An Open Source Tool for Fault Tree Analysis

featuring Dr. Julien Delange as Interviewed by Suzanne Miller

---

Suzanne Miller: Welcome to the SEI Podcast Series, a production of Carnegie Mellon University's Software Engineering Institute. The SEI is a federally funded research and development center sponsored by the US Department of Defense and operated by Carnegie Mellon University. A copy of today's podcast is available at the SEI's website at sei.cmu.edu/podcasts.

My name is Suzanne Miller. I am a principal researcher here at the SEI. I am very pleased to introduce to you once again—he has been a guest of ours many times—to Dr. Julien Delange who is one of our researchers at the SEI, and who is going to be talking to us today about Fault Tree Analysis (FTA) and tools for doing that.

Dr. Julien Delange comes to us from the European Space Agency and has been working for several years now on the Architecture Analysis and Design Language (AADL).

Welcome, Julien.

Julien Delange: Thanks for having me, Suzanne.

Suzanne: I am very glad to talk to you about this. So fault tree analysis is a standard systems engineering tool for understanding how failures can happen and have happened. This is something that is very important within the systems-engineering community, so I can certainly understand why it is been taken up by the AADL team.

Why don't you tell us a little bit about how you came to be working in this area, and what your current progress has been in developing this open-systems tool.

Julien: It started in fact when we worked for a project with the SAVI [System Architecture Virtual Integration] consortium.

Suzanne: SAVI is the consortium, the avionics consortium, that is using AADL to do various kinds of experiments and actually use it in their work in developing avionics products.

Julien: That is correct. SAVI stands for System Architectural Virtual Integration. In fact, during this project, we were working on AADL and safety. If you look at the different standards required for avionics safety, fault-tree analysis is one of the analysis you need to do.

Suzanne: Right. Every standard needs that.

Julien: In fact, we started to implement different tools. Many analysis like FHA (Functional Hazard Assessment) or FMEA (Failure Mode and Effects Analysis), the tool is not difficult to support. Basically people are using spreadsheets or document like this. It is easy to export the analysis results in Excel or Word. What we faced for fault tree is that we have no tool.

Suzanne: There was not an existing tool out in the space that you were working in that related to the avionics.

Julien: There was. In fact to be honest there are some commercial tools available, but that is an issue when you are doing research because as a community you want a tool for example that is not expensive and you can modify. There was a tool that was available online, but it is really outdated like the tool was about five or eight years ago.

Suzanne: In today's world, yes, that is outdated.

Julien: For example you have to change the source to make sure it works. On Linux there was some issue with Java. For example, backwards compatibility issue. The issue as well as how to integrate that with OSATE and the AADL modeling environment.

We decided, Peter Feiler and myself, to start a new tool. In architecture, there is a modeling framework called EMF, Eclipse Modeling Framework. We built on top of it a new model to design a fault tree. We used it, and after that, there is a really good framework called Sirius developed by a French company called Obeo. We worked with them to make the graphical presentation.

We did that really quickly. We came up with this new tool called EMFTA. This tool is totally integrated into Eclipse and allows you to edit and design your fault tree. It is totally open source. It has been released under the BSD license and anybody can pick up the source on the SEI Github repository. It is totally integrated within OSATE. You can even download OSATE, the latest OSATE version and test it.

Suzanne: Now within using the virtual integration capabilities of AADL—if part of what you are trying to analyze is the compliance to standards that require a fault tree—you can look and see how much of a fault tree I can build with the current representation of my model. Can you see what is missing and things that you are going to have to bring into the model to make it complete enough to do the fault tree?

Julien: That is correct. We have this, and what is really nice with this new tool is that we wrote this tool from scratch. We started to see how we can generate the fault tree from the model better, so how we can optimize the fault tree.

For example, *Is there a way to improve the fault tree? Is there a way to compute probabilities of a failure*? For example, *what is the probability of this failure according to my model, according to how my model is designed? Do I have redundancy?Do I have common failure? So what are the failures that affect different components*? this type of thing.

How I can optimize my fault tree, for example, if I have different nodes in the same place in my fault tree maybe I can optimize it. Maybe I can suggest some refactoring of the fault tree, this type of thing. What is nice is by having the source it was easy for us to add new features and new functionalities into this new tool. Something that is, for example, not supported in some other tools.

Suzanne: Not only do we get a basic fault tree, but we get some optimizations that are not possible when you are not doing virtual integration, right? This is the synergy between the fault tree analysis and the modeling using the AADL language and the OSATE toolset.

Julien: That is correct. Another thing that is really useful in AADL is an SAE [Society of Automotive Engineering] standard.

Suzanne: Society of Automotive Engineering, their avionics division, is the one that supports the standard?

Julien: There is a group that is called the S18 Group related to safety. What is nice we worked with this group to improve the fault tree and ask them if our tool makes sense for them. It is like having the endorsement from the safety community and also spread the word, *Hey, this tool exists.*

Suzanne: Now is this tool limited in its current instantiation to just avionics kinds of systems? So it can be used for automobiles. It can be used in other kind of transport, and it can be used even in finance or insurance or any kind of application where you want to be looking at how different faults could lead to different interactions in components of your system.

Julien: That is correct.

Suzanne: So, even if you are not using an AADL, you may want to take a look at this fault tree analysis tool if you have risks related to failure. I mean do not we all have risks related to failure in our systems?

Julien: Correct and even in the example of EMFTA we have a medical example for an isolette system.

Suzanne: Yes, medical devices I can see. I know the FDA requires all kinds of documentation on safety.

Julien: Automotive is the same thing, so you can support any domains.

Suzanne: So, if we have listeners out there that are thinking about how they would want to get access to this, you said it is on the [SEI's] GitHub repository. They would go into the SEI website and that link will be available on our website with this podcast, so people can just look there for that repository. I assume there is some documentation there.

Julien: There is full documentation about the functionality, how to design a fault tree, how to have a different representation as a graph or a table. It is a different optimization and feature we provide, but also if you get the source on GitHub you have to build the source.

Suzanne: You have to compile it. Yes.

Julien: What is nice is for the end user, we integrate this tool inside of OSATE. So you just download OSATE.

Suzanne: The executable is already there in OSATE.

Julien: Basically even if you do not use AADL, you can still use the fault-tree analysis capability it is no problem. Also, we have this bridge between AADL and the fault tree, but if you are using another language you can also…

Suzanne: Connect to another language?

Julien: Exactly. That is not a problem.

Suzanne: Well, I know there are people out there that that are going to be very excited about this: safety engineers, systems engineers that have to do these kinds of analyses. I have done these kinds of analyses in the past, and they are very, very time consuming to do when you do not have this kind of tool support. That is extremely exciting.

What are you going to do next? Are you going to build a course to go along with this, or are you going to take this into some other safety-related modeling kinds of things? What is up on the agenda?

Julien: We started this tool last year for the SAVI project. We were working with Boeing, Rockwell Collins, and Honeywell on that project. Right now we have a new LINE project at the

SEI that is focused on security. It is funny because we talk about fault tree today, but in the security committee there is something called an attack tree.

Suzanne: They have an attack tree. They have got a vulnerability tree. They have lots of trees. There is a big forest in security.

Julien: Basically, we are using the same framework to build that architecture from the AADL model. We currently are working on publishing the tool, raising the tool, applying the tool. We will apply the tool in the avionics domain, also for the SAVI consortium. There is a lot of description about identity security. For example, can you control a plane?

Suzanne: We do not want people controlling planes that are not the pilots.

Julien: There is some claim that it is possible. What is interesting is with the model, we will be able to show if you can reach the plane and the controls. The plane all the systems that control the plane from..

Suzanne: From a model.

Julien: Yes and also can you from the entertainment system reach out to.

Suzanne: That is the classic that people talk about.

Julien: There is also the ADS-B system. For example can you fake planes into the ground station and things like this. We will show that with the attack tree and also as a model that is called attack impact.

Last thing is we are having a big event in September, there is an event called ES Week Embedded System Week in Pittsburgh in October. I will do a tutorial for a half a day that involves security and safety. I will probably use this fault tree analysis tool for my tutorial.

Suzanne: We will include information about Embedded Systems Week on the podcast page as well.

Julien: We have the tutorial for half a day. The AADL Standardization Committee is the same week as SEI. Everybody is welcome to come.

Suzanne: We have talked to some of them in the past.

Julien: Finally we have a workshop about high integrity systems called HILT. We will have talk from Phil Koopman from Carnegie Mellon University. John Knight from the University of Virginia and also Bernard Dion from ANSYS, the company that is providing SCADE, the

SCADE system and SCADE suite, to design safety-critical systems. It will be a big week, a lot of events and hopefully a really good tutorial.

Suzanne: I am sure it will be wonderful. I might even be able to get away and attend. I would love to see that tutorial.

Julien, thank you for joining us and updating on it. This is very exciting work doing things that are open source and accessible to the community is very important to our work. So I thank you for sharing this with us, and I look forward to talking with you in the future.

Julien: Thank you.

Suzanne: Thanks again to Julien and our audience for joining us today. We have several things that are available to you through the podcast link. We have the podcast itself. We will have the link to embedded systems week. We will also have a link to the OSATE tool and the github for the source code for the open source tool for fault tree analysis that Julian was talking to us about.

As always, if you have any questions please do not hesitate to contact us at info@sei.cmu.edu and do not forget that in addition to being on the SEI website at www.sei.cmu.edu/podcasts. This podcast will also be available through Carnegie Mellon University's iTunes U site. Thank you very much for joining.