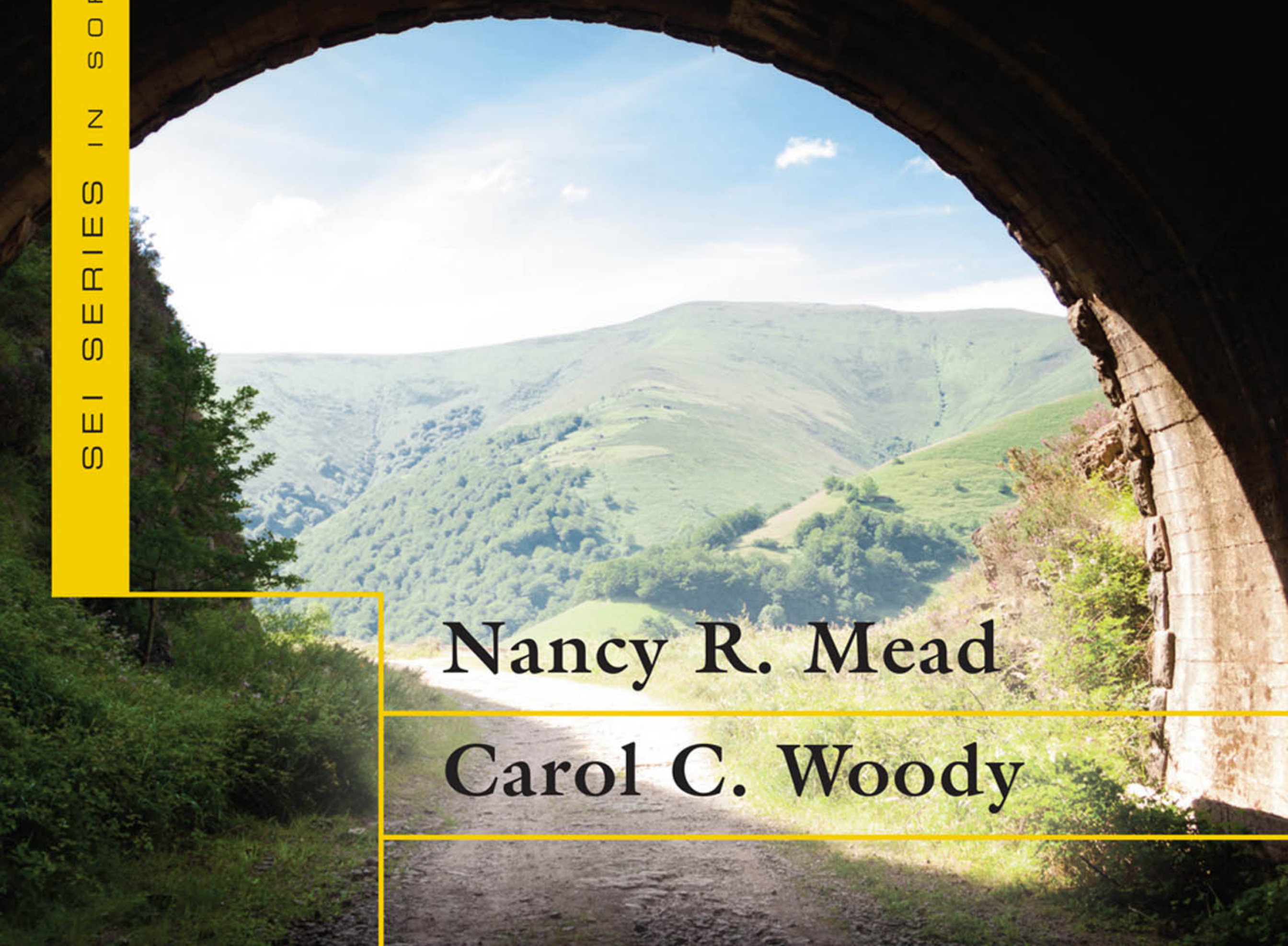
SEI SERIES IN SOFTWARE ENGINEERING

Cyber Security Engineering

A Practical Approach for Systems and Software Assurance



Nancy R. Mead

Carol C. Woody

Praise for *Cyber Security Engineering*

"This book presents a wealth of extremely useful material and makes it available from a single source."

—Nadya Bartol, Vice President of Industry Affairs and
Cybersecurity Strategist, Utilities Technology Council

"Drawing from more than 20 years of applied research and use, CSE serves as both a comprehensive reference and a practical guide for developing assured, secure systems and software—addressing the full lifecycle; manager and practitioner perspectives; and people, process, and technology dimensions."

—Julia Allen, Principal Researcher,
Software Engineering Institute

Table 4.5 *SwA Competency Designations*

		Knowledge/Skill/Effectiveness
KA	**Unit**	**Competency Activities**
Assurance Across Lifecycles	Software Lifecycle Processes	L1: Understand and execute the portions of a defined process applicable to their assigned tasks. L2: Manage the application of a defined lifecycle software process for a small internal project. L3: Lead and assess process application for small and medium-sized projects, over a variety of lifecycle phases, such as new development, acquisition, operation, and evolution. L4: Manage the application of a defined lifecycle software process for a large project, including selecting and adapting existing SwA practices by lifecycle phase. L5: Analyze, design, and evolve lifecycle processes that meet the special organizational or domain needs and constraints.
	Software Assurance Processes and Practices	L1: Possess general awareness of methods, procedures, and tools used to assess assurance processes and practices. L2: Apply methods, procedures, and tools to assess assurance processes and practices. L3: Manage integration of assurance practices into typical lifecycle phases. L4: Lead the selection and integration of lifecycle assurance processes and practices in all projects, across an organization. L5: Analyze assurance assessment results to determine best practices for various lifecycle phases.

(*Continued*)

Table 4.5 *Continued*

Knowledge/Skill/Effectiveness		
KA	**Unit**	**Competency Activities**
Risk Management	Risk Management Concepts	L1: Understand the basic elements of risk analysis. L2: Explain how risk analysis is performed. L3: Determine the models, process, and metrics to be used in risk management for small internal projects. L4: Develop the models, processes, and metrics to be used in risk management of any sized project. L5: Analyze the effectiveness of the use and application of risk management concepts across an organization.
	Risk Management Process	L1: Describe an organizational risk management process. L2: Identify and classify the risks associated with a project. L3: Analyze the likelihood, impact, and severity of each identified risk for a project. Plan and monitor risk management for small to medium-sized projects. L4: Plan and monitor risk management for a large project. L5: Develop a program for analyzing and enhancing risk management practices across an organization.
	Software Assurance Risk Management	L1: Describe risk analysis techniques for vulnerability and threat risks. L2: Apply risk analysis techniques to vulnerability and threat risks. L3: Analyze and plan for mitigation of software assurance risks for small systems. L4: Analyze and plan for mitigation of software assurance risks for both new and existing systems. L5: Assess software assurance processes and practices across an organization and propose improvements.

4.4.4 A Path to Increased Capability and Advancement[9]

The SwA Competency Model can provide direction on professional growth and career advancement. Each competency level assumes competency at the lower levels. The model also provides a comprehensive mapping between the CorBoK (KAs and units) and the competency levels. The complete mapping can be found in Appendix D, "The Software Assurance Competency Model Designations." Table 4.6 illustrates this mapping for the System Security Assurance KA.

4.4.5 Examples of the Model in Practice[10]

There are a number of ways the Software Assurance Competency Model can be applied in practice. An organization in which software assurance is critical could use the type of information in Table 4.6 to do all of the following:

- Structure its software assurance needs and expectations
- Assess its software assurance personnel's capability
- Provide a roadmap for employee advancement
- Use as a basis for software assurance professional development plans

For example, an organization intending to hire an entry-level software assurance professional could examine the L1–L2 levels and incorporate elements of them into job descriptions. These levels could also be used during the interview process by both the employer and the prospective employee to assess the actual expertise of the candidate.

Another application is by faculty members who are developing courses in software assurance or adding software assurance elements to their software engineering courses. The levels allow faculty to easily see the depth of content that is suitable for courses at the community college, undergraduate, and graduate levels. For example, undergraduate student outcomes might be linked to the L1 and L2 levels, whereas graduate courses aimed at practitioners with more experience might target higher levels. In industry, the model could be used to determine if specific competency areas were being overlooked. These areas could point toward corresponding training needs. With a bit of effort, trainers can tailor their course offerings to the target audience. The model eliminates some of the guesswork involved in deciding what level of material is appropriate for a given course.

[9] This section is drawn from "Building Security In: A Road to Competency" [Hilburn 2013b].

[10] This section is drawn from *The Software Assurance Competency Model: A Roadmap to Enhance Individual Professional Capability* [Mead 2013a].

Table 4.6 *The Competency Specification for the System Security Assurance KA*

Unit	Competency Activities
For Newly Developed and Acquired Software for Diverse Applications	L1: Possess knowledge of security and safety risks associated with critical infrastructure systems (e.g., in banking and finance, energy production and distribution, telecommunications, and transportation systems). L2: Describe the variety of methods by which attackers can damage software or data associated with that software by exploiting weaknesses in the system design or implementation. L3: Apply software assurance countermeasures such as layers, access controls, privileges, intrusion detection, encryption, and code review checklists. L4: Analyze the threats to which software is most likely to be vulnerable in specific operating environments and domains. L5: Perform research on security risks and attack methods, and use it to support modification or creation of techniques used to counter such risks and attacks.
For Diverse Operational (Existing) Systems	L1: Possess knowledge of the attacks that have been used to interfere with an application's or system's operations. L2: Possess knowledge of how gates, locks, guards, and background checks can address risks.

	L3: Design and plan for access control and authentication.
	L4: Analyze the threats to which software is most likely to be vulnerable in specific operating environments and domains.
	L5: Perform research on security risks and attack methods, and use it to support modification or creation of techniques used to counter such risks and attacks.
Ethics and Integrity in Creation, Acquisition, and Operation of Software Systems	L1: Possess knowledge of how people who are knowledgeable about attack and prevention methods are obligated to use their abilities, both legally and ethically.
	L2: Possess knowledge of the legal and ethical considerations involved in analyzing a variety of historical events and investigations.
	L3: Follow legal and ethical guidelines in the creation and maintenance of software systems.
	L4: Play a leadership role in the practice of ethical behavior for software security.
	L5: Create new case studies for use in education about ethical and legal issues.

It can also be used by faculty who are already teaching such courses to assess whether the course material is a good fit for the target audience. The authors of this chapter are currently teaching software assurance courses and use the model to revisit and tailor their syllabi accordingly.

4.4.6 Highlights of the SEI Software Assurance Competency Model[11]

The Software Assurance Competency Model was developed to create a foundation for assessing and advancing the capability of software assurance professionals. The span of competency levels L1 through L5 and the decomposition into individual competencies based on the knowledge and skills described in the SwA CorBoK [Mead 2010a] provide the detail necessary for an organization or individual to determine SwA competency across the range of knowledge areas and units. The model also provides a framework for an organization to adapt its features to the organization's particular domain, culture, or structure.

The model was reviewed by invited industry reviewers and mapped to actual industry positions. These mappings are included in the SEI's report; the model also underwent public review prior to publication. Dick Fairley, chair of the Software and Systems Engineering Committee of the IEEE Computer Society (IEEE-CS) Professional Activities Board (PAB), endorsed the SEI Software Assurance Competency Model "as appropriate for software assurance roles and consistent with A Framework for PAB Competency Models."[12] In presentations and webinars delivered by the author on software assurance, only about half of the participants had a plan for their own SwA competency development. However, more than 80% said they could use the SwA Competency Model in staffing a project.

The most important outcome of this model is a better trained and educated workforce. As the needs of the software industry for more secure applications continue, the recommendations of this model can be used to ensure better and more trustworthy practice in the process of developing and sustaining an organization's software assets. That guidance going forward is a linchpin in the overall effort to create trusted systems and provides the necessary reference to allow organizations and individuals to help achieve cyber security.

[11] This section is drawn from *The Software Assurance Competency Model: A Roadmap to Enhance Individual Professional Capability* [Mead 2013a].

[12] http://www.cert.org/news/article.cfm?assetid=91675&article=156&year=2014.