

IBM Podcast

[ MUSIC ]

MATHENY: Welcome to this IBM podcast, Achieving compliance with ISO 26262. I'm Angelique Matheny with IBM. The upcoming ISO 26262, covering functional safety aspects in the entire lifecycle of in-vehicle electric and electronic systems will add, in many cases, additional requirements to the current EE engineering of automotive OEMs and suppliers.

ISO 26262 will enforce, amongst other things, improved risk and quality management. It will require enhanced traceability, verification and validation efforts, and will demand more documentation for EE system hardware and software engineering.

In today's podcast, we'll discuss how these requirements can be satisfied with the IBM Rational software platform for automotive systems. Karla Ducharme, IBM Rational Automotive Market Manager, joins us and will present the specific workflows and templates available from Rational, and she'll explain the further directions regarding tool qualification support. Hi, Karla. Welcome to the podcast. Thanks for joining us today.

DUCHARME: Hi, Angelique, thanks for having me.

MATHENY: Let's just jump right into the questions. We've got some good ones today. Karla, can you quickly explain the main requirements arising from the upcoming ISO 26262? What does ISO 26262 mean for OEM and suppliers?

DUCHARME: Well, the ISO 26262 standard, right now it's a draft standard. It's published, but it's not the final version, which should be coming out shortly. And it covers the functional safety aspects for automotive electric and electronic systems, as you mentioned, the EE-type of systems, and that includes the hardware and the software development.

There are other aspects to the safety of the vehicle which could be different types of systems. There could be physical-based systems that covers the EE portion of it. It not only defines the aspects of the development, but it addresses the entire lifecycle management. It includes the production, the operation, servicing and the decommissioning of the vehicle and the vehicle parts.

So ISO 26262 is an adaptation, that you could say an extension, of the IEC 61508 Center that's been out there that many have been following for a while. But it's specific for the application to these EE systems within road

vehicles.

And for now it's really going to be targeted at, say, the passenger road vehicles, not the heavy trucks and other things, and that may be coming in the future, but it makes this IE 61508 much more automotive-specific and thus more automotive usable and consumable, you might say.

Since it's an automotive safety lifecycle, or perhaps you could say a process framework, it defines, depending on the safety level, which it defines as an ASIL, which, ASIL stands for the Automotive Safety Integrity Level, or how safe that system needs to be based on how much damage may happen if that particular part of the system fails...

It will define the activities, the methods that organizations shall apply in the various engineering phases.

It describes how organizations should monitor, assess their activities in the different process steps, and what kind of engineering assets and artifacts organizations should produce based upon that ASIL.

Many people I know are already working in safety relevant engineering environments, and they have many standards and processes already in place. So the ISO 26262 is not a big surprise.

The process steps, the engineering activities such as the execution of a hazard and risk analysis method like FMEA, which is Failure Mode Effect Analysis, a very stringent risk and quality management. They're not uncommon in this domain. So it could be just taking that and adding new activities or practices to what they already do.

But what's really specific about ISO 26262 is that, as we mentioned, it defines these risk classes, the ASILs, and it uses those to determine how much should be done for a particular design item or work item in order to be able to adequately cover the given risk of that particular item.

And by doing so, the ISO 26262 standard really defines the requirements for the validation to ensure that there's an acceptable level of safety will be achieved for that part and that will contribute to the overall safety of the vehicle.

MATHENY: Now, these requirements which you just talked about, how are these requirements addressed by the IBM Rational offering for automotive EE development?

DUCHARME: That's good. Well, the IBM Rational software platform for automotive systems is a comprehensive offering. That's our offering both for the OEMs, which would be the ones that would be selling the car as a car manufacturer, as

well as the supplier they have.

It really implements a series of best practices which are required by the ISO standard. And these types of activities would be the quality management, requirements engineering. It can support specific activities as mentioned in the FMEA or the calculation of the ASIL.

It could be a model-based approach using a tool, Rhapsody, a requirements-based approach in DOORS, definitely tracking the safety, the ASIL level of each individual requirement as a trace to a particular design item.

We have specific testing approaches. We have test coverage determination and test RT, which really covers the entire software to make sure that you've tested every possible permutation and combination.

I actually also work in aerospace and defense. Very similar to what we call MPDC coverage. We have the simulation, including the verification and validation of real-time behavior, working with a partner we have, [Enchron].

And that's another component of our offering, is that we understand the ecosystem. We really want to make sure our platform is open to really help integrate tightly in both the offerings and the products that we have, but as well as

those that are the third party or that our customers may have developed on their own through their years of working in automotive industry to really have a nice platform that is interconnected to support this type of development.

And we also have a lot of support for what I would call the supporting processes which aren't necessarily the design, but items such as configuration management, automating workflows, making sure that you have different roles and responsibilities performing those activities.

And those are going to be really important when it comes to audit checks, to make sure that not only do you define a process but can you show that you follow it and make sure you have those artifacts.

Generating those reports automatically instead of spending a few man weeks of time to come up with a report. Those will be important characteristics of the software platform that we provide.

MATHENY: Karla, given the fact that the IBM software systems already offers these capabilities, what else needs to be done by OEM and suppliers?

DUCHARME: Well, our platform addresses all kinds of automotive product development. They can be used for

non-safety applications, for our safety-related ones, such as we're discussing today, different types of development, more of the system hardware or the pure software-oriented, to really what OEMs or suppliers would need to do would be to pick or configure the pieces of our platform that work for them.

If they are a supplier, perhaps they don't need to use some of the system design, some of the sys ML. For this, we do provide some out of the box workflows that they can use as is, or take those and modify them to give them a quick start at what we would call an accelerator to having some of the workflow management, some of the supporting processes and support for some of the standards that are in the automotive industry and our design tools as well.

So, we're helping our clients take some of these artifacts, introduce them into and adapt them for their existing processes, existing roles they have in their development processes and responsibilities as they define them.

So what we see in many cases people are starting pilot projects to introduce these new concepts and methods that are needed for the ISO standards and to see, okay, what do they need to change and what can remain the same.

And it's important to mention that each user will need to

qualify their development tools, the whole tool chain that they have in their engineering environment. So depending upon the tool and how that tool is used, the user will need to ensure that that tool is adequate for the task given the risk and the ASIL level of the type of artifact they're working on.

MATHENY: So, how is Rational addressing the questions about tool qualification?

DUCHARME: Well, for tool qualification, we are doing a couple of things. And as I said, tool qualification depends on how the tool is used. So this determines what impact that tool could have regarding safety. So, for example, can the tool introduce a bug into a piece of software?

The question also, how the tool is used within the tool chain in the development process determines how the big chances are that potential error will be detected such as do you review the output of the tool.

So both the probability that the tool will insert or cause an error as well as the likelihood that an error will either be identified or found during development, contribute to the so-called what I would call the tool confidence levels.

And it's this tool confidence level that determines how much

an organization must invest up front in tool qualification.

And they actually have a specific chapter in the ISO standard that really deals with this in much more detail.

As you can see, because everything relates back to the question how the tool is used within a given tool chain and development process which will be unique for each of our customers, it's difficult to provide a general usable tool qualification.

What we're planning to do is to provide information which is the usage models that are common for that particular type of tool. It will be different for our requirements tool versus a modeling tool, versus a CM tool.

What kind of errors could be introduced, how to mitigate those errors, as well as information relative to our own internal processes from a development perspective, how we address issues that are raised and make other people and other customers aware of those issues, part of our support process.

And all those will contribute and will be pieces of information that each customer can use in situ in their own tool environment to greatly decrease the effort they have to qualify our tools in the context of their environment.

There are companies I know that are coming out with certificates, and with those certificates in and of themselves don't provide the value, but along with the certificates they provide the information to allow automotive customers and automotive companies to more easily qualify their tool in their environment, that's the value part. The whole idea of the usage models, the types of errors that could be identified, things like that are very important.

So in the standards, there are four approaches to qualifying tools. One is increased confidence from use. Second is the valuation of the development process -- and that would be someone like Rational who actually creates development tools.

The validation of the software tools, as well as the fourth one is the development and compliance with a safety standard. That last one, in most cases, wouldn't be applicable, except for a few exceptions.

Now, what we're focusing on, the first three approaches, and combinations of them. So with our large install base that we have, especially for core products such as DOORS and Rhapsody, we can demonstrate that our tools possess an increased confidence from use.

To do so, we have, among things, a well-structured, verified and controlled process how we manage and report bugs, how we communicate any misbehavior and how we fix any problems. Our internal quality checks the validity of our development and support processes.

So with our open connection tool platform, we're able to integrate third-party products in a way that the entire development process can be covered in a single tool and its uses for a certain activity, let's say, the use of Rhapsody for doing a fault free analysis, can be quantified by suitable verification and validation of a generated outcome, for example, by a manual review of the generated model.

MATHENY: Karla, our last question today, what would you recommend to automotive OEM and suppliers? How should they get started?

DUCHARME: Well, I think that for the automotive suppliers and as well as the OEMs, they already have some processes. As mentioned before, they're already addressing some of these aspects about safety, because they have taken safety as a serious product quality and something they want to build into their products for a very long time. So they already have workflows, they have methods, they have a lot of these things in place.

What I see most companies doing are starting to, what I would call, do pilot projects of what tooling do we need to adopt, what changes do we need to come up with in our own workflow, our own processes, to really meet the new requirements of the ISO 26262 standard.

They may have to stand up new roles within the organization.

They may have to add new steps, perhaps validation steps, introduce the creation of new artifacts in the development process, and how is that going to work within the context of how they currently design and develop and deliver those products into their, I guess, end customer community.

But if a customer is completely new to safety relevant development, well, they really need to consider many different aspects like the organizational ones, the roles, responsibilities, process-related ones, verification validation and culturally.

The safety isn't just about enhanced documentation and auditability, it requires a certain culture. So, again, they would probably start out with a proof, a pilot project or proof of technology or some kind of proof point so they could see where they are now and what it's going to take to get them to be somewhere where they can be compliant with the new standard.

In either case, where somebody has a significant amount of process and infrastructure around the safety-oriented culture or someone that's coming into it new, IBM Rational can help them set up the right environment, allow them to quickly adopt what they already have to the ISO 26262 standard and related methodologies...

...getting them going quicker, the processes, the workflow, and to establish traceability between a large number of work artifacts and the assets that they're going to be producing.

So we're here to help our customers with qualifying our tools within their tool chain and development process as well.

MATHENY: Karla, thank you so much for sharing your time today. This is a great discussion, and we really appreciate it. That was Rational's Karla Ducharme, discussing achieving compliance with ISO 26262, how to manage functional safety and automotive EE development.

To share this podcast with your colleagues, or if you're interested in more podcasts like this one, check out the Rational Talks to You podcast page at [www.ibm.com/rational/podcasts](http://www.ibm.com/rational/podcasts).

And for your viewing pleasure, we'll post a link to our brochure titled, A New Approach to Automotive Electric

Electronic Engineering Lifecycle Management, Managing  
Engineering Data and Processes Using a Single Source of  
Truth. Be sure to check it out today. This has been an IBM  
podcast. I'm Angelique Matheny. Thanks for listening.  
Keep tuning in as Rational Talks to You.

IBM Podcast

[ MUSIC ] [END OF SEGMENT]