AADL and Aerospace

featuring Peter Feiler and Myron Hecht interviewed by Suzanne Miller

---

Suzanne Miller: 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 at Carnegie Mellon University in Pittsburgh, Pennsylvania. A transcript of today's podcast is posted on the SEI website at sei.cmu.edu/podcasts.

My name is Suzanne Miller. I am a principal researcher here at the SEI, and today I am pleased to introduce you to my friend and colleague Peter Feiler, who is the technical lead and author of the Society for Automotive Engineering's Architecture Analysis and Design Language, known as AADL. Peter's research includes dependable real-time systems, architectural languages for embedded systems, and predictable system analysis and engineering. In 2009, he received the Carnegie Science Award for information technology for his work with AADL.

The AADL Standards Committee is meeting in Pittsburgh this week with members from throughout the globe to discuss evolving elements of a standard and to work together on action items from prior standards meetings.

So, Peter, you've brought Myron Hecht from Aerospace Corporation to talk with us today about his involvement with the AADL standards committee and what aerospace is using AADL for. Why don't you give us a little introduction please?

Peter Feiler: Sure. Myron Hecht, as you said, is at Aerospace Corporation. He doesn't deal so much with the aircraft industry, but with space. They're doing a lot of work for NASA and JPL [Jet Propulsion Laboratory] in terms of safety and various other functions. Myron's specialty is safety analysis.

Suzanne: So, Myron, why don't you tell us what your involvement with the AADL standard is and what is it that you find important about AADL for the kinds of safety-analysis work that you do?

Myron Hecht: Okay. Well, AADL to me represents a way of enabling practitioners in the dependability community.

By dependability, I mean reliability, safety, and security, to be able to interchange models and thoughts and analyses in a structured way. The problem with the field at this point is that there are a lot of good ideas, but we don't understand each other because it takes too long to figure out what everybody is doing.

The biggest problem that we have in these analyses is the unstated assumptions and unstated limitations. The sooner we get onto a standard platform where we're all speaking the same discipline really, the sooner we can begin to make major progress in building the next generation of computerized systems, which people's lives may depend even more on the computer itself, without any manual intervention. I have no idea how we're going to do driverless cars. I have no idea how we're going to do home medical devices for critical illnesses unless we really get greater confidence in our ability to do the analyses.

Suzanne: So, how does AADL contribute to helping us to make the transition from unstated to stated assumptions and limitations?

Myron: Well, the most important contribution that AADL made from its origination in the aircraft industry, when it was born out of an earlier project from DARPA, where they really intended to develop real-time systems for avionics applications, simply by specifying them in the design.

When you work in that environment, one of the things that you're really worried about is what happens if things go wrong. If your car radiator blows over, you can stop by the side of the road.

Suzanne: Not so much if you're at twenty thousand feet.

Myron: Yes, that's the problem. You've got to keep going when you are on an airplane. The aircraft industry, basically its entire existence, depends on being able to assure the public that nothing bad is going to happen to them if they get on this contraption.

Suzanne: That contraption is more and more controlled by software, not mechanics.

Myron: Exactly. So, that was the origin of AADL. Along with that came this thing called an error annex. The error annex gave a way a specifying the behavior of the system when things went wrong, in other words when failures and errors happened. So the ability to express the failure behavior of the system enables us to express our assumptions and also enables us to express the limitations of the analysis that we're doing.

Suzanne: So, is the error annex the area that you've been working on with the standards committee?

Myron: Yes. Well, I've been watching Peter do the development and Peter was very receptive to my ideas initially. Most of what is in the error annex is not mine, but nevertheless, I do believe

that I influenced it. The reason why I influenced it is because Peter was open and had the conversations that we had in various corners of the world, Toulouse, I think, Vienna, several other AADL meetings.

Peter: Yes, but Myron is a little bit modest because he used the first version of the error annex, which came out in 2006, and extended some original tooling work by Ana Rugina to build a tool suite that helps him in his actual work, which is with real customers and maybe you can comment a little bit about that.

Myron: All right. So, what we want to do in AADL—because it's both a design language, which has if you will, the capabilities in it to do safety analyses. It [AADL] is called the architecture analysis and design language which, so it does both design and analysis—is that we can actually take a design, something that people work with something that designers use, and then that evidence and those artifacts immediately and without any manual conversion, without having to say, *Give me something, you change it, I don't want to know about it, because I need to work with something stable.* Then coming back six month or a year or two years later and saying, here's the result of our analysis and showing it to the designers and saying, oh, by the way, we changed that.

Suzanne: So you can do much closer to time of design when you do the analysis?

Myron: Not only that, there's no effort involved in transformation. If the people doing the design are not the same people as the ones doing the analysis, but they're using the same artifacts, then I just take what they give me, and I can begin to do work on it.

The techniques we use involve taking a description to the architecture, and the description of its error behavior, and by doing that you can start doing wonderful things. You can start thinking about *Gee, what are the combination states that it can be in? In what state is it working?*

Suzanne: How can it reach this state where this terrible thing would happen?

Myron: Right. Exactly. How could it recover? What's the quantitative reliability and availability? What's the probability of getting in to particular state, for example, using a fault-tree analysis. All of this is possible immediately, almost, or can be possible as we develop the tools to do this. Now, the point about this is that if the designers are aware from the beginning that their design is being analyzed, A, they're more careful, and B…

Suzanne: What gets measured gets done. That's an old adage, and it applies here, too.

Myron: Well, I think what is more to the point is that they get insight into the failure behavior and the weaknesses of their system and what they might have to do to improve it. Not only that, but the sponsor of their work, who is typically not the designer himself or themselves, is going to

know what's going on. Going to be able to monitor that part of the process and program manager.

Suzanne: It gives them their insight into what's going on and what's going on with how to correct some of the error-behavior kinds of conditions.

Myron: So that constant feedback between a design and analysis, which now becomes a very tightly coupled loop in a very, very rapid process, is one of the key enablers to enable us to build complex safety-critical, life-critical, and mission-critical systems.

Suzanne: So, what plans do you have that are new? There is a new constraints annex being built, which I think also connects with the error annex in some ways?

Myron: Well, they all work together.

Suzanne: What do you see as sort of the next steps for you in your work with the AADL?

Myron: Well, given the error annex and the proper tools, we'll be able to take—and by the way the commitment of the designers to use AADL—then we can start developing a basically a set of analyses and a set of tools to perform those analyses. What I'm also very interested in is I become a senior engineer, which means that you become later in your career, is that you worry about presenting it to the stakeholders, the regulators, and the managers.

Suzanne: The certifiers.

Myron: The certifiers, everybody who wants to know about that system and who wants to know that they're not going to be making a terrible mistake by approving it.

So, the error annex, the specification, the tools, and the way that we present the results, all go together to enable that to happen.

Suzanne: Excellent. And, you're applying this in the space domain.

Myron: Right.

Suzanne: So you're also giving the committee feedback, if there are areas where the notations need to be extended or the notations don't work the way they're expected in that domain, so you are actually giving them some more feedback in that arena also, aren't you?

Myron: Well, with all due respect to the space environment, it's not the most challenging environment we have to deal with and AADL handles it pretty well.

Suzanne: That's good!

Myron: It's quite similar to the avionics environment from which it came. As a matter of fact, the control systems on the satellites, we call them avionics.

Suzanne: Okay. So that makes it a natural fit then.

Myron: I guess. People get lazy. They couldn't invent another word like astronaut, astronics, or whatever it is.

Suzanne: We have enough extra words, especially in the software industry. We don't need anymore.

Myron: I think, in more complex situations, I think that driverless vehicles are really going to be the...

Suzanne: I don't think I need to be driving when that happens. I mean, I don't know. I didn't say that right. I don't' think I want to be riding when that happens. We're not there yet.

Myron: Yes, but a failure like that is, I think, one of the areas we're addressing. I did want to say that one of the things that I think AADL tool users contribute—and I do consider myself one of the primary pioneering users (that's not necessarily a compliment to myself, but it's the fact that somebody's got to get their arrows in the back and that's me)—is I am able to identify needs in the analysis and needs for additional properties and descriptors and links that….

Suzanne: That make it more useful for things like you are talking about, not just doing analysis, but presenting it as well as connecting it to other kinds of analyses that you would normally want to do as part of your safety analysis.

Peter: That's exactly what we appreciate both in terms of committee—we get user input, since we are revising the error annex—and then also in terms of from the SEI side—putting a tool suite together and turning the revised capability into a practice to connect it with the practice that real people do. Like Myron was pointing out, generate reports that people are used to seeing and are able to process, not just computer geeks.

Suzanne: Very good. Myron, thank you for joining us. Thank you for coming out this week to Pittsburgh and I hope you're enjoying the week with all of your colleagues here. Peter, thank you for letting us talk to some of the folks here that have been contributing along with you to moving AADL forward.

I think if we do get things like driverless cars, it's going to be because we have these kinds of languages and this capability of building confidence in what we've done, and so I think it's very important.

Thank you so much.

Peter: You're welcome.

Suzanne: If you, our listeners, would like more information about AADL and the work of the standards committee, please visit the AADL Wiki site at www.aadl.info, that's all one word.

Peter: Or, the public AADL wiki at www.aadl.info/wiki.

Suzanne: This podcast is available on the SEI website at sei.cmu.edu/podcasts, and on Carnegie Mellon University's iTunes U site.

If you have any questions, please email us at info@sei.cmu.edu.