A Software Assurance Curriculum for Future Engineers

featuring Nancy Mead as Interviewed by Suzanne Miller

Suzanne Miller: Modern society depends on software systems of ever increasing scope and complexity in virtually every sphere of human activity: business, finance, energy, transportation, education, communication, government, and defense. Because the consequences of failure can be severe, dependable functionality and security, collectively known as software assurance, are essential. In today's podcast we will be talking with an SEI researcher who has been and is working to develop a software assurance curriculum to teach future engineers.

Welcome to the SEI Podcast Series, a production of the Carnegie Mellon University Software Engineering Institute. The SEI is a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University.

My name is Suzanne Miller. I am a principal researcher here at the SEI. Today I am pleased to introduce you to Dr. Nancy Mead. A transcript of today's podcast is posted on the SEI website at sei.cmu.edu/podcasts.

Nancy is an SEI Fellow and principal researcher at the Software Engineering Institute and an adjunct professor of software engineering at Carnegie Mellon University. She is currently involved in the study of security requirements engineering and the development of software assurance curriculum. She also served as director of education for the SEI from 1991 to 1994. Her research interests are in the areas of software security, software requirements engineering, and software architectures.

Prior to joining the SEI, Nancy was a senior technical staff member at IBM Federal Systems where she spent most of her career in the development and management of large, real-time systems.

Welcome, Nancy. Thank you for talking with us today.

Nancy Mead: Thank you, Suzie. I am delighted to be here.

Suzanne: I want to start off by having you give us a definition of software assurance. I gave just a brief one, but it is really more than what I said. What does this mean for today's software engineers, and are they paying enough attention to it?

Nancy: There are a lot of definitions, but the one that we used in our curriculum work is 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

Now, software assurance is broader than this definition in a way. Our focus was on vulnerabilities, attacks, security. The broader definition would include things like performance and other kinds of quality requirements. But our focus was definitely on correct functionality and security.

Suzanne: You can see where that would be because there is also a lot of other work being done in performance and other attributes of software. But you are really filling a gap in terms of looking at the vulnerability aspects and security aspects as software is being developed. Not just after it's fielded.

Suzanne: So that is really where that focus comes from.

Nancy: Some of our team members said, *Well, you should be thinking about safety*. We agreed, and actually had to put some disclaimers in that we were not covering all of those important areas.

Suzanne: There has been a lot of work—that is another podcast—but there is a lot of work in software that influences assurance as well.

Nancy: Exactly.

Suzanne: OK. What is the current state of software assurance education today? How much is this emphasized in the undergraduate and graduate curriculum that our software engineers go through?

Nancy: It varies widely from one institution to another, but the basic answer is *Not enough*. It depends on having qualified faculty, interested students, deans, and executives who have vision

and so forth and so on. In high schools and community colleges, it is even further behind than it is at our four-year and graduate-level universities.

Suzanne: So, even though we have high school students writing production-level software in some cases, they are really not aware of some of the dangers that they may be introducing in the systems that they build or the apps that they build for phones and such.

Nancy: That is absolutely correct. Just because it is being used at a production level doesn't mean that it's production quality.

Suzanne: It is not necessarily trustworthy at that level.

Nancy: Exactly.

Suzanne: That is part of what this whole curriculum is trying to change. Tell us please, about the SEI's leadership role in improving these software assurance programs.

Nancy: With support from Department of Homeland Security, we developed a series of curriculum documents starting at the master's level. That drew on our prior work in developing the master of software engineering curriculum. The master of software assurance curriculum included course syllabi. Then we went on to do recommendations for undergraduate and community colleges, and we talked about how our work would relate to information systems programs.

We also developed a complete set of syllabi at the graduate level and we developed some of the standard courses that we would like to see in the curriculum. The Master of Software Assurance Curriculum Project document is our flagship document and was endorsed by both IEEE Computer Society and the ACM [Association of Computing Machinery], the two biggest professional societies in our field.

We also developed an executive course that is available on our STEPfwd facility and materials for the *Assurance Management* course and *Assured Software Development 1*, which focuses primarily on requirements and architectures. Once again, trying to get the early stages of lifecycle before people have started coding and before they have introduced vulnerabilities.

We have a repository of course materials and lecture materials available from our website for free download. We've also maintained a LinkedIn group of software assurance educators. We currently have about 500 members in that group.

Carol Sledge who worked with me on many of these activities has been instrumental in outreach to universities, and we have made a number of presentations at conferences. We have done seminars and webinars. Several years ago we did a very early podcast.

For now, the transition work is continuing as an SEI activity, although at a lower level of effort than when we were working with Department of Homeland Security.

Suzanne: As someone who has taught courses and built curricula in the past, this is huge. You have got everything from helping guide what a software engineering department would want to invest in, as well as giving them assets.

You're not just giving them, *Here is what you should teach*. You are actually giving them good materials that they can use. So this is a huge service to the academic community, as well as to the students. What have you seen change in the approach of universities and academics in response to having these assets available?

Nancy: We had a number of universities that made changes to their curricula to try to offer courses, tracks, and even degree programs in software assurance. Among them are Stevens Institute of Technology. Of course, Carnegie Mellon, the U.S. Air Force Academy, University of Detroit-Mercy, University of Houston, Illinois Central College, and also (ISC)², a training and certification organization.

At a deeper level, (ISC)² mapped the curriculum to their course offerings. We published that mapping. At Polytechnic University of Madrid they designed a complete Master of Software Assurance that is available. A really exciting new development is with Illinois Central College. They have implemented a two-year program under the leadership of Girish Seshagiri at ISHPI and Julie Howar, who is a dean at Illinois Central.

The program is a two-year program. There is an option for students to do an industry apprenticeship, so that they are employed by industry, and they get their tuition paid for. If they continue they have the option to continue to a four-year degree. They started offering the program this fall. They have 20 students enrolled. There are 13 that were accepted into the apprenticeship program. Julie tells me that they are still getting phone calls coming in. It is really exciting, and it is a unique program. The other thing that is important about it is that, prior to this, at the community college level the focus was primarily, if it existed, on securing systems after they were in the field.

Suzanne: Operational security.

Nancy: Exactly. This is one of the first programs to focus on secure software development.

Suzanne: Nice. This is one of my favorite projects. I know Carol well, and so I get to talk to her about this kind of thing on a fairly regular basis. I know that this work involved collaboration with many of the best and brightest minds in the field.

Can you tell us a little bit about some of the—you have mentioned a couple of the collaborators— but tell us about some of the other folks that have contributed to this really massive project.

Nancy: It was quite a number of volunteers, and that was terrific. On the SEI staff we had Julia Allen, Bob Ellison, Carol Sledge, and Carol Woody. Julia, as you know, was at one time a deputy director here at the SEI. She has a tremendous view of how things are seen from the industry side.

Suzanne: And from an executive perspective. She is really good at representing that sort of persona.

Nancy: Bob has worked with me for years. We have done a lot of work on survivable systems together. He was the developer of the assurance management course. Carol, as I mentioned, worked with us right along throughout the curriculum development effort and primarily on outreach. She also worked with me on the Assurance Software Development 1 course. She has done a terrific job.

Carol Woody has taught the material both here at Carnegie Mellon, as I have, and she has also taught it in executive environments and to some of our DoD customers. It has been a very nice collaboration in-house, but we had a lot of folks externally as well.

Mark Ardis at Stevens Institute of Technology, Mark was one of the original developers of the master of software engineering curriculum and actually worked here at the SEI for a while. He was a terrific person to have on board.

Beth Hawthorne with Union County College—that is a two year school—Beth is heavily involved with ACM, so she was able to help us with some of the networking that we had to do with the ACM staff. She also had that unique community college perspective.

Nancy: It's very interesting. My granddaughter did a community college degree while she was still in high school. When we went to the graduation we saw that there was a very diverse group in the graduating class, many of whom had been working or in the military and then gone back to school, maybe going for a completely different degree than what they had before. So, yes, it is very different.

Nancy: Some of the other members included Tom Hilburn, who is from Embry-Riddle Aeronautical University. Tom worked with us indirectly at the SEI as a resident affiliate and occasionally as a contractor. He worked with me on software engineering curriculum projects.

Glenn Johnson with (ISC)². I've mentioned that they mapped our curriculum to their own course work and I gave a briefing to their board of directors who later helped us with the software assurance competency document that was an outgrowth of the curriculum effort.

Andrew Kornecki, a faculty member at Embry-Riddle as well, and one of our safety and real-time systems specialist. Jim [James] McDonald at Monmouth University, he was a department chair in software engineering and also had a long history with us. Then Dan Shoemaker at University of Detroit Mercy. We met through our work with Department of Homeland Security and who has collaborated with us on many activities, including the curriculum work.

Suzanne: This is not the only curriculum work that you have done. You and I worked on a larger SEI team on a rollout of software competencies to the Defense Acquisition University, which is the global learning environment for staff who work in acquisition and deliver and sustain effective and hopefully affordable war fighting capabilities for the Department of Defense.

Tell us a little bit about some of the other activities for transitioning ideas like the software assurance into our stakeholder community at the SEI because we have not just…You focused on academic and students with the curriculum, but we all work with DHS programs and DoD programs. How do you get some of these ideas into those communities as well?

Nancy: One of the interesting outgrowths of the curriculum work was the Software Assurance Competency Model. What the competency model does is to describe five levels of competency in software assurance from novice to expert. And then to look at each of the curriculum areas to describe what a novice or an expert or someone in between should know.

We were able to use that work when we started working with DAU, the project that we were both involved in, and we were able to leverage it by using some of the areas and comparing them to the DAU competencies. We also did a comparison with a DHS competency model that had been developed in parallel, and our software assurance competency model was again endorsed by IEEE Computer Society. We were very pleased.

Suzanne: IEEE has done other competency models. They have done one in software engineering. INCOSE has got one in systems engineering. So the idea of competency models is one that is used to get professionals to be more aware of areas of knowledge and skills that they may need to update and may need to refresh, or it may be new to them if they have been working in a very narrow band in their discipline. So these are very valuable tools for professionals, not just for educators.

Nancy: Absolutely. Interestingly we started the Software Assurance Competency Model about the time that IEEE was thinking about the software engineering competency model, but we finished ours first.

Suzanne: Sometimes the size of the committee has something to do with how long things take, and IEEE tends to have pretty large committees.

Nancy: I ended up being a reviewer for the IEEE document as well.

Suzanne: What other areas in software engineering and cyber security do you see in the curricula of our software engineering universities especially that need more emphasis, and what does that lead you to in terms of work for you in this area?

Nancy: Well, there is a lot that has changed in the five or so years since we first published the Master of Software Assurance curriculum. For example, cloud computing wasn't really on anybody's radar at the moment. The risks associated with mobile, even though they existed, were not emphasized and were not publicized. Risks associated with COTS software and acquisition.

Suzanne: COTS is commercial off-the-shelf software.

Nancy: Yes. Thank you. Then supply chain risk management. A lot of those activities and interests were going on either in parallel with our curriculum work, or they hadn't started yet. There are a lot of new areas.

Suzanne: All the areas you've mentioned, the SEI has researched in the issues: in cloud, in mobile, etc., but in terms of your work, it is really looking next at translating what we've learned about those into something that educators can use. Is that correct?

Nancy: Absolutely.

Suzanne: That is special stuff. I applaud you and your collaborators. I know how much work this has been, and continuing to work in this area is fantastic. I want to thank you for joining us and talking about this today.

To view a technical report that Nancy co-authored on this topic, please visit the SEI digital library at resources.sei.cmu.edu/library. In the search field enter the name of the technical report, which is Software Assurance Curriculum Project Volume 1 Master of Software Assurance Reference Curriculum, or you can type Nancy's name in the author field. We will include links to these assets in our transcript.

This podcast is available on the SEI website at sei.cmu.edu/podcasts and on Carnegie Mellon University's iTunes U site. As always, if you have any questions, please don't hesitate to email us at info@sei.cmu.edu. Thank you for listening.