The difference between functional safety and cyber security is "calculated risk"

Karamba Security COO Amir Einav explains how functional safety works alongside cyber security in the connected car. By Elle Farrell-Kingsley

Cyber security is an increasingly important consideration for electric vehicles (EVs). It is closely intertwined with functional safety yet merits its own standard. ISO 21434, which addresses cyber security features, took a note from ISO 26262, which focuses on functional safety.

For ISO 21434, "anything safety is relevant. It must be addressed in the threat analysis, mitigations and verifications to become ISO verified," says Amir Einav, Chief Operating Officer at Karamba Security. Karamba Security is a cyber security company specialising in securing connected devices.

Continual safety and security

Breaking down the relationship of the ISOs, the concept of continual security (ISO 21434) was taken from functional safety (ISO 26262). "When you are introducing continuous security, you are touching the heart of the difference between cyber and functional safety," Einav tells *Automotive World*.

The distinction between the two, he says, is that "continuous functional safety focuses on monitoring, measuring and witnessing incidents and statistics, and then fixing them. Comparatively, in continuous security, there's the same concept of monitoring. If you have an issue, you can perform an update of your software, requiring a continual view of the vulnerabilities."

When it comes to cars, "the difference between functional safety and cyber security is calculated risk," Einav explains. "Functional safety is a statistical exercise. There is a certain amount of risk associated with this world, and risk can only be mitigated by calculating it correctly," requiring accuracy to four points after the decimal.

For example, Einav suggested that if a safety calculation was proved wrong following a car's release, the event's statistics might increase from one out of five million to one out of two million. This would mean new calculations would have to occur as there's new data.

Charging represents an additional cyber attack vector with EVs

Cyber security, however, is more complex, as it is not just physics and nature analysed as threats, but people. “Continuous security in cyber means that you’re still going to have to manage the software in the car years down the road. It’s not like the one year into functional safety when we see the real statistics, and there’s the potential we made a mistake as nature will change.”

Connected cars

Many consumers have expressed concerns about adopting EVs due to the threat of hacking. In reality, any connected car is at risk of being hacked, including an internal combustion engine (ICE). Einav adds, “It’s interesting that regular consumers look at the EV as the issue with security when it is the connected car that has to do with security.”

Connectivity is the first layer of threat, he explains. Any device connected to the internet is considered connected. Smart fridges, clocks, printers and watches are connected too, but there’s no current standard regulation. Yet cars cannot be road-ready without passing additional cyber security and functional safety regulations, offering connected cars a greater layer of protection compared to other household connected devices.

> Continuous security for them is natural; gadgets such as your phone are continuously updated. So, for them, having a continuous support model for the software is the way to go

The threat of cyber attacks

EVs do, however, have an additional attack vector–charging stations. There are software discussions between the charging station and the vehicle as they exchange data, which is the key and allows a hacker to perform a cyber attack. Einav acknowledged that many fear the direct safety risks of potential cyber attacks. However, he believes there is little threat to consumer safety, considering ransomware threats are more prominent. "If there is a way for a hacker to utilise someone's safety concern, they will typically try to benefit from ransomware instead."

He revealed one example of a cyber attack where a manufacturer had its entire fleet stolen, noting, "The current cyber style is to take away the car, rather than physically harm the driver."

Karamba works with companies, such as charging stations, that apply the same cyber security standards as vehicles due to these security and safety concerns. Interestingly, it isn't an enforced regulation. Instead, companies are choosing to do this as they connect to this automotive world: "It's friendly and provides common grounds to say I'm ISO certified".

Cyber security ecosystem

Einav mentions that as many new players are entering the automotive industry, with connected innovations extending to micromobility and artificial intelligence (AI), "they will also need to follow the cyber rules because regulation is for everybody. The ISO is very clear because it allows everybody to ensure that cyber security is at the forefront of functional safety."

Similarly, with more tech companies, such as Ericsson, Google and Apple, entering the original equipment manufacturer (OEM) industry, there's the potential for these regulations to evolve as tech companies approach connectivity and the connected car differently. "When the big tech companies enter the industry, they refer to ISO standards as the lowest requirement. Meanwhile, an automotive company might meet the standard and leave it there."

Tech companies may look to innovate and develop their business beyond standard ISO regulations, which could impact the connected car further. "Continuous security for them is natural; gadgets such as your phone are continuously updated. So, for them, having a continuous support model for the software is the way to go."

Ultimately, ISO 2626's functional safety and ISO 21434's cyber security work harmoniously and offer a level of protection to the connected car. Continuous safety has already been blended with continuous security–as one develops, the other grows. As Amir notes, "A safety component is just another software component."