The Safety Behind Connected Vehicles

John Quain (00:05):

Welcome to the Smarter World Podcast, focusing on the technology and issues behind today's connected world. I'm your guest host, John Quain [00:00:13]. In this episode, we're going to delve into the complex safety technologies that protect drivers in today's connected vehicles, and we'll explore some of the challenges at the forefront of this evolving field. Connected and increasingly autonomous vehicles offer those of us on the road a lot of benefits. But as the cars become more electronic, more like roiling computers, the role of safety becomes absolutely critical. How will a car respond when something goes wrong in its electronic system or in a single component? That's what safety seeks to anticipate and protect against.

(00:51):

To gain insight into vehicle safety, I'm joined by Gareth Price, functional safety manager at McLaren Applied, and Franck Galtié, director automotive functional safety at NXP Semiconductors. Welcome, gentlemen.

Gareth Price (01:06):

All right, hi.

Franck Galtié (01:06):

Hi, John.

John Quain (01:06):

Well, Gareth. Let me start with you. We all know about the things that make cars safe today like tire pressure monitoring systems and airbags and ABS brakes, and even some of the ADAS, or advanced driving assistance systems that are in cars like radar, obviously, and [inaudible 00:01:23] excommunication and blind spot detection. But what is the safety like in the world that you and Franck live in, and the world of functional safety?

Gareth Price (01:31):

So for me, it's really about risk. It's about quantifying the risk involved in the deployment of these new features that you mentioned. New and old features, and basically functional safety is, if you're in the business, it's a business of producing these automotive components or products that are free from unreasonable residual risk, is a term that we use to quantify what we mean by risk. As you said, that risk can be associated with anything from gearboxes to cruise control systems.

(02:05):

So we know there are inherent risks in the use of these items, these components, within a vehicle. We know that when they go wrong, there are hazards. There are hazards that put life at

risk. This is the risk we're talking about, not necessarily financial, but the risk of harm. We want to reduce that risk. As engineers, we admit that we're not going to be perfect and that we'll always be some risk left. We're never going to be able to design perfect systems that have no risk in them whatsoever. Driving by its nature is a very risky thing to do.

(02:44):

Lots of people die on the roads every year. I think 1.3 million is a number usually banded around. So people somehow take on that risk when they go about their daily business in their vehicles. But at the same time, they're not expecting the vehicles to fail unexpectedly. So when they use the brakes, they expect them to work. When they change gear, they expect it to work.

(03:10):

So in this business of developing systems like gearbox controllers, we need to rate the risks involved in the use of these products. Usually, the best way to do that is to use something that somebody's used before. This is where the International Standards Organization comes in and helps us out. So they've created this standard, ISO 26262 that focuses on things like random hardware failures and systematic failures within these components that I've been talking about. This standard gives us some guidance. It's not a legally binding document. It is just guidance. But it helps us to try and evaluate the risks of the use of these systems, and the detection and mitigation of these inherent hazards.

(04:05):

So it gives us some guidance. There are other standards as well. There's ISO/PAS 21448, which is commonly known as SOTIF, safety of the intended function. This is associated with more highly autonomous vehicles or ADAS systems, where it's not necessarily a random hardware failure that's going to cause some kind of hazard. But it's potentially the intended function, the actual feature that is being provided, that is inherently dangerous. Something like cruise control. If something goes wrong, you're either going to crash into the back of the car, or all of a sudden, it's going to brake if it's going strangely wrong.

(04:43):

So this SOTIF standard is there to try and formulate a way of, again, evaluating the risk involved in those kind of features, or the limitation of the performance of those kind of features. So we got two areas covered here. We got the deterministic land of hardware failures, systematic failures, and we've got this non-deterministic world of intended function, cruise control.

(05:07):

I usually use the analogy, cruise control, well, how can that go wrong as an intended function? Well, if you've developed the system badly, maybe the cruise control, the radar involved in it can't detect heavy snow, or doesn't know what to do with heavy snow. It may imagine it's an object and put the brakes on.

John Quain (05:26):

That's a good breakdown. People don't expect, as you said, the transmission to stop and the brakes to suddenly fail. Franck, maybe you can tell us a little bit of how that functional safety came to be and what the core of it was. I guess a lot of engineers used to tell me, "It's not like a computer where we have one chip. We have two or three. We build a lot of redundancy into that." Is that where all this started to happen?

Franck Galtié (05:50):

The beginning of the story was that we used to have cars which were mostly mechanical cars and not so much electronic inside. Then with the new features and also all the new features starting with the ABS was one of the first one where we said, "Oh great, electronics can really help and save lives." ABS, ESP, this kind of thing. So we had more and more electronic systems into the car. Then it was like ... In some of the design, we see up to 60, 70 ECUs here and there in the car. So it becomes very huge. This is, I think, the reason why we have seen, let's say, from the return from the field that there was more and more return from the field because of electronic failures, and because the electronic was supposed to, let's say, bring added value to the car and help you to be, I would say, either safer or drive in a more comfortable way.

(06:47):

This was actually bringing additional, let's say, failures or failures in the system and then sometime can become very dangerous. It's quite straightforward to understand that when we started to include electric power steering into a vehicle. Then it's great to have this very smooth assistance on the steering system with [inaudible 00:07:11]. But we can easily understand that if there is a failure somewhere and the motor is just starting to turn on the right, and unexpectedly it can become very dangerous if you are driving on the highway.

(07:23):

This is exactly the sense of this ISO 26262 as Gareth mentioned, is that it's really about this either systematic fault, which is the wrong design of the electronics. So you made the design. But then there are still some bugs inside. There's hardware on them for [inaudible 00:07:40], which is more like, "Okay, I did the good design. But unfortunately, the electronic is not perfect," and you can still have some kind of failures during the operation of the devices. So during the life cycle of the device, it can be a gate oxide breakdown or it can be any kind of short circuit between different lines of a microcontroller or of an IC or whatever in your electronic design. Then this can become really dramatic.

(08:06):

I think this is the reason why we have this new ISO 26262 standard which came up, I think it was 2010, 2011. The benefit of this standard is actually that we have a state-of-the-art. It's define actually a state-of-the-art which will be common to everybody. Everybody will design some with his own way and without any standardization, then who can we compare a design A with a design B? And how can we be sure that we can have a good level of confidence in the design?

(08:38):

Because at the end, this is what is needed. As a driver when I drive my car, I want to be sure that the features that I have in my car are not dangerous, but I can really trust them. So it's really a question of trust. As an electronic provider, NXP is a semiconductor manufacturer. Also we are tier two. We are part of the chain, and then we ... We need to prove that what we did, we did a good job. So we did everything which is as good as possible, based on the state-of-the-art. And at least this standard has the advantage to define the state-of-the-art.

(09:11):

What we should not forget as well is that at the end, as Gareth said, is that we want to save life. If there is an issue in that we are killing people because, as you said, we cannot be perfect. We know that perfection does not exist. Then at the end, we still have a residual risk. The risk is acceptable or not. But at the end when you kill somebody, even if it's still in the acceptable [inaudible 00:09:38], you kill somebody. Then everybody will try to understand why. So there is also a kind of liability, I would say, not issue, but at least a liability concern where you need to demonstrate that you did everything right. You have not made any kind of negligence or whatever during the design or during the validation of your product or that you have not hidden anything in the safety documentation that you are delivering to your customer or whatever.

John Quain (10:04):

You're absolutely right. You can reboot your smartphone or your laptop. But you can't reboot your car going 65 miles an hour, or 100 kilometers an hour down the road. That's not really an option. So maybe we could get to some sort of examples. Franck, you were talking about the individual chips in semiconductor and those components. But Gareth, you're also involved in the much more practical, most cars that most of us drive and the systems that go in it. You have to integrate this into a complete system. Maybe you could explain a brief example of the functional safety considerations when you do that and how that works.

Gareth Price (10:40):

As you can imagine, we start at the top with a vehicle and driver. That's in effect, our environment. That's what we're trying to argue about, where we're trying to find solutions to problems potentially. Usually, we're adding a feature to the vehicle. So something topical, an electric motor, for example. Lots of vehicles now are delivered with electric motors within them to provide economy. For McLaren cars, it's more providing performance and economy, depending on the mode of operation. These things are becoming very important. They're not novel technology. Electric motors have been around for a while. So the failure modes associated with them are understood. They fail. They stop driving. They stop providing this talk to the road service in some way.

(11:32):

So we start to analyze the object of our interest. So for example, if I'm making an electric motor, I'm going to analyze that electric motor and the inverter that's providing it with the energy in the context of the vehicle and I'm going to assume that it's going to go wrong in some way. Some of the worst hazards that you can have, I think Franck alluded to this earlier, the [inaudible

00:11:54] Effect. If you're traveling across the road into oncoming traffic, that's really dangerous. Although it's not so dangerous because the front of the car tends to be a crumple zone. Slide impacts tend to be very, very dangerous. So if you're coming across the road, you're presenting the side of the vehicle to oncoming traffic. So it's highly dangerous.

(12:15):

Therefore, we rate it as such. We say, "The risk associated with these [inaudible 00:12:19] hazards is high. Therefore, we've got to do a lot of work to ensure that these things don't happen." So we've analyzed the vehicle. We know these hazards occur with this electric motor. Then we start saying, "Okay, what are we going to do if the hazard occurs?" We don't try and work out the probability of it occurring. We just assume it is going to occur if it's physically possible. Then we start saying, "Well, what do we do? How do we detect it happening and what are we going to do to mitigate the hazards involved in the scenario that the vehicle is in?" That's when we come up with what we tend to call safety goals.

(12:54):

These are the top level requirements to ensure the safety. For example, with an electric motor, let's say it goes wrong. It creates a large braking force. Usually, they're regenerating energy back into the battery. So they do provide some braking effect. If that goes wild, you may create instabilities in the vehicle. So your safety goal may be written to avoid that. So you may say, "Okay, I want to prevent unintended deceleration." It's unintended because the driver doesn't expect it. There's been a failure. So then we've got our first requirement. That's what we're going to do. We're just going to try and prevent that unintended de acceleration.

(13:30):

Now unfortunately, one of the solutions would be to turn everything off. Well, you've still got to decelerate to force then because you're no longer driving. So a lot of the time, these mitigations and these safety goals actually only reduce the hazard. They don't necessarily get rid of it completely, especially if the hazard is very high. Once we've done that, we look at the system level. We go down in the software. It's a standard development process.

John Quain (13:55):

Is there specificity in some of the standards for situations like that? The reason I ask is adaptive cruise control. So when that was introduced, some cars would stop and you'd sit there for two seconds, and then they'd release the brake. And some cars stop and hold onto the brake. They hold the brake even when the system's disabled. Are the standards that specific for these systems?

Gareth Price (14:21):

For ISO 26262, ISO 21448, not really. They're really framing a development process and a description of the evidence that you must produce to provide some kind of assurance that the product that you have developed is free from unreasonable risk. Doesn't tell you what you need to do. Doesn't tell you the functionality. You need to argue over that. So something like adaptive

cruise control, yeah, it's very different from different manufacturers the way it reacts. In fact, I was in my car the other day and it's a relatively new car, and it doesn't have a handbrake. It has a button now that I can put on and off. I was just playing around with it, and accidentally put on the handbrake. The handbrake came on, and the car started to decelerate. I couldn't turn it off.

(15:12):

I was thinking, "Oh, if I turn it ... oh, it won't turn off. It's stuck." It continued to be engaged until the vehicle came to a stop, and then it disengaged. I thought to myself, "Somebody's planned that on purpose. That isn't something that's happened accidentally. Somebody has worked out that they think, with some evidence, that is the safest thing to do when the handbrake is applied during travel." So they're obviously measuring the speed and going, "Why would somebody want to put the handbrake on? They're not a rally driver. Why would somebody want to do that? They're obviously either in distress or there's a problem." Maybe the concept, the safety concept associated with that scenario is to continue to engage the handbrake.

(15:54):

So there was no failure there. Actually, there was a failure. It was me, which is usually the weakest link in this whole story. It's usually the driver doing something wrong, or reacting to a failure in such a way. We always say, "You really want these safety mechanisms to kick in before the driver realizes," because they are bound to overreact. It's just human nature. They'll overreact and make the situation even more hazardous. So you really want to get in there as soon as possible, or don't vary what you're doing. Don't turn the handbrake off and on and off and on, because that'll really scare somebody and they'll start to panic. Just do something as benign as possible. So you're searching out the benign.

(16:35):

As you said, different manufacturers have different ideas of what that is. Now there is some standardization coming in, especially now that more autonomous features are coming in that are highly complex, like Tesla's autopilot, like these adaptive cruise control, Highway Pilot, whatever you want to call them. I think these are trade names. How the driver actually understands the use of that feature, they're not going to read the manual. Nobody reads the manual. They just get in and they, "I can do this thing. I can use this function." They may not read the small print that says, "Actually, this is only usable really in these traffic situations. If you use it outside of those traffic situations, we can't detect that you're doing that, and actually that feature may not be safe."

(17:19):

People don't read things like that. They just get in and use them. So yeah, it's a minefield. I think there are efforts out there to come up with standardized use of these functions. But usually there's standardized testing methodology, so proving that the function doesn't fail very regularly, is robust in its design, rather than the use of it.

John Quain (17:41):

I want to return to that in a minute. But I also wanted to ask Franck about the components. We started out saying, "Well gee, when the electronics got really complicated years ago, they were responsible for more failures, which was the exact opposite of what we were trying to do." Now we take the chips for granted. We take radar for granted. We take the ECUs for granted. Knock on wood, but they rarely fail for me, and I test a lot of cars and hold onto cars for years. How did you get to that point in terms of the functional safety?

Franck Galtié (18:17):

So I think that's exactly what Gareth explained. On the system level, we do exactly the same at the semiconductor level. Gareth mentioned that the safety goals which already at the system level. So we are far from the safety goals when we develop a microcontroller or microprocessor. However, what we have to do is that we have to define what we call our top level safety requirements, and we have to assume some safety goals for sure, and then trying to understand what is the top level safety requirements that we can derive from those safety goals and that would be applicable to our own components, so microprocessor or sensor or IC, whatever component we are developing. So it becomes our own safety goal. So we don't call it safety goals, we just call it top level safety requirement.

(18:56):

Then similar approach then at system level, you analyze the functions that you have to realize with your device, and then analyze all the failures modes that you can encounter. and then you analyze all the failure modes that you can encounter. Then you look at all the failure modes and you try to tackle all the failure modes, so at least to detect and react on all the failure modes and/or mitigate the effect of the failure modes. So it's the similar approach than at system level. We are for sure getting more and more experience in the semiconductor industry about functional safety, and then in the automotive industry, the ISO 26262, as you may know, is actually coming from the IEC 61508, which is more like industrial standard.

(19:36):

In the IEC 61508, most of the constraints are really put at the system level. You can use any kind of semiconductor component. You can use any microcontroller or sensor or whatever to build your system as long as you manage the redundancy and the safety channels and safety functions at the system level.

(19:53):

For the automotive, this is quite different. Automotive is always trying to reach more integration level, and then cost reduction, as you know. Then having more and more features into the semiconductor, and then into system and chip, or very complex ICs. The ISO 26262 is actually pushing functional safety down to the component itself, which is not the case for the industry or domain.

(20:20):

This means that we, as a semiconductor company, we have to develop our component, and this is called safety element out of context. So it means that we don't develop one specific

component for one specific system. But we expect to have multiple customers. As you can imagine, we don't want to have only one customer and one system. We want to sell our microprocessor to everywhere, everybody in the world. We expect to use our microcontroller for steering system, [inaudible 00:20:46] system, or even if it's not exactly the same every time, we have some kind of microprocessor.

(20:51):

But then what we do is that we develop following this safety element out of context, and then we can ensure that we are analyzing all the failure modes of our devices, putting the right safety mechanisms and safety measures in place. We confirm with safety analysis that our architecture is actually safe. This is what we deliver to our customer, and this is what we can give a level of confidence and we can get the trust from our customer, and they can trust our development. They say, "Okay, we can use this device in our [inaudible 00:21:21] system, because we know that they have made all the analysis." So then they have given all the evidences.

John Quain (21:26):

Interesting. I assume, too, you have over-compensated in a way, because if it's going to be an automotive, that's probably the most reliable level that you can make, even though that chip may go into an e-Bike that's only going to go 28 kilometers an hour, and maybe into a tablet that it doesn't really matter if it fails once in a while, but that you have to really gauge for that automotive application.

Franck Galtié (21:49):

You're absolutely right. Indeed, we are imagine that we do over-design. But actually, you're right. We have a new way to target the highest AZ level, in the most critical system that we are targeting. So if we say that the same device will go in a motorbike, as you said, or will go in a McLaren car, then it's the same for us. We have to develop in the same way and we have to consider the IS constraints. What also impact us quite a lot with this nice safety element out of context is that we can develop without being in the context of an item, so really for a specific system. So we have some kind of a freedom.

(22:25):

But on the other side, as you said, we have to comply with the standard for multiple type of use cases, which will bring additional safety mechanism some time, over-design. The big risk is that, or the big challenge, is to really understand the system perfectly, because if we don't understand the system perfectly, we may introduce some safety measures in the device which will not be so useful at system level, because Gareth, for example, will implement some safety mechanisms at the system level which will actually not use our own embedded safety mechanisms. This is the challenge that we have in the semiconductor industry is to better understand the system so that we can design the right component with the right level of safety.

Gareth Price (23:05):

I think that's a challenge as well, because typically tier one and OEMs were expecting these high quality functionally safe products from NXP. I'm going to show them their system designs because it's their own IP that they've got and they don't want to share. So it's a bit strange for me when I go out and I'm selecting a microcontroller, I just expect it to be safe. It's not a unique selling point. I expect it to already be there with everything that I need. But I don't ever think of these emergent hazards that I think Franck is talking about, where the micro process or microcontroller manufacturer has no visibility of-

John Quain (23:42):

Right. We've come right away, actually, in a few years of just expecting that kind of reliability out of those components. That brings up the topic that is the sexy and also incredibly difficult one of the autonomous vehicles in getting from here to AVs that are actually level four, level five, whatever, what we all imagine. I'm guilty as charged of pushing those technologies. I test vehicles. I'm supposed to test them. I'm supposed to do that. But obviously, people are using features like autopilot and adaptive cruise control in situations where we're not technically supposed to. So maybe, Gareth, you could explain what some of the interrelated safety issues are right now with that.

Gareth Price (24:26):

It's a bit hot topic and a lot of money is being pumped into the autonomous space, tens of billions of dollars and pounds and yen. It's a big business. Some people are saying that we're doing this to save these 1.3 million lives on the road. I'm not convinced about that. I think that we'll save ... autonomous systems will save people because you're removing an unreliable person potentially from the situation. But there's a problem with the statistical information we have associated with autonomy. We know how many vehicle accidents are potentially caused by driver. But we don't know how many are avoided by the driver. So we only have a partial story or a partial problem space, and it's complex. It's not an autopilot on a plane, let's say. If you look out your window onto a busy street scene, it's a highly complex problem. If you look out of your window in different areas of the world, it's a different problem. It just looks completely different because our cultures are different.

(25:32):

The way we deal with organization and death and just living is very different across the world. And now we're trying to produce autonomous vehicles that can deal with that very complex problem space. So it is a big challenge. The industry knows this. We have the beginnings of some kind of standard to follow, the SOTIF standard, which gives some idea of how you would deal with autonomous functions. Maybe not full autonomy at the moment. It is in early stages of development. But it's going in the right direction, I think, in terms of how we should approach these problems.

(26:10):

They're not as deterministic as we're used to. We're used to looking at failures and just trying to prevent them by producing very highly reliable devices, or providing safety mechanisms to catch

when those devices fail. But now the problem space is different. Now it's about the unknown, what tends to be called the black swans. We don't know these issues exist until they exist. Again, this goes back to the engineer saying, "Well, there's an unknown element to the features that we're providing out into the environment." We should recognize that. We should recognize that actually the residual risk now becomes slightly unknown because we don't know how these systems are going to react under certain conditions.

(26:48):

So the new standards are much more focused on the verification and validation of these systems, these autonomous systems. There's lots of people struggling to find out how to do that. How do you know the unknown? It's a very difficult question to quantify. Lots of people are struggling over it. In fact, my experience looking around the industry, ISO are working at it, UNECE are working at it, IEEE, underwriter labs, the BSI. There's lots of people in this problem space trying to work out how do we know if these autonomous systems are safe enough?

(27:19):

Ultimately, we'll put them on the road, and less people will die, we hope. You don't really want to play with people's lives, though, do you? As an engineer, I have this ethical duty to say, "Actually, I believe based on this evidence that the thing that I'm deploying isn't going to kill more people than an average driver." I think that's the current level that we're going for."

John Quain (27:38):

Yes. It's certainly what we're after, obviously. That's the ultimate goal. Driving is fun. But it's also the safety issues, the thing that's been pushing everything. Coming back to front for a minute, there's so many other issues that come up now once you look at that. There's the security issues with having more of these systems and relying on them. There are the environmental safety issues. Is this vehicle going to have to react much more quickly, the systems have to be faster. Of course, Gareth just alluded to the AI issues, which I don't think are really solving the problems people thought they were going to solve, at least in autonomous vehicles. But maybe you could explain some of the complexity now that comes down to you and the semiconductors that it [inaudible 00:28:20] rely on.

Franck Galtié (28:21):

First of all, I have to admit that I really love autonomous driving. The reason why, it's really because this automotive industry became sexy. I joined this automotive industry in 2004 or something like this. I remember my colleagues at that time said, "Oh, why are you going there? It's so boring. It's just small improvement after another one, and then the future one is looking like the previous one. So very boring, boring industry," and so on. With this autonomous driving coming in the game, wow, it was very sexy. It's really given new dynamic into this industry and also completely changed the relationship and the way of working between OEMs, tier one, tier two, and so on and so forth.

(29:06):

Just to come back to what you said, John, as Gareth said, is that this autonomous driving is more and more going in the direction of how can we be as good as a driver, and how can we manage all the environmental conditions? So we have so many things, so many information, to analyze. Then this leads actually to more and more sensors here and there, more cameras and [inaudible 00:29:29] with 4K, 8K and something like this. 8 to 12 cameras, multiple radars, Lidars, and so on. So it's a huge amount of data, massive data, that you have to analyze. There is clearly an impact on the performance that we have to deliver at system level. This is the first thing.

(29:48):

One thing which is actually coming in the game is this artificial intelligence, as you mentioned. How can I manage a massive amount of data and analyze them quickly? Artificial intelligence seems to be the solution. Just it seems to be the solution because everybody said, "Yeah, great. Neural network is great. It's like a brain. So let's just use it, then it's going to be fine." But actually, it's not fine. At least from a safety perspective, we are not yet at the right level, I believe. So today, there are some kind of architecture tweak where you can say, "I will have a main channel doing all the massive computation with artificial intelligence, and to make it safe, I will do a safety envelope." Or somebody call it sometime ODD checker, so design domain checker. So it's going to be a safety pass, saying, "Okay, your main calculation is okay so I can drive the car on this part of the world because it's free from object," or something like this.

(30:44):

But what we see more and more is that even this second safety channel was supposed to be deterministic, because as Gareth said at the beginning, ISO likes determinism. So the things have to be deterministic. And artificial intelligent and neural network are maybe not the perfect definition of something deterministic. Then we said, "Let's use traditional algorithms and so on." But today, we see that this will not be sufficient, even in the safety channel, we'll have to manage also massive amount of data to take the right decision in to be as safe as a human driver.

(31:18):

This is why AI come into the game also in the safety channel. Then the big deal is how can I make it safe? Neural network are generally implemented in a big brain device, like multiples core microprocessor or whatever. And we have to find a way to make it safe, at least even from the ISO perspective, which is not the only problem that we have, because we can make it safe from a systematic full point of view, hardware [inaudible 00:31:43] full point of view. But we're going to have the problem about, "Does this training set the right one?" As Gareth said, is that it's okay as long as you train, versus something you know. But what about something you don't know? If you have not considered everything and the environment is changing a lot, depending on weather conditions or the country you are driving, and so on and so forth. So this is very difficult to manage this.

(32:07):

You mentioned also security, and I just want to give a word about the security, which is coming also most and more important than impacting also the safety of the vehicle. It's clearly one of

the reason why a vehicle may not be safe anymore is the vehicle is more and more connected to the cloud, and to the other vehicles and so on, to your smartphone and so on and so forth. So you have multiple attack surfaces where any hacker can actually modify or take the control of the car, and then endanger the driver and the people in the vehicle. So this is why safety and security are becoming more and more interdependent. There is a nice term, a nice word, from [AugMix 00:32:43] that I really like, actually. It's called cyber safety. I really like it, because it's what is the impact of security of a cyber attack on the safety of the vehicle.

John Quain (32:52):

Right. It's not the sexiest topic in the world, except when you have a problem, and then it becomes suddenly a point of attention. I've been one of those people that's had to reboot my car and close the door and turn it on and off just to reboot the system and do a safety update after it had been hacked. Coming back to that maybe, Gareth, you have to do the systems. That means that every chip, every component, has to be some how secure. Maybe you can explain what goes into those efforts.

Gareth Price (33:24):

You're right at identifying it as a system level problem. It's the whole vehicle that is at risk. In fact, with more highly autonomous systems and this unknown element, they're going to have to be updated in the field because we're going to learn new things about the way they operate and realize, "Oh, we've just spotted an unknown. We need to update." So in order to address these issues in a timely manner, we're going to have to have something like over the air updates. You're not going to be able to take everybody who's got a car, it's going to all of a sudden take them to a dealership to have them updated. That would just be unmanageable. You wouldn't be able to do that. Then you would have to work out, "Well, what if somebody doesn't update it and this unknown is still there?"

(34:04):

So it seems like we're going to have to be updating our vehicles regularly when we discover these unknowns. That immediately opens the door to a cybersecurity threat, and therefore, a safety threat. So what do we do? Well, let's have another standard. That's always a good thing. There are cybersecurity standards coming this way. I think ISO 21434 is out next year, 2021. It's aligned with 26262, so the V model outlined within that, the development cycle, within ISO26262 is sort of replicated. So you can see that you can do similar tasks, but with a slightly different focal point.

(34:46):

For the security stuff, you're probably going to be looking at attack factors. So you're assessing the threats, rather than the hazards. There's analogies in there where you come up with a functional security concept rather than a functional safety concept. So they're very much aligned. But again, it's early days. Cars are currently connected and there's been numerous examples of people hacking them. So it is a system design issue. But it's also, Franck was saying,

this sexy realm of cybersecurity. These hackers out there. It's very different from the gray world of functional safety and automotive domain.

(35:25):

These worlds are now merging into one where the automotive manufacturers must consider cybersecurity. In fact, in the new version of ISO 26262, calls it out in terms of, "You need to address it. It needs to be clearly communicated when you're developing these systems because they are dependent on each other." So failures of your cybersecurity design will ultimately affect the safety of your vehicle. Therefore, you need to consider it.

John Quain (35:51):

20 years ago, people told me, "Well, we'll never let them cross the canvas. We're not going to let people do that, and that's just not going to happen." Now here we are 20 years later, and that's just not a reality anymore. You have to have the interaction of these different systems and sensors seeing something, and triggering the brakes or triggering something else in the vehicle.

Gareth Price (36:13):

To know that the guy who was dealing with the CD player understands the guy who's dealing with the clutch control, they're in different worlds of automotive. So just to imagine that they would speak to each other, no, that's not going to happen naturally. You're going to have to put in place procedures, processes, structure, within your organization to deal with those now cross-company issues.

John Quain (36:37):

I'm more optimistic maybe than some people, because automotive designers do that already. If I change something in the interior of the car, that usually has to go to a different set of engineers down that hall that are doing something else with the face of the car. They're all so integrated already, that hopefully if there is a group of people that are able to do that, seems like this is an industry that should be able to do that. One paradoxical thing that you mentioned I wanted to bring up with Franck, and that is so you open up that connected car which is what we started with. Now you've made it so that you can upgrade the vehicle, but paradoxically, you've also added another attack vector into the situation by doing so. I wanted to ask, Franck, some of these chips used to be fixed function, they can't change. That's the perfection of them. But now, does that mean that more people designing systems and the OEMs want these chips to be upgradeable or changeable in firmware to account for unforeseeable things?

Franck Galtié (37:33):

Yes. The answer is yes. We have to move to a different balance between hardware and software into a chip. As a semiconductor company, we are generally defining everything for functional safety as hardware mechanisms. So it's good from one perspective, is that it's quite fast generally. Then this is very well deterministic, but it's not flexible at all. Right now, we need to

do this. So it has to be very well adapted to the system. This is one thing. Then since we want to be flexible across multiple systems, then it would be good to have a different solution which is more flexible. The point that you mentioned is, I think, the key one is that over the air update, it's going to not be just about cybersecurity, I think.

(38:14):

I do believe that with everything connected to the cloud, you will very much analyze all the information, all the diagnostic and the feedback from the vehicle that would be given to the cloud and the OEMs will analyze it and they will be able to anticipate any risk in term of safety. It's not about security attack or whatever. Just like, "Oh, my functional safety concept. I was foreseeing this. And finally, based on the feedback, based on the data, that are provided to the cloud, I see that maybe my safety concept is not robust enough. So I would have to update also my safety concept on the fly." In that case, if you have a hardware safety concept, then you cannot update. So we have to move more from hardware based safety concept to a more software based safety concept.

(38:58):

This is actually the direction that we are taking at least in NXP is that we are thinking more and more about some software safety concept and software features that can help us to get rid of this fixed hardware solution.

Gareth Price (39:10):

I can see the OEMs are doing the same thing. They're realizing that they need far more software engineers than they'd ever predicted. To de-risk their business, it's not necessarily a safety risk, although it is connected. But if you have to recall millions of vehicles, that's going to really affect your company's profitability, whereas if you can update them, keep them at this optimal safe level remotely, that just makes a lot more sense. It's more profitable. People are safer, and you could potentially [inaudible 00:39:38] it by adding features. You can have the crazy insane mode if you pay your $1000 and press this button, and all of a sudden, it appears in your car.

John Quain (39:48):

I wanted to ask one more thing, because I'm curious about the systems, Gareth. One engineer was saying, "Look, I can see a way to fix the transmission issues that we have through software and I can change that. But I can't just download that to the car, because I don't know the rest of the power train torque front to rear issues are, what the wear and tear issues are. The car's supposed to go 150,000 miles without any kind of service there if I change these." How do you integrate that with the people that make the chips, all the way to the OEM?

Gareth Price (40:19):

For those kind of in field updates, I think to try and second guess how the vehicle's going to react is going to be very difficult. I'd imagine if you were deploying those systems, you would simulate as much as you could. You would get your vehicles on test tracks. You would have

some kind of confidence. It would be in your processes that you've got this level of confidence that what you are deploying is safe. The proof would be in the pudding, though. People are doing it now. Cars can be updated over the cellular network, and they are. We haven't seen any problems yet. So it seems like currently it's working. But we are expanding the problem space by adding more features and having more vehicles doing this, like I've got a vehicle now, it doesn't update over the air. I think you'd have to buy potentially a high end vehicle for that to be the case.

John Quain (41:06):

I think that's a great discussion to give people a great sense of the functional safety and the issues involved. Thanks again to Gareth and Franck for joining us in talking about functional safety. Thanks for joining me. My name's John Quain. Join us next time on the Smarter World Podcast.