AADL and Dassault Aviation

featuring Peter Feiler and Thierry Cornilleau 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 the standard and to work together on action items from prior standards meetings. Peter, thank you for bringing Thierry Cornilleau to see us today. He is here with the AADL standards committee. Could you introduce him to us and tell us a little bit about how he is connected to the AADL committee?

Peter Feiler: Sure. Thierry actually works for Dassault Aviation. For obvious reasons, they are interested in AADL. One of the things that he brings to the table, obviously, is the problem space, but also, from their end, interest in ARINC 653, which is another standard and the connection between AADL and ARINC 653. We have an annex in that context, and Thierry was working with Julien Delange on that.

Secondly, Dassault itself is very progressive in using formal method tools. There is, for example, a language called AltaRica that is being used for fault modeling of systems and then fault analysis which then obviously ties into the error model annex. It is from those domains where he then can come and help us make sure what we define as a standard fits with their needs and their industry.

Suzanne: So, Thierry, have you been involved in AltaRica also? So, you work with AltaRica at Dassault?

Thierry Cornilleau: Hi. I'm not, in fact. We, we have many experts and safety experts. We are not only involved in AltaRica. For me, I am more an expert in avionics and AMA (Aerospace Mechanics and Avionics) and so on.

Suzanne: So, the language aspect.

Thierry: The language aspect and the avionics architecture by itself.

Suzanne: OK. So, that is what you are bringing to the standards committee is both that language base as well as understanding some of the problems.

Thierry: Yes and no. It, it was a long story because before me there was a Serge Bruillot who was involved in the introduction of the standard. At that time, we made a lot of experiments at Dassault with AADL. But, between v1 [version 1] and v2 [version 2], we stopped the efforts because there was a slowdown on the tool side.

Suzanne: OK. On the OSATE tool?

Thierry: Yes. Now, we are very impressed by new stuff introduced by Peter and his team. I will push certainly next year to begin new experiments on AADLv2.

Suzanne: So, you are here as much to find out what the new things are with AADL and to connect with other AADL committee members.

Thierry: Yes. Because in Europe, as you know, we are in economic crisis. So, it is difficult to find money to attend continuously the committee [meetings] and also to provide some inputs for the committee.

Suzanne: So, this is an opportunity for getting back into the committee again and seeing what progress they have made in the time that you were not able to be involved?

Thierry: Yes. Yes.

Suzanne: So, what kind of experiments that are new, that you have not done before, that you believe are possible with some of the improvements to AADL?

Thierry: The major improvement I saw this week is the error modeling annex.

Suzanne: Which you have a great deal of interest in, if you have fault tolerance issues, yes?

Thierry: And, the second major improvement I also saw this week is the maturity of OSATE.

Suzanne: OSATE, for those who are not familiar with it, is a tooling environment that implements AADL within the Eclipse open-source environment. So, it is an open-source set of tools that people exploring AADL can use to do experiments like Dassault does.

You said there's a couple of major improvements to AADL. What do you think you can do with those improvements that you haven't been able to do before?

Thierry: Probably, I wish to warn my management to begin study about the way to modernize fine tuning on top of ARINC 653 base and the work did by Peter and his team. It could be a good step to cover next month, yes.

Suzanne: So, basically connecting the error modeling annex and some of that work to the ARINC 653 annex in a way that you can then leverage the things you already have going on with AltaRica and other things you are doing at Dassault. So, all of this is basically to make safer avionics systems for all of us.

Thierry: Not necessarily safer but to rise quicker development.

Peter: From the committee side, what is interesting with Thierry is that there are some other people in his organization who are members of the ARINC 653 committee, for example.

Suzanne: So, you get to talk directly with those folks.

Peter: Exactly. This is where then he connected Julien Delange, who was the main author of the ARINC 653 annex we had with those people. We had direct connection between the two committees. What is interesting about ARINC 653, in addition to laying out a partitioned architecture, is that they also have some guidance for health monitoring, but it is not formalized guidance yet.

Suzanne: And by health monitoring, you mean the health of the avionics system.

Peter: Yes, health of the avionics system. That provides some basic guidance. With our now more formalized notation, one could get into a discussion with them in what way can we now provide more formalized guidance on expressing this health monitoring architecture that they are suggesting to people. So, what we get into is that the AADL Committee cooperates with other committees to put AADL to use in other settings as well. That is kind of fun to do.

Suzanne: That's actually a very nice way of leveraging the work of both committees. Every committee works hard. So, being able to get some synergy between them is a really good thing.

Well, Thierry, I hope that you have enjoyed your week here in Pittsburgh. I know it has been a little bit rainy, but hopefully we will get some sun before you leave. I hope that you get to make

some of the experiments and get to do some of the research that you are talking about with AADL, and then come back to the committee and contribute what you learned from them. Thank you very much.

Thierry: Yes, of course. Thank you.

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 http://www.aadl.info/aadl/currentsite that's all one word.

Peter: Or, in short, www.aadl.info.

Suzanne: 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.