Practice 8 Sources of frequent interruption or distraction that degrade the effectiveness of the work environment are identified and minimized	effectively. eSCM:tech_exe_2_3 Optimize the overall performance of the technology infrastructure needed to deliver all services.
Practice 04 Maintain the Qualification of Components		7.2.3.1			
Practice 05 Maintain the Qualification of Personnel					
Practice 06 Maintain Technology Awareness				<i>P-CMM Continuous Workforce Innovation</i> Practice 8 Innovative and improved workforce practices and technologies are evaluated and selected for implementation.	eSCM: tech_over_1_2 Establish and implement procedures to acquire, deploy, and upgrade technology. eSCM: tech_over_5_4 Establish and implement procedures to proactively identify and introduce appropriate technology. eSCMM: tech_exe_1_2 Establish and implement procedures to integrate an organization's technology infrastructure with that of the client, as appropriate.
Practice 07 Assure Work Environment Continuity					eSCM:org_over_13_2 Establish and implement disaster recovery procedures. Establish and implement procedures to ensure the continuity of service during contract completion.

Table 4: Work Environment Practices Mapped to Sources
Part 3 – Safety Sources

Work Environment Practice	DEF STD 0056	IEC 61508	MIL-STD-882C	MIL-STD-882D
Practice 01 Determine Work Environment Needs	5.5.3 7.3.3 Determination of Design Rules and Techniques	7.3.2 Requirements (Part 2) 7.3.2.2e 7.4.6 Requirements for proof tests and diagnostic tests (Part 2) 7.4.4 Requirements for support tools and programming languages (Part 3) 7.4.4.2. 7.5.2 Requirements (Part 3) 7.5.2.2 7.9.2 Requirements (Part 3) 7.9.2.1	4.2d System safety program objectives 4.3b System safety design requirements 4.3c 4.3d Task 102b.System Safety Program Plan. Task 203 Safety Requirements/ Criteria Analysis	
Practice 02 Establish Work Environment Standards				4.6 Verification of mishap risk reduction
Practice 03 Establish Work Environment	Part 2, 5.6.2 Part 2, 5.8.1 Part 2, 7.3.1	7.4.7.4 (Part 2)	Task 206 Operate and Support Hazard Analysis Task 302 Test and Evaluation Safety 302.2 Task 207 Health Hazard Assessment 207.2 Task 206 Operate and Support Hazard Analysis 206.1,2 4.4.4 Development procedures and training	
Practice 04 Maintain the Qualification of Components		7.14.2 Requirements (Part 1) 7.14.2.1 7.7.7.2 Requirements (Part 2) 7.7.2.2. 7.7.2 Requirements(Part 3) 7.7.2.7 a) b) 8.2.5 (Part 1)		
Practice 05 Maintain the Qualification of Personnel	5.3.5 Quality of Staff		Task 102 System Safety Program Plan 102.9	
Practice 06 Maintain Technology Awareness				
Practice 07 Assure Work Environment Continuity				

Table 4: Work Environment Practices Mapped to Sources
Part 4 – Security Sources

Work Environment Practice	ISO/IEC 17799	ISO/IEC 21827 SSE CMM	ISO/IEC 15408 Common Criteria	NIST 800-30
Practice 01 Determine Work Environment Needs	<p>7.1 <i>Secure areas</i></p> <p>7.1.1 Physical security perimeter</p> <p>7.1.2 Physical entry controls</p> <p>7.1.3 Securing offices, rooms and facilities</p> <p>7.1.4. Working in secure areas</p> <p>7.1.5 Isolated delivery and loading areas</p> <p>7.2 <i>Equipment security</i></p> <p>7.2.1 Equipment siting and protection</p> <p>7.2.2 Power supplies</p> <p>7.2.3 Cabling security</p> <p>7.2.4 Equipment maintenance</p> <p>7.2.5 Security of equipment off-premises</p> <p>7.2.6 Secure disposal or re-use of equipment</p> <p>9.1.1 Access Control Policy</p>	<p>BP.02.02 Identify and characterize the system assets that support the key operational capabilities or the security objectives of the system.</p> <p>BP.09.05 Provide security related guidance to the other engineering groups.</p> <p>BP.13.01 Establish configuration management methodology</p> <p>BP.19.01 Define product evolution</p> <p>BP.20.02 Determine support requirements</p>	<p>ALC_TAT Tools and techniques</p> <p>ACM_AUT Automation</p> <p>ALC_DVS Development security</p> <p>ALC_LCD Life cycle definition</p>	
Practice 02 Establish Work Environment Standards				
Practice 03 Establish Work Environment	<p>4.1.4 Authorization process for information processing facilities</p> <p>5.1.1 Inventory of assets</p> <p>6.3.2 Reporting weaknesses</p> <p>6.3.3 Reporting software malfunctions</p> <p>7.1 <i>Secure areas</i></p> <p>7.1.1 Physical security perimeter</p> <p>7.1.2 Physical entry controls</p> <p>7.1.3 Securing offices, rooms and facilities</p> <p>7.1.4. Working in secure areas</p> <p>7.1.5 Isolated delivery and loading areas</p> <p>7.2 <i>Equipment security</i></p> <p>7.2.1 Equipment siting and protection</p> <p>7.2.2 Power supplies</p> <p>7.2.3 Cabling security</p> <p>7.2.4 Equipment maintenance</p> <p>7.2.5 Security of equipment off-premises</p> <p>7.2.6 Secure disposal or re-use of equipment</p> <p>7.3 <i>General controls</i></p> <p>7.3.1 Clear desk and clear screen policy</p> <p>7.3.2 Removal of property</p>	<p>BP.01.04 Manage periodic maintenance and administration of security services and control mechanisms.</p> <p>BP.13.01 Establish configuration management methodology</p> <p>BP.13.05 Communicate configuration status</p> <p>BP.19.03 Adapt development processes</p> <p>BP.19.04 Ensure critical components availability</p> <p>BP.20.03 Obtain engineering support environment</p> <p>BP.20.04 Tailor engineering support environment</p> <p>BP.20.06 Maintain environment</p> <p>BP.20.07 Monitor engineering support environment</p>	<p>ALC_TAT Tools and techniques</p> <p>ACM_AUT Automation</p> <p>AMA_CAT TOE Component categorization report</p> <p>ALC_DVS Development security</p> <p>ALC_FLR Flaw remediation</p> <p>ALC_LCD Life cycle definition</p>	<p>3.1.2 Information-Gathering Techniques</p> <p>4.4.3 Operational Security Controls</p>

Table 4: Work Environment Practices Mapped to Sources
Part 4 – Security Sources

Work Environment Practice	ISO/IEC 17799	ISO/IEC 21827 SSE CMM	ISO/IEC 15408 Common Criteria	NIST 800-30
	8.1 Operational procedures and responsibilities 8.1.1 Documented operating procedures 8.1.2 Operational change control 8.1.4 Segregation of duties 8.1.5 Separation of development and operational facilities 8.2.1 Capacity planning 8.5 <i>Network management</i> 8.5.1 Network controls 8.7.4 Security of electronic mail 8.7.5 Security of electronic office systems 9.2 <i>User access management</i> 9.2.1 User registration 9.2.2 Privilege management 9.2.3 User password management 9.2.4 Review of user access rights 9.4 <i>Network access control</i> 9.4.2 Enforced path 9.4.5 Remote diagnostic port protection 9.4.9 Security of network services 9.6.2 Sensitive system isolation 9.7.2 Monitoring system use 9.7.3 Clock synchronization 9.8 <i>Mobile computing and teleworking</i> 9.8.1 Mobile computing 9.8.2 Teleworking 10.4 <i>Security of system files</i> 10.4.1 Control of operational software 10.4.2 Protection of system test data 10.4.3 Access control to program source library 10.5 <i>Security in development and support processes</i> 12.1.5 Prevention of misuse of information processing facilities			
Practice 04 Maintain the Qualification of Components	7.2.4 Equipment maintenance 12.3 <i>System audit considerations</i> 12.3.2 Protection of system audit tools			

**Table 4: Work Environment Practices Mapped to Sources
Part 4 – Security Sources**

Work Environment Practice	ISO/IEC 17799	ISO/IEC 21827 SSE CMM	ISO/IEC 15408 Common Criteria	NIST 800-30
Practice 05 Maintain the Qualification of Personnel	4.2 Security of third party access 4.2.1 Identification of risks from third party access 4.2.2. Security requirements in third party contracts <i>6.1 Security in job definition and resourcing</i> 6.1.2 Personnel screening and policy 6.2 User training 6.2.1 Information security education and training 6.3.2 Reporting weaknesses 6.3.3 Reporting software malfunctions <i>9.3 User responsibilities</i> 9.3.1 Password use 9.3.2 Unattended user equipment	BP.01.03 Manage security awareness, training, and education programs for all users and administrators. BP.09.05 Provide security related guidance to the other engineering groups. BP.09.06 Provide security related guidance to operational system users and administrators.		
Practice 06 Maintain Technology Awareness		BP.19.02 Identify new product technologies BP.19.03 Adapt development processes BP.19.05 Insert product technology BP.20.01 Maintain technical awareness BP.20.05 Insert new technology		
Practice 07 Assure Work Environment Continuity	8.4 Housekeeping 8.4.1 Information back-up <i>11.1 Aspects of business continuity management</i> 11.1.1 Business continuity management process 11.1.2 Business continuity and impact analysis 11.1.3 Writing and implementing continuity plans 11.1.4 Business continuity planning framework 11.1.5 Testing, maintaining and re-assessing business continuity plans			