NATIONAL CENTER FOR MANUFACTURING SCIENCES

Accelerating Cybersecurity for Software-Defined Vehicles

Overview

The use of computerized controls in automobiles has greatly expanded in recent years. Current estimates put the number of microchips in the average car at 1,000 to 3,000. Modern software-defined vehicles provide an impressive array of capabilities, including driver assistance features such as automatic emergency braking, blind spot warning, and lane-keeping assistance; connectivity solutions that provide up-to-date information about vehicle performance; infotainment systems that pair with smartphone integration systems to deliver information and entertainment via touchscreen displays; and the capacity for over-the-air (OTA) updates of new features and functionality.

While vehicle connectivity has major benefits, it also makes vehicles vulnerable to cybersecurity threats that can affect driver and passenger safety. The 2021 Global Automotive Consumer Study from Deloitte found that 64% of Americans have concerns about automotive cybersecurity risks. These concerns are well-founded: in December 2022, a Sirius XM radio connected vehicle service exposed more than 12 million cars in North America to remote hackers due to a security vulnerability that could have enabled hackers to remotely locate, unlock, start, flash the lights, and honk the horn on cars. Fortunately, the company patched the vulnerability within 24 hours, but the threat of cyberattacks on software-defined vehicles remains high.

Modern software-defined vehicles contain five linked, layered subsystems (See Figure 1):

(1) the safety and time-critical subsystem (powertrain components), which directly impact vehicle and passenger safety including brakes, throttle, steering, ignition, protection/defense, and the advanced driver assistant system computer and sensors;

(2) sensors and vehicle-to-vehicle (V2V) communication, which provide major inputs to the safety critical subsystem;

(3) operational and vehicle-to-everything (V2X) communication, which includes general and non-critical safety subsystems;

• • •

"An important step in developing cybersecurity systems involves putting them through a threat and risk analysis (TARA)."

• • •

(4) business-related processes, which pertain to telematics and fleet management systems (FMS);

(5) user-experience components, which include infotainment, applications, and communications.

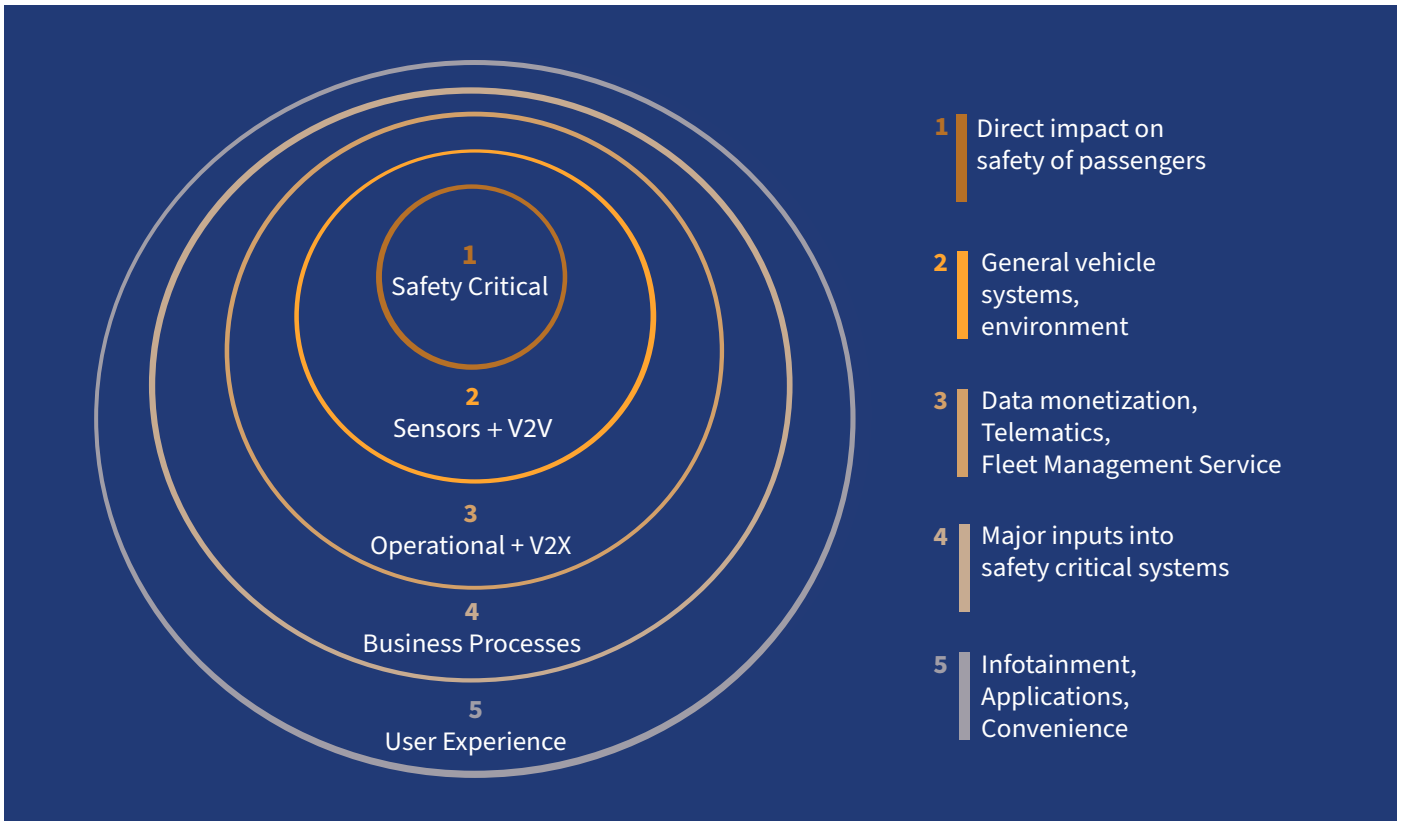

Figure 1. E/E Architecture Multi-Layer Asset Model

Today's top-of-the-line vehicles have up to 150 million lines of software code, distributed among as many as 100 electronic control units (ECUs), along with sensors, cameras, radar, and light detection and ranging (LIDAR) devices. Each vehicle exists in a connected ecosystem and acts as a virtual local area network (LAN) with numerous endpoints (e.g., every onboard connected ECU and many smart sensors), which are all subject to cyberattacks. Therefore, manufacturers must implement cybersecurity mechanisms that are vehicle-specific and even more extensive than those used for IT platforms.

If a vehicle's computer systems are not properly protected, hackers can tap into weaknesses through OTA software updates, enabling them to take control of vehicles from anywhere in the world. Cybercriminals could also unleash malware that could infect individual vehicles, or even entire fleets, by falsifying performance and maintenance data to cause undetectable wear and tear on vehicle components, leading to expensive repairs and irreversible damage. Part failures could cause accidents, damage property, and injure or kill vehicle occupants.

In fact, vehicle cybersecurity can have an even greater impact. It is critical to preventing disruptions in the supply chain and transportation systems that could put Americans, the industrial base, and forward-deployed weapons at risk of attack and exploitation.

A New Approach to Vehicle Cybersecurity

NCMS is working to advance the cybersecurity and safety of next-generation, software-defined vehicles. A recent collaboration between the Army, GuardKnox Cyber Technologies, and Synergistic employed state-of-the-art hardware and software tech-

nologies to prevent cyberattacks. Using the Army's next-generation combat vehicle as a surrogate to industry, this work has demonstrated how advanced cybersecurity methods can be applied to the vast network of sensors and vehicle computer systems for individual vehicles and across entire fleets. The goal was to create a modular open systems approach (MOSA)/service-oriented architecture (SOA)-based cybersecurity solution designed to preserve the safety of vehicles, drivers, and passengers.

Designing cybersecurity for software-defined vehicles presents several challenges, due to the need to protect vehicle reliability as well as end-user safety, security, and privacy. In addition, allowing OTA updates is essential, since these vehicles require continual feature updates in real time. To balance these demands, the research team investigated next-generation hardware, software, and electrical/electronic (E/E) network technologies.

Designing Next-Generation Cybersecurity Architecture

A comprehensive and layered approach to vehicle cybersecurity must not only reduce the possibility of a successful vehicle cyberattack, but also mitigate the potential consequences of a successful intrusion. This design includes such components as the GuardKnox SOA software stack, Comm Engine, and Lockdown Core security methodology. More important, secure-by-design architecture is utilized, which means that all required security solutions to address complete threat mitigation of the system are designed from the beginning rather than "bolted on" later. The security design itself does not rely on continuous cloud connectivity for ongoing updates, therefore eliminating one route of entry for attackers.

The resulting design includes high-level software and hardware architecture, along with a design for separating hardware from software. Although it is not possible to fully separate hardware from software in mixed criticality environments, there are approaches that can cover most use cases. This design ensures that applications that communicate with one another may reside on a different chip in a different ECU and need not even be aware of the physical location of the remote applications with which they exchange information.

The high-level architecture for hardware and software centers on a secure gateway/common compute module, which acts as the network backbone, connecting, segmenting, and orchestrating all cross-domain communications. The design supports advanced vehicle architectures that mix new Ethernet backbone technology with legacy controller area network (CAN) systems. It enables a mixed-criticality environment, allowing both critical and non-critical applications to run on the same hardware/system-on-chip (SoC). The security architecture uses programmable logic to achieve hardware-level separation between all physical interfaces. This leads to a dedicated communication path for each one prior to reaching any software.

By providing hardware-level separation, attacks such as denial of service (DoS) cannot spread to or even reach the software, thus affecting at most a single interface, or in most cases being stopped altogether. The system detects and prevents the injection and spread of malicious messages between the various computers/ECUs. All incoming messages are inspected, and only approved/legal messages are allowed through. All cyberattack attempts can be logged and reported to a security operations center (SOC) for further technical and statistical analysis. Therefore, all known and unknown threats are stopped in real time.

Threat and Risk Analysis (TARA)

An important step in developing cybersecurity systems involves putting them through a threat and risk analysis (TARA). This process defines, identifies, and classifies data assets in the system; determines ground rules and assumptions; defines relevant threat actors and classes of risk; analyzes the threat, potential impact, and likelihood of occurrence to determine the overall risk; and defines a risk mitigation strategy and mitigation solutions.

The process applies governing compliance standards and protocols, which in this case included the three pillars of the Cyber Survivability Endorsement Implementation Guide (CSEIG)—prevention, mitigation, and recovery—and the NIST SP 800-53 risk management framework. These frameworks facilitate security mitigation mechanisms related to high-level system and software architecture assets. As a result, a cross-correlation matrix was developed to show the appropriate threat mitigation solutions that can be used to address key system threats.

Some key takeaways for the automotive industry gained from the TARA include:

- Manufacturers must ensure that each new hardware, software, and firmware component is formally documented and certified as safe for the vehicle driver and passengers.
- OEMs' and Tier 1 suppliers' product-qualification procedures must be extended to all cybersecurity components to prevent rogue hardware, software, and firmware from creeping into the supply chain via the production line and at maintenance sites.
- All downloads of new versions of software and firmware must be performed using encrypted object-code images signed with electronic signatures that can be verified against the data in the OEM depository.

About NCMS

The National Center for Manufacturing Sciences (NCMS) is a cross-industry technology development consortium, dedicated to improving the competitiveness and strength of the U.S. industrial base. As a member-based organization, it leverages its network of industry, government, and academia partners to develop, demonstrate, and transition innovative technologies efficiently, with less risk and lower cost.

NCMS enables world-class member companies to work effectively with other members on new opportunities – bringing together highly capable companies with providers and end users who need their innovations and technology solutions. NCMS members benefit from an accelerated progression of idea creation through execution.