Sixteen Standards-Based Practices for Safety and Security

Dr. Linda Ibrahim
Federal Aviation Administration

This article presents 16 standards-based practices for safety and security. These practices were derived from four safety standards and four security standards and then harmonized to recognize the commonalities among the safety and security disciplines. Implementation of these practices should lead to establishing a safety and security capability, identifying and managing safety and security risks, and assuring that products and services are safe and secure throughout their life cycle.

Safety and security are critical properties of products and services today. There are many separate standards that pertain to safety and to security covering, for example, systems, software, management, and engineering. There are also many underlying process frameworks that help organizations develop and improve their essential management and engineering processes. However, there has been a lack of alignment among both specialized standards themselves and between those specialty areas and underlying process frameworks broadly used for process improvement. To fill these gaps, the Safety and Security Extensions Project was launched, co-sponsored by organizations within the Federal Aviation Administration (FAA) and the Department of Defense.

The Safety and Security Extensions Project developed the essential practices presented in this article. The safety and security practices produced from this project were required to be based on widely recognized safety and security standards[1] and harmonized across the safety and security disciplines. After separate safety practices and security practices were derived capturing their respective source standards, the practices were harmonized to address commonalities, coordinate activities, align terminology, and encourage the merger of the safety and security disciplines. Additionally, the project provided a mechanism for implementing these specialty-engineering practices in the context of existing process improvement frameworks to align safety and security improvements with more general process improvement endeavors.

The project team comprised more than 30 experts from government and industry in the United States and the international community. The resultant practices enjoyed multiple broad national and international reviews over the two-year project duration. The final report [1] fully describes the project and the safety and security practices. That report also provides guidance regarding using these safety and security practices with integrated capability maturity models as underlying process improvement frameworks.

The purpose of this article is to spread awareness of these essential, integrated, harmonized, standards-based practices and to encourage their use in organizations concerned about safety and security. Note that these practices are not software-specific, but address a broader product and service scope. These 16 practices will form a basis for the emerging international standard, International Organization for Standardization/International Electrotechnical Commission 15026 Systems and Software Assurance.

The 16 standards-based practices for safety and security are organized by goal and summarized in Table 1, and then briefly described in the next section. Lastly, further information is provided regarding using these practices.

The 16 Standards-Based Practices for Safety and Security

Establishing a Safety and Security Infrastructure

The first five practices help establish safety and security capability and infrastructure.

Practice 1: Ensure safety and security awareness, guidance, and competency. Those who engage in different safety and security activities need appropriate knowledge and skills. This practice includes identifying competency and awareness needs, ensuring those needs are met, and retaining records of qualifications and training. It includes qualifications required to access, use, and maintain a safe and secure work environment. The practice applies to managers, acquirers, developers, maintainers, operators, and general staff.

Practice 2: Establish and maintain a qualified work environment that meets safety and security needs. The work environment should address safety and security needs. This includes ensuring that facilities, tools, and equipment are calibrated or otherwise qualified in accordance with appropriate standards. New technology

Table 1: *The 16 Standards-Based Practices for Safety and Security (titles only)*

Establishing a Safety and Security Infrastructure
1. Ensure Safety and Security Competency
2. Establish Qualified Work Environment
3. Ensure Integrity of Safety and Security Information
4. Monitor Operations and Report Incidents
5. Ensure Business Continuity
Managing Safety and Security Risks
6. Identify Safety and Security Risks
7. Analyze and Prioritize Risks
8. Determine, Implement, and Monitor Risk Mitigation Plan
Satisfying Safety and Security Requirements
9. Determine Regulatory Requirements, Laws, and Standards
10. Develop and Deploy Safe and Secure Products and Services
11. Objectively Evaluate Products
12. Establish Safety and Security Assurance Arguments
Managing Activities and Products
13. Establish Independent Safety and Security Reporting
14. Establish a Safety and Security Plan
15. Select and Manage Suppliers, Products, and Services
16. Monitor and Control Activities and Products

should be provided when necessary to improve the work environment.

Practice 3: Identify required safety and security information and maintain storage, protection, and access and distribution control for it.
This practice ensures that a capability exists for retaining and protecting required safety and security information. Access is controlled, and information is distributed or made available to authorized stakeholders when needed.

Practice 4: Monitor operations and environmental changes, report and analyze safety and security incidents and anomalies, and initiate corrective actions.
The operational environment is monitored, including changes in threats, hazards, vulnerabilities, impacts, and risks. Safety and security incidents and anomalies are detected, collected, reported, analyzed, and retained to assist future analyses. Analysis may lead to initiating corrective or preventive actions, risk mitigation actions, further investigation, or other actions.

Practice 5: Establish and maintain plans to ensure continuity of business processes and protection of assets.
This practice includes identifying and assessing risks to business continuity, and establishing plans to protect the business and to counteract potential business disruptions from adverse conditions, failures, and threats. Business continuity plans are tested to ensure they are up to date and effective.

Managing Safety and Security Risks

These three practices pertain to identifying and managing safety and security risks.

Practice 6: Identify risks and sources of risks attributable to vulnerabilities, security threats, and safety hazards.
This practice includes identification of security threats or safety hazards, and vulnerabilities, faults, and failures that could be exercised or exploited. Risk sources may be natural or man-made, both accidental and deliberate.

Practice 7: For each risk associated with safety or security, determine the causal factors, estimate the consequence and likelihood of an occurrence, and determine relative priority.
Causal factors for threats or hazards may include hardware, software, human and environmental factors. The severity and likelihood of an occurrence are assessed and combined to obtain an estimate of risk for each threat or hazard. The practice also addresses prioritization of these risks.

Practice 8: Determine, implement, and monitor the risk mitigation plan to achieve an acceptable level of risk.
This practice pertains to determining controls or countermeasures to reduce risks to an acceptable level. A risk mitigation plan documents the approach and activities to ensure safety and security criteria are met, and these essential risk mitigations become included as product or service requirements. Risk mitigation plans are implemented and monitored and corrective actions taken as required to control safety and security risks.

Satisfying Safety and Security Requirements

The next four practices focus on determining safety and security requirements, and ensuring they are met throughout the life cycle.

Practice 9: Determine applicable regulatory requirements, laws, standards, and policies and define levels of safety and security.
This practice addresses the determination of applicable safety and security laws, mandates, regulatory requirements, external policies, and standards. It includes establishing internal policy regarding safety and security, defining criteria for determining safety and security levels[2], and denoting methods, techniques, rules, and tools required for each level.

Practice 10: Develop and deploy products and services that meet safety and security needs and requirements, and operate and dispose of them safely and securely.
Starting from the determination of safety and security requirements and levels, this practice guides all life-cycle activities to ensure products and services are designed, developed, transitioned, deployed, operated, maintained, and disposed of to address established safety and security needs and requirements.

Practice 11: Objectively evaluate products and services to ensure safety and security requirements are achieved and products and services fulfill their intended use.
This practice addresses verification, assessment, and audit throughout the life cycle to determine whether products and services meet safety and security requirements. It also addresses validation to determine fulfillment of intended use. Evaluation activities are performed at an appropriate level of rigor as determined by required safety and security levels, and evaluation evidence is collected to support safety and security claims.

Practice 12: Establish and maintain safety and security assurance arguments and supporting evidence throughout the life cycle.
To demonstrate that safety and security assurance needs have been satisfied, it is essential to retain documentation that provides an argument for the safety and security of a product or service. This argument, with supporting evidence, is built, collected, and retained throughout the life cycle.

Managing Activities and Products

The last four practices address safety and security management so that safety and security activities and products are planned, tracked, measured, monitored, and improved.

Practice 13: Establish and maintain independent reporting of safety and security status and issues.
Reporting safety and security status and issues should reflect the degree of independence appropriate to the needed level of safety and security associated with the product or service. Staff members and external organizations need to be informed about both reporting channels and notification mechanisms.

Practice 14: Establish and maintain a plan to achieve safety and security requirements and objectives.
This practice involves establishing the plan, establishing commitment to the plan, and coordinating and communicating plans, status, and direction to participants and stakeholders.

Practice 15: Select and manage suppliers, products, and services using safety and security criteria.
This practice addresses the capability of suppliers to meet safety and security needs. Appropriate criteria are used in supplier selection, and suppliers are required to deliver safety and security assurance with supplied products and services, including off-the-shelf products.

Practice 16: Measure, monitor, and review safety and security activities against plans, control products, take corrective action, and improve processes throughout the life cycle.
This last practice broadly encompasses several process and product control and monitoring activities. It includes measuring, monitoring, and reviewing activities against plans; assuring that changes to requirements, products, plans, and procedures do

not adversely affect safety and security; taking corrective action to address any safety and security problems or issues; and improving safety and security processes throughout the life cycle.

Applying the Practices

Organizational Context

Whatever your organizational perspective, these practices are useful if you are concerned about safety and security. The practices address safety and security in several contexts, including strategically, to support enterprise-wide safety and security work; 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.

Although the practices are harmonized, they can be implemented in the context chosen by the organization, which may be security only, or safety only, or both safety and security.

Process Improvement Context

The safety and security standards-based practices described above were developed to be used with respect to two integrated capability maturity models, the FAA integrated Capability Maturity Model (iCMM) [2] and Capability Maturity Model Integration (CMMI®) [3] and their respective appraisal methods. The architectural mechanism for realizing this alignment is called an *application area*. This construct was devised to ensure visibility, improvability, and appraisability of the safety and security practices, to facilitate their selective use, and to utilize the depth of existing framework practices for implementing safety and security without disrupting the underlying process frameworks already in use.

An application area groups together related standards-based *application practices* considered essential for achieving requisite outcomes particular to the application/discipline. In the case of the safety and security application area, the 16 practices presented in this article are denoted *application practices*. Application practices are carried out with associated guidance from the source standards for the application (i.e., the harmonized guidance from the eight source standards for safety and security that is provided for each practice in [1]).

However, to align the specialized safety and security practices with the essential and more general practices in the iCMM and CMMI, each application practice is further supported by *implementing practices*. These are particular practices in the CMMI and iCMM reference models that are used to implement application practices, when interpreted by the safety and security context information associated with each application practice.

For example, to implement application practice No. 1 *Ensure Safety and Security Competency*, implementing practices are from the training process areas in iCMM (PA 22 Training) and CMMI (Organizational Training); those practices would be carried out with particular focus on ensuring safety and security competency.

Thus an application area is structured to include the following: purpose, required goals/outcomes (application goals), expected practices (application practices), and for each application practice: description, typical work products, notes, and a list of *particular implementing practices* from the reference models. The generic practices of CMMI or iCMM apply to an application area so capability levels can be determined by appraisal methods associated with these reference models.

The excerpt in Figure 1 illustrates, for Practice 3 described in the previous section, how application practices and implementing practices are presented.

Application Practice 3 -
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 document and information. Manage and control required information, including documentation, data, and asssurance 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.

Process Area 17 Information Management *(from iCMM)*

Best Practice 17.01	Establish and maintain a strategy and requirements for information management.
Best Practice 17.02	Establish an infrastructure for information management, including repository, tools, equipment, and procedures.
Best Practice 17.03	Collect, receive, and store information according to established strategy and procedures.
Best Practice 17.04	Disseminate or provide timely access to information to those who need it.
Best Practice 17.05	Protect information from loss, damage, or unwarranted access.
Best Practice 17.06	Establish requirements and standards for content and format of selected information items.

Figure 1: *Presentation of an Application Practice and Its Implementing Practices*

The safety and security application area, and the application area construct are fully described in [1]. The application of these safety and security practices in the context of other standards and frameworks is additionally described in [4].

Summary

This article has presented 16 essential standards-based practices for safety and security. It further illustrated how an organization can align implementation and improvement of these 16 practices using a more general process improvement model. This should lead to more efficiency and effectiveness in process improvement efforts for those organizations concerned about safety and security.◆

References

1. Ibrahim, L., et al. Safety and Security Extensions for Integrated Capability Maturity Models. Washington: Federal Aviation Administration, Sept. 2004 <www.faa.gov/ipg>.
2. Ibrahim, L., et al. The Federal Aviation Administration Integrated Capability Maturity Model (FAA-iCMM). Vers. 2.0. Washington: Federal Aviation Administration, Sept. 2001 <www.faa.gov/ipg>.
3. CMMI Product Team. Capability Maturity Model® Integration (CMMI ®), Vers. 1.1 - CMMI for Systems Engineering, Software Engineering, Integrated Product and Process Develop-

® CMMI is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

Coming Events

November 6-9
6th Annual Amplifying Your Effectiveness Conference
Phoenix, AZ
www.ayeconference.com

November 6-9
5th Working IEEE/IFIP Conference on Software Architecture (WICSA)
Pittsburgh, PA
http://sunset.usc.edu/~softarch/wicsa5

November 7-9
Airborne Early Warning and Battle Management Conference
Washington D.C.
www.marcusevansbb.com/AEW

November 13-17
International Association for Computing Machinery SIGAda 2005 Conference
Atlanta, GA
www.sigada.org/conf/sigada2005

November 14-18
STARWEST 2005
Anaheim, CA
www.sqe.com/starwest

November 14-18
5th Annual Capability Maturity Model® Integration Technology Conference and User Group
Denver, CO
www.sei.cmu.edu/cmmi/events/cmmi-techconf.html

November 14-18
3rd International Conference on Software Process Improvement (ICSPI) 2005
Orlando, FL
www.icspi.com

May 1-4, 2006
2006 Systems and Software Technology Conference
Salt Lake City, UT
www.stc-online.org

ment, and Supplier Sourcing (CMMI-SE/SW/IPPD/SS, Vers. 1.1) Continuous Representation. Pittsburgh, PA: Software Engineering Institute, Mar. 2002 <www.sei.cmu.edu>.
4. Ibrahim, L., C. Wells, and R. Bate. Extending Systems Engineering Frameworks for Special Application Areas: Case Study Safety and Security. Proc. of the 15th Annual International Symposium of the International Council on Systems Engineering, Rochester, N.Y., July 2005 <www.faa.gov/ipg>.

Notes

1. The safety and security practices are derived from the following eight standards:
   For Safety:
   - MIL-STD-882C*. Military Standard System Safety Program Requirements. U.S. Department of Defense, Jan. 1993 <https://safety.army.mil/pages/systemsafety>.
   - MIL-STD-882D*. Standard Practice for System Safety. U.S. Department of Defense, Feb. 2000 <https://safety.army.mil/pages/systemsafety>.
   - IEC 61508. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. International Electrotechnical Commission, 1997 <www.iec.ch/61508>.
   - DEF STAN 00-56. Defence Standard 00-56, Safety Management Requirements for Defence Systems. Ministry of Defence, United Kingdom, Dec. 1996. <www.dstan.mod.uk> or <http://cms.brookes.ac.uk/modules/other/58_DEF_STAN_00-56.pdf>.

   * Although MIL-STD-882D supercedes MIL-STD-882C, the knowledge in MIL-STD-882C was also integrated into the 16 practices, as proposed/endorsed by the safety community. We found no inconsistencies between the standards and included them both.

   For Security:
   - ISO/IEC 17799:2000(E). Information Technology – Code of Practice for Information Security Management. 1st ed. International Organization for Standardization, 1 Dec. 2000 <www.iso.ch>.
   - ISO/IEC 15408. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Vers. 2.1. Common Criteria Project Sponsoring Organizations, 1999 <www.commoncriteriaportal.org>.
   - ISO/IEC 21827:2002. Systems Security Engineering Capability Maturity Model. International Organization for Standardization. (Systems Security Engineering Capability Maturity Model, Model Description Document Vers. 3.0, June 2003, Systems Security Engineering Capability Maturity Model (SSE-CMM) Project.) <www.sse-cmm.org> or <www.iso.ch>.
   - NIST 800-30. Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology, Special Publication 800-30, 2001 <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>.

   The Safety and Security Extensions final report [1] includes mappings of the safety and security practices to source practices/clauses, and demonstrates coverage of these eight source documents, at an appropriate level of detail.
2. Each safety and security level denotes an expression of trust or an acceptable range of values of risk containment associated with a product or service.

About the Author

Linda Ibrahim, Ph.D., is chief engineer for Process Improvement at the Federal Aviation Administration (FAA). She led development and is lead author and architect of FAA-integrated Capability Maturity Model Vers. 1.0 and Vers. 2.0, and its appraisal method, and she co-managed the Safety and Security Extensions project. Ibrahim has worked in software engineering for more than 30 years in the United States, Europe, and Middle East, and is a member of the Capability Maturity Model® Integration Steering Group. Ibrahim has a Bachelor of Arts in Mathematics, a Master of Science in information science, and a doctorate in electrical engineering.

Federal Aviation Administration
800 Independence AVE SW
Washington, DC 20591
Phone: (202) 267-7443
Fax: (202) 267-5069
E-mail: linda.ibrahim@faa.gov