CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Software Assurance: A Master’s Level Curriculum

Key Message: Knowledge about software assurance is essential to ensure that complex systems function as intended.

Executive Summary

Because complex systems affect nearly every aspect of our lives – in areas such as communication, transportation, banking, defense, and energy – it is crucial that these systems are resistant to and resilient against threats. Securing those systems requires professionals with the knowledge and skills necessary to understand and meet the challenge. Unfortunately, there are not enough of these professionals to meet the growing demand.

Many colleges and universities have degree programs in areas such as software engineering and information security, but programs and tracks in software assurance are lacking. In collaboration with educators from Embry-Riddle Aeronautical University, Monmouth University, and Stevens Institute of Technology, CERT has developed the first curriculum that focuses on assuring the functionality, dependability, and security of software and systems.

In this podcast, Nancy Mead, CERT; Tom Hilburn, Embry-Riddle Aeronautical University; and Rick Linger, CERT, discuss a master of software assurance curriculum and how academic institutions can integrate this into their existing offerings.

PART 1: WHY DO WE NEED THIS CURRICULUM?

Definition of Software Assurance

This curriculum defines software assurance as follows:

Application of technologies and processes to achieve a required level of confidence that software systems and services function in the intended manner, are free from accidental or intentional vulnerabilities, provide security capabilities appropriate to the threat environment, and recover from intrusions and failures.

Purpose and Motivation

This curriculum builds upon and extends earlier work such as the U. S. Department of Homeland Security Build Security In website, which is intended for professional software security and assurance practitioners.

Based on this earlier work, the team realized that the development of knowledge and skills needed to occur earlier in the educational pipeline, both for current students and those already in the workforce.

A second motivation was to build upon and extend efforts to develop curricula for the Master of Software Engineering degree programs.

Special Areas of Emphasis

Areas of special emphasis and unique properties (shown in italics) that distinguish this curriculum from traditional software engineering and computer science programs include a focus on

- software *and services*
- development *and acquisition*
- *security* and correct functionality: defective software isn’t dependable or secure

- *software analytics*: the ability to analyze software to ensure that it has both the right security properties and the right functionality
- *system operations*: monitor and assess to ensure that systems continue to have the right security properties in their operational environment
- *auditable evidence*: the ability to produce rigorous evidence of assurance processes and outcomes

Curriculum Sponsor and Developers

The sponsor for this work is the U. S. Department of Homeland Security National Cyber Security Division. The program manager is Joe Jarzombek.

The curriculum team sought input from invited reviewers as well as via a public review. Developers of the curriculum include:

- SEI: Nancy Mead, Julia Allen, Rick Linger, Jennifer Kent (editor)
- Stevens Institute of Technology: Mark Ardis
- Embry-Riddle Aeronautical University: Tom Hilburn, Andrew Kornecki
- Monmouth University: Jim McDonald

PART 2: CURRICULUM KNOWLEDGE AREAS AND COURSES

Curriculum Knowledge Areas

Knowledge areas are organized into two categories and seven topics as follows:

- Assurance Process and Management
  - Assurance Across Life Cycles: requirements, specification, design, implementation, testing, evaluation, operational use
  - Risk Management: understand, identify, and classify risks; analyze potential impacts; understand mitigation methods
  - Assurance Management: business case, cost-benefit models, ROI, compliance
  - Assurance Assessment: measurement, business survivability and continuity, system monitoring, auditable evidence
- Assurance Product and Technology
  - System Security Assurance: analysis of threats, attack methods, defensive techniques, ethics and integrity
  - System Functionality Assurance: correct functioning, methods for all life cycle phases, assured software analytics
  - System Operational Assurance: monitoring technologies and methods, responding to adverse events, maintain business survivability

Curriculum Architecture and Courses

- A masters degree program focused on software assurance (referred to as standalone)

  - This consists of eight courses that cover the body of knowledge and a capstone experience course. The eight courses include assurance management, assurance assessment, operational assurance, system security assurance, and software analytics, and three development courses that address requirements, architecture, design, construction, and testing.

- A software assurance track within an existing degree program

  - This consists of six courses and a capstone course.

PART 3: WHAT STUDENTS AND EMPLOYERS CAN EXPECT; GETTING STARTED

Student Outcomes

Students of this curriculum will have the ability to

- deal with the security and quality of software systems in a comprehensive way
- understand and be able to describe and apply assurance concepts in business terms: management, assurance assessment, people, and processes
- understand system requirements and specifications, and how they meet business needs
- assess software quality and security at a technical design level
- serve as a focal point for integrating assurance activities across the organization

Steps for Getting Started

Those interested in implementing aspects of this curriculum can get started by taking the following steps:

- Download and read the curriculum report. Understand the outcomes, body of knowledge, architecture, and course descriptions.
- Determine what you are doing in your existing curriculum that matches up with assurance curriculum outcomes, and identify potential changes and improvements.
- Identify courses with minimal prerequisites and start with one of these.
- Consider creating a software assurance track within an existing program.

The CERT curriculum development team is prepared to assist institutions in getting started.

Near Term Plans

The curriculum team will be tackling the following tasks in the coming year:

- Identify assurance specializations within other degree programs (beyond software engineering), for example programs focused on IT.
- Determine how to adapt the curriculum for international degree programs.
- Develop more detailed course outlines and supporting resources and course materials.
- Form a network of educators and provide support and mentoring to them.

In the longer term, address how to apply the curriculum at the community college and high school levels.

The team has done initial work to identify a set of undergraduate courses in software assurance.

Resources

CERT Software Assurance Curriculum website

Software Assurance Curriculum Project Volume I: Master of Software Assurance Reference Curriculum: Software Assurance Curriculum Project Volume I: Master of Software Assurance Reference Curriculum

Software Assurance Curriculum Project Volume II: Undergraduate Course Outlines: Software Assurance Curriculum Project Volume II: Undergraduate Course Outlines

MSwA Course Outlines: MSwA Course Outlines

A workshop presentation on getting started in software assurance