The New Automotive Security Standard 21434

Nitin Dahad, EE Times (00:04):

This is a Smarter World Podcast, focusing on the technology and issues behind today's connected world. I'm host, Nitin Dahad, Editor, EE Times and Embedded.com. In this episode, we'll discuss the new automotive security standard 21434, which is the automotive engineering cybersecurity standard. We'll be discussing that with an NXP's head of automotive security, Timo van Roermund. Timo, hello!

Timo van Roermund (00:31):

Hi Nitin.

Nitin Dahad, EE Times (00:32):

So Timo, what's been happening in automotive security? And how has it changed over the last few years?

Timo van Roermund (00:38):

Well, until a few years ago, vehicles had limited or no means to connect with the outside world. Although, maybe [inaudible 00:00:43] access, some audio streaming with mobile devices, or maybe communication with the manufacturer for emergency services. However, they were mostly isolated from the environment and the internet and as such, they were not really a target for attackers. But, that is changing rapidly. Modern vehicles are connected with various networks, think about cell and Wifi networks. They may communicate with other vehicle, to vehicle2X communication. And may also feature technologies like Bluetooth and NFC to connect to smart devices, like a smartphone. And all of this connectivity of course improves user experience. It enables search and it increase road safety. However, it also presents immense cybersecurity challenges. And that is because, the vehicle, as well as, the supporting infrastructure are repeating targets for hackers. These systems have both [inaudible 00:01:34] and valuable assets. And that is why cyber security is now really a must have for the auto industry.

Nitin Dahad, EE Times (01:41):

We've been quite familiar with the standards for things like automotive safety. You've got the ISO 26262, and then now, there's this new one for security. NXP, actually... it recently issued some news on this security standard called SAE 21434. First, can tell us what the standard is? And what does it cover?

Timo van Roermund (01:59):

Yeah, certainly. And let me, actually, first explain you a little bit about the regulation behind it. So, it's important to know that also a new regulation was developed. It's a regulation for

automotive cyber security, which is known as UNR 155. This regulation was developed by UNECE Work Package 79, more commonly known as the World Forum for Harmonization of Vehicle Regulations. And this new regulation, demands that automakers ensure that the entire auto supply chain is secure. It is the automaker's responsibility to manage, that all risks associated with contracted tier 1 and tier 2 suppliers and service providers. And this new regulation will be adopted in various regions, starting in Europe, Japan, and Korea. And these regions, by the way, represent more than a third of the global vehicle production.

Timo van Roermund (02:50):

Suppliers will need to support the vehicle manufacturers in this. And in particular, by supplying them with the appropriate information to demonstrate that supplier related risk are identified and managed. And exactly, that is where this new standard ISO/SAE 21434 comes into play. Because, this automotive cybersecurity engineering standards lays out clear organizational and procedural requirements throughout the entire vehicle life cycle. So, from concepts and development to production, to operations and maintenance, and finally the commissioning. And as such, the standard is very supportive in implementing the requirements of this regulation to organizations along the supply chain.

Nitin Dahad, EE Times (03:33):

You talked about UNR 155, but was that sort of initiated with some key players? Or how did that come about?

Timo van Roermund (03:39):

Yeah. So, efforts to create an automotive cybersecurity standard, actually, already began more or less five years ago in 2016. At that time, SAE International and ISO started the joint initiative to create an industry standard for automotive cybersecurity engineering. These two organizations had individually worked on automotive safety and security related standards in the past, but that was a first of a kind, that they joined forces.

Timo van Roermund (04:03):

And if you look at other data or ISO created in the past, ISO 26262 develop an automotive functional safety standards and SAE, okay... that's for example, J361, which is known as a Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. And then these two organizations ultimately joined efforts. They reached out to automakers, components and substations suppliers to all kinds of cyber security defenders, but also governing organizations. And in total, more than a hundred experts from over 82 companies in 60 countries were involved in this effort. So, it was really a massive effort and the result is the standard ISO/SAE 21434. And as I said, it provides a well-defined cybersecurity framework and it establishes cybersecurity as an integral element of engineering throughout the entire life cycle of a vehicle.

Nitin Dahad, EE Times (04:54):

Before we go on to whether it's for products or processes, could you explain to me, what does this secure by design actually mean? I know it's addressing the components, servers and processes, but what does that actually involved or is that going towards a certification, that it can't be attacked?

Timo van Roermund (05:09):

Yeah. So, security by design eventually means, that you really take security into account from the very first start. So not as an afterthought. So, if you basically only think about what to do in terms of securing a vehicle after, the fact is you're typically too late. And you can't have, let's say, sufficient coverage, there's a good chance that you overlook things. So, security by design essentially means, that you really start from the concept phase, or maybe you start specifying a system. What needs to be done, and then step by step, take the right decisions and implementations, and that's all the way until the end of life of a device.

Nitin Dahad, EE Times (05:42):

So that means, following some of the guidelines that have been issued in the US and Europe, by the standards organizations on secure by design.

Timo van Roermund (05:49):

Yeah, correct. And there have been many different frameworks and best practices guides. And essentially, what the standard does is, provides now, common baseline. And it basically, turns these best practices or many of those at least into a set of, let's say, clearly defined requirements.

Nitin Dahad, EE Times (06:04):

So, then, let's move on to 21434. Is this for products or processes? Let's just talk a little bit about where does this apply.

Timo van Roermund (06:12):

A very good question. That's a question, that's often asked. So, with the regulation standards, both... as I mentioned a few times, focused on cyber security engineering. So, what does it mean? Well, that they specify requirements on organizations, on policies and the processes. Actually, both the standards and regulation of technology agnostic... so they do not contain specific technical requirements on product and technology. But the other specify, what needs to be done if you designed systems for security.

Nitin Dahad, EE Times (06:41):

Why do you think this news is significant? How do you anticipate will change automotive security?

Timo van Roermund (06:46):

In the first place, it's very significant because this standard is, actually the first generic cybersecurity standards for the automotive market and industry. Because so far, it only had standards for specific automotive applications or security technologies, and actually most of the standards for also falls on the technical side of things. The second reason, to why there's a significant, is also because of the challenging timeline. Because, I didn't mention it yet, but Europe is planning to require compliance with regulation from July 2022 onwards. So next year.

Nitin Dahad, EE Times (07:18):

Oh, Okay.

Timo van Roermund (07:19):

And that means, basically, from that moment on, vehicle manufacturers need basically to comply with the regulation in order to gain [Motorscore's 00:07:27] type approval for new vehicle types. And two years later, actually also for existing ones. And the other regions that I mentioned, Japan and Korea, they plan to follow a similar timeline. And what's also important is that, this will indeed, definitely impose a significant change. Because, the introduction of this regulation standards, in the end, mean that the industry has to accelerate the shift from security... to obscurity to, indeed, security by design.

Nitin Dahad, EE Times (07:55):

Can I just ask you, you mentioned Europe, Japan and Korea. So what about all the other regions?

Timo van Roermund (07:59):

So, this regulation was developed at the United Nations level and any of the contacting parties of that group can adopt this regulation. And most likely, most of them will. And these contacting parties are various countries across the world and all of them have an vehicle type approval system in place. There are some notable exceptions and that's primarily the United States and Canada. Nonetheless, they are after the best. Also efforts ongoing to create a global technical regulation also at United Nation level. That is going to be, basically in fairly similar regulation. But in this case, not tied to vehicle type approval. And those regulations could then eventually also be adopted in the United States and Canada.

Nitin Dahad, EE Times (08:45):

This will change automotive security significantly, because at the moment it's all been about functional safety. So, what change do you see in automotive security now as a result of this?

Timo van Roermund (08:54):

Yeah. So, it basically means that, as I said before, the industry really has to accelerate. It shifts from security to security by design. That has started already before, but basically, there's no way

to avoid it anymore. So, what I really expect as a change is that, this movement is accelerating and also that, as much close of collaboration between supply chain parties.

Nitin Dahad, EE Times (09:16):

So, I think that leads us to the next question, who is impacted? You talked about everybody, but let's just explain that to our audience.

Timo van Roermund (09:22):

As I listed, the entire supply chain is impacted. So, the vehicle manufacturers, but also IATF volunteer to suppliers, service providers and whatever have you. So, the regulation itself may be applicable to vehicle manufacturers only. However, it does require them to provide evidence that supplier related risks are identified and managed. And that means, that collaboration with the supply chain. So that all suppliers is required. And via that, effectively, it does required towards the entire supply chain complies with this new standards ISO/SAE 21434.

Timo van Roermund (09:57):

And it's also interesting to share that the standard itself was only published fairly recently, actually on August 31st. However, we have seen first customer inquiries mentioning the regulation standards. Already more than a year ago, so... long before the standards and also the regulation were there. It's actually not surprising given the tight timeline. Because vehicle manufacturers are required to comply basically from summer next year onwards already. So, it's really a challenge to achieve that. And I would say that, most industry players are well aware of the challenge that are ahead. Although, there are of course, clearly, leaders that take a very proactive approach, but also follow us, that are little bit more reactive.

Nitin Dahad, EE Times (10:36):

Preempted my next question, which was... then, is well understood in the industry. It looks like, it is well understood in the industry.

Timo van Roermund (10:41):

Yeah, I know exactly. It is well understood, right? So that's what I said to you. See, that's clearly through the fact that we received his inquiries already, quite a long time ago. So, I don't think at this point of time as, anyone really doubting, if the standards has any significance, if they need to look at it, it just depends. Let's say, how far advanced the different suppliers and a manufacturer are in terms of accommodating that.

Nitin Dahad, EE Times (11:05):

Let's bring it to you now, as an NXP. NXP's been certified by TÜV-SUD. But, what does that mean for NXP now?

Timo van Roermund (11:12):

That's what ensures.. that means, that NXP is well prepared to address these upcoming challenges. So, what we've done is that we have leveraged our long-standing expertise in security, to also address the needs of the automotive industry. And what we've been doing in the last one and a half to two years is that, we've been updating our existing policies and processes. As we've refined them and extended them where needed to fully meet the requirements of this new standard. And to TÜV-SUD has actually validated that. So, TÜV-SUD is an independent external certification body. And they audited our organization of policies and processes. And after successful audit they certified NXP and via that, NXP has all positions to help tier one and OEM customers to meet the requirements of the regulation.

Nitin Dahad, EE Times (11:59):

That kind of implies that, if the whole supply chain needs to be certified or at least verified, then I think you're very much part of that supply chain. Now that certified to enable the manufacturers to obtain that certification.

Timo van Roermund (12:11):

Yeah, correct. And there's no requirements that suppliers are certified. And the alternative will be that customers are going to audit their suppliers individually. We believe it is in the end, much more efficient for everyone. If you do it as one source versus for a party. And basically everyone else can use that result and build.

Nitin Dahad, EE Times (12:30):

What's next in automotive security? We still hear about cars with a potential to be hacked. And I guess this will go a long way towards addressing that. But, what would you say is next? And what still needs to be addressed? And what's coming?

Timo van Roermund (12:42):

Well, there'll be challenges continuously, because it's important to realize that security is evolving, right? It's an evolving target. You always have to be able to get smarter for the new attacks are emerging, et cetera. But let me, maybe highlight, one specific technical challenge that I've seen rising and that is basically to address the threats imposed by quantum computers. Such quantum computing devices do exist today and the innovation is happening quickly. But, it does impose quite a threat to, for example, existing crypto algorithms.

Nitin Dahad, EE Times (13:12):

That you see, is the biggest threat for the future, is what you're saying or not even future. Now, I guess.

Timo van Roermund (13:19):

That's a good question on definitely... Let me put it this way, it's clear that there's a challenge that needs to be addressed. What exact timeline is, in terms of... and this might become a reality. They are... Your opinions are differing, but effectively what you need to realize is that if you would have, in general purpose, quantum computer with sufficient cubits, that you could basically solve the mathematically complex forms that are used, basically, in all public key crypto technologies today. So, that includes RJ analytical curve, cryptography. And in the end, it doesn't matter so much, if you believe whether these devices will come and what the timeline is. And that is basically, because the crypto standards... to what I said are coming. Competition for replacing cryptography standards, with new ones that are secure against attack was actually initiated by [NX 00:14:12] already five years ago. And this competition resulted in four finalists. And two of those were actually given to partnership with NXP.

Nitin Dahad, EE Times (14:20):

I think, that's a good point to end it on. Otherwise, we could go right into the challenges of automated security. Thank you, Timo.

Timo van Roermund (14:26):

My pleasure. Thanks for having me.

Nitin Dahad, EE Times (14:28):

This has been the Smarter World Podcast. With me, Nitin Dahad. Thanks for listening and see you next time.