Establishing the Demand Signal for Good Software Assurance (SwA)

Carol Woody, Ph.D.

Principal Researcher

Software Engineering Institute

January 23, 2024

DM24-0065

About this Panel

GOAL

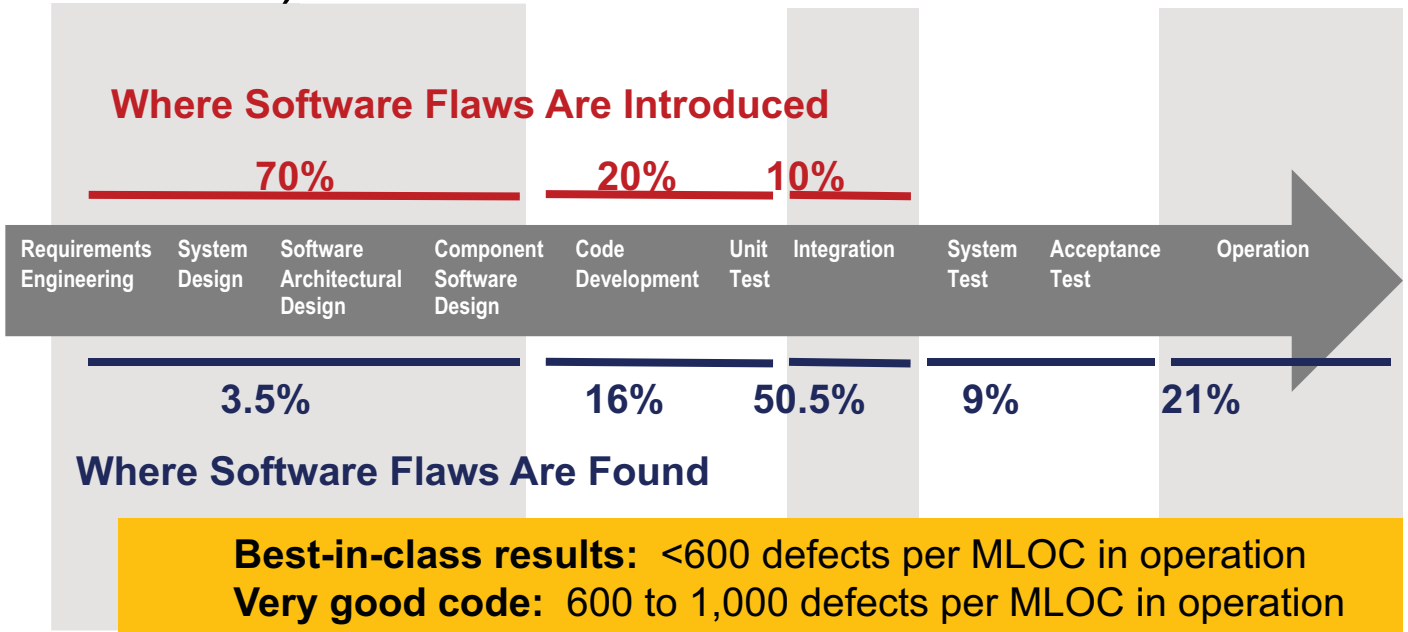
Instead of reacting to attacks and vulnerabilities, acquisition and development should build better technology with fewer potential vulnerabilities in the first place:

> *Software Assurance:* Establish confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner. [CNSS Instruction No. 4009]

> *Software Assurance:* The level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the lifecycle.[DoDi 5200.44]

Panel participants have demonstrated expertise in aspects of delivering better results and are here to share their experiences and lessons learned.

Research Shows All Software Has Defects (and Potential Vulnerabilities)



Best-in-class results: <600 defects per MLOC in operation
Very good code: 600 to 1,000 defects per MLOC in operation
Average quality code: 6000 defects per MLOC in operation

5% of operational defects are potential vulnerabilities

Sources: *Critical Code*; NIST, NASA, INCOSE, and Aircraft Industry Studies

Panel Participants

Software Engineers:

- Michael Murrah, Ph.D., Software Engineer at Missile Defense Agency (MDA)
- John J. Keane Jr., The Software Angel of Death
- David Brown, founder & CEO of Purposeful Cloud

Educators:

- Carol Lee, Director and Chief of the Center for Assured Software, NSA
- Tom Hurt, Professor, Information Technology (Cybersecurity) DAU Cybersecurity Learning Team
- Rita Creel, Adjunct Professor, George Mason University and Director, Software Architecture & Engineering, The Aerospace Corporation

Instructions for Each Speaker (10 minutes per panelist)

Describe your experience in delivering good software assurance capabilities

Provide your input to the following:

- What has been your motivation for addressing the SwA challenge?
- If you were starting your career planning today, what would you want to learn about software assurance (SwA) to position you to be an exceptional job candidate?
- Where would you want to be able to learn this (school, OJT, online, ChatGPT)?
- What practices and environments do workplaces need for these educated workers to have an impact?
- How might you evaluate job candidates for this capability?

Wrap-Up – Audience Input

Based on the discussion, what resources/education are needed to ensure you and your people can address SwA?

Any other thoughts or ideas about preparing for good software assurance?