SIEMENS
Ingenuity for life

Siemens Digital Industries Software

Strategies to secure connected cars with firewalls

Executive summary

Vehicle network security requirements are becoming more stringent as vehicle systems face hostile adversaries through a variety of entry points. White-hat hackers have demonstrated gaining remote access to dashboard functions and transmissions of connected vehicles. In response to the posed threats, governments around the globe are legislating liabilities for self-driving vehicles (the U.S. SELF DRIVE act of 2017 is an example). That makes a firewall a vital component of a multilayered approach to vehicle security as well as overall vehicle safety and reliability.

Dr. Ahmed Majeed Khan
Senior Development Engineering Manager
Mentor, A Siemens business

Contents

Automotive software security threats

Cars are equipped with more software than the most sophisticated machines of our time. In a 2009-10 publication, *IEEE Spectrum* reported that the U.S. Air Force frontline jet fighter, the F-22 Raptor, included 1.7 million lines of software code. The F-35 Joint Strike fighter had 5.7 million lines of code and the Boeing 787 Dreamliner contained 6.5 million lines of code. At that time an average car was equipped with more than 10 million lines of code. Premium brands like the Mercedes Benz S-Class were equipped with more than 20 million lines of code. Today, Ford's F-150 truck is equipped with 150 million lines of code. [1,2,3]

With the megatrends of connectivity, electrification and autonomous driving, automotive software content has become even more relevant. Software complexity and connectivity increase the vulnerability of automobiles to security threats, and real-world examples are well documented. The deep hackers Charlie Miller and Chris Valasek remotely accessed a Jeep Cherokee and were able not only to control its transmission but also gained access to other functions including the windshield wipers; the automobile eventually crashed.[4] Chrysler was forced to recall 1.4 million Jeeps after the incident. Within a year the same hackers gained control of another Jeep through the on-board diagnostics (OBD) port of a controller area network (CAN) and were able to control the braking and steering systems.

In 2015, a security researcher demonstrated an attack on GM's OnStar RemoteLink system with an inexpensive homemade device that enabled him to track the vehicle, unlock it, trigger the horn and alarm and start its engine.[5] In 2018, a Tesla Model S was stolen in seconds by hackers who exploited an encryption weakness and cloned its key fob.[6] No automobile brand is safe from black-hat cyberattacks in an era in which there are freely available car hacking handbooks on the internet and open-source, low-cost hacking tools like Wireshark and ChipWhisperer.

Upstream Security provides data in its *Global Automotive Cybersecurity Report 2019* [7] that indicates that the number of successful black-hat cyberattacks is growing. From 2010 to 2018, there was a six-times increase, and the cyberattacks came from a diverse set of entry points including the OBD port, OEM applications and through remote access. The increased number and effectiveness of cyberattacks has increased the urgency for developing security solutions. An unprecedented level of government intervention is resulting in regulations to prevent cyberattacks.

Automotive cybersecurity regulations

The U.S. Security and Privacy in Your Car (SPY Car) Act of 2017 is intended to protect consumers from security and privacy threats to their motor vehicles. The bill directs the National Highway Traffic Safety Administration (NHTSA) to issue cybersecurity regulations for vehicle manufacturers. These regulations require vehicles for sale in the U.S. to provide protection against unauthorized access to electronic controls or driving data, including information about a vehicle's location, speed, owner, driver or passengers. The bill also prevents access to driving data collected by the electronic systems, whether it is stored onboard the vehicle or collected and transmitted to the cloud.

The SPY Car Act also mandates that automobile manufacturers provide cybersecurity labels for all vehicles to inform consumers about the extent to which the vehicle provides cybersecurity and privacy protection. The labeling must be in a standardized dashboard form that is easy to understand.

The Safely Ensuring Lives, Future Deployment and Research In Vehicle Evolution (SELF DRIVE) Act of 2017 goes a step further. The SELF DRIVE Act makes it illegal for OEMs to sell, import or exhibit even partially automated vehicles without a cybersecurity plan. The plan must include intrusion detection and prevention and incident responses.

Because the average life of a vehicle is about 10 years, today's state-of-the-art cybersecurity will become obsolete over the life of the car, and any plan that is based only on prevention mechanisms is destined to fail. OEMs will need good detection mechanisms to identify, report and respond to incidents, and to improve cybersecurity plans. The SELF DRIVE Act also requires OEMs to assign persons responsible for automotive cybersecurity.

Basics of automotive network security

The NHTSA has an automotive cybersecurity research program based on the threat analysis approach. The program has a threat model that identifies the conditions that need to be in place for a potential attack to make an impact. The model groups threats into categories such that mitigations can be developed for specific groups of threats. NHTSA's model is a combination of three modeling methods. It uses Microsoft's STRIDE, ASF and Open Web Application Security Project's Trike as a baseline. The threat types in the NHTSA threat model are borrowed from Microsoft's STRIDE:

Spoofing identity. In identity spoofing threats, an application or program can masquerade as another and gain advantages that are not typically allowed for that program.

Tampering with data. Data tampering involves the malicious modification of data, including making unauthorized changes to a database and alteration of data as it flows between computers.

Repudiation. An example of repudiation is a user or program that can refuse the authenticity of something good or reasonable.

Information disclosure. Information disclosure threats involve the exposure of information to individuals who are not authorized access to it. For example, users have the ability to read a file that they were not granted access to, or an intruder can read data in transit between computers.

Denial of service. These attacks deny service to valid users. An example is making a website unavailable or unusable by flooding it with illegitimate requests so that the legitimate users cannot be serviced.

Elevation of privilege. An unprivileged user gains privileged access, for example by changing group membership, and can compromise or destroy the system.

Attack surfaces

Cyberattacks on cars begin with hackers finding a way inside the car – defining the attack surface. The next step is compromising an electronic control unit (ECU). A third element is finding a control feature that can be exploited and compromised to gain access to certain functions.

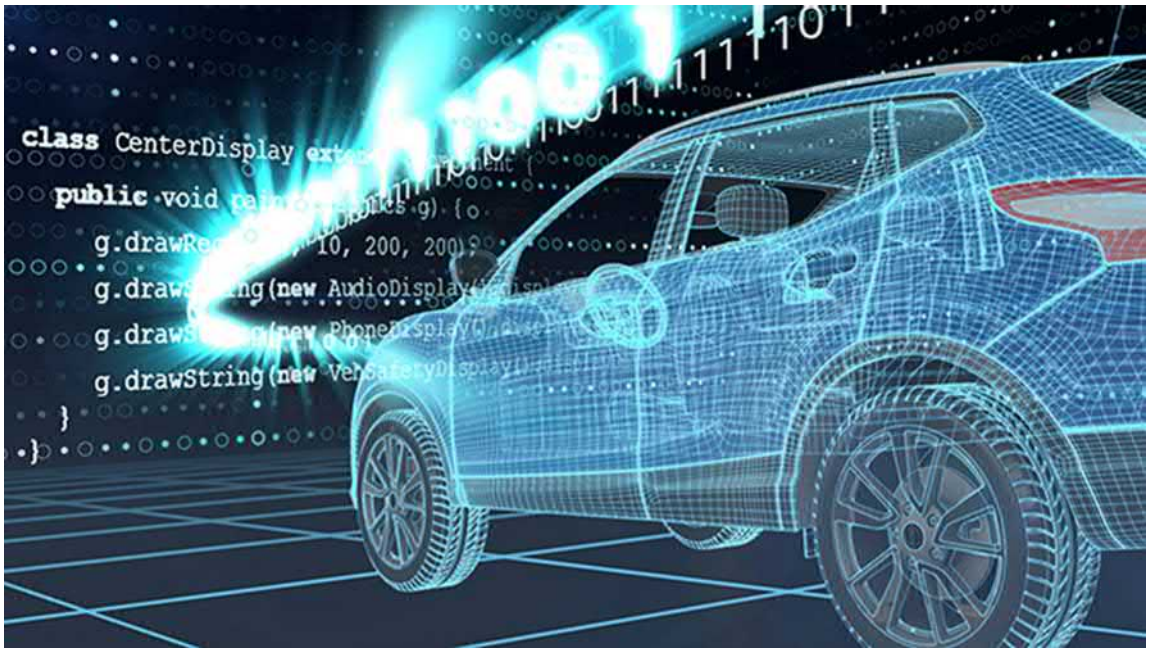
Attack surfaces of cars can be divided into four categories:

Direct physical. Direct physical attacks can be conducted using the harness connectors, the OBD or charging ports or the vehicle network. Manufacturers and consumers must realize that cars operate in hostile environments. Owners can loan cars to others and give up possession for repairs or maintenance; in each instance hackers can gain direct physical access inside the car.

Indirect physical. In indirect physical attacks, a carrier introduces a malware threat in the form of a CD, SD card, USB device or firmware update that becomes a Trojan horse inside the car.

Wireless. Short-range wireless includes Wi-Fi, Bluetooth, near-field communication (NFC) and radio frequency (RF). Cars in the connected and autonomous worlds will be equipped with all these technologies that increase the attack surface of the car.

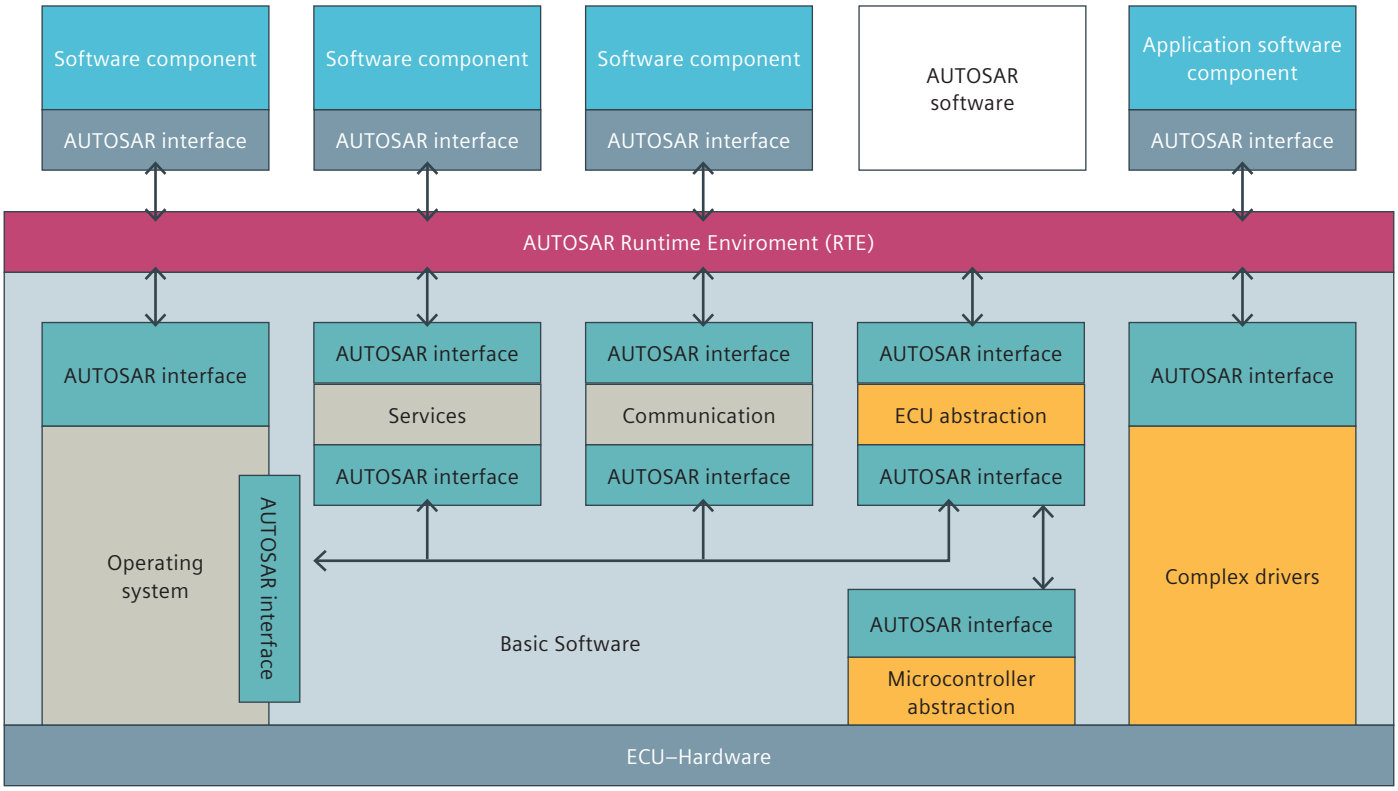
Sensor fooling. Although there is little news or research indicating that sensors are being controlled by hackers to create a cyberattack, sensors certainly provide a potential attack surface. The potential culprit of the Boeing 737 MAX disasters was a sensor that was emitting illegitimate data and causing the logic to behave incorrectly, leading to the unfortunate crashes. Sensor data can potentially be manipulated to produce inaccurate data, opening another attack surface to hackers.



Automotive Open System Architecture (AUTOSAR)

Before discussing security, it is useful to examine the Automotive Open System Architecture (AUTOSAR). AUTOSAR is a worldwide development partnership of automotive interested parties founded in 2003. It pursues the objective of creating and establishing an open and standardized software architecture for automotive electronic control units. The goals of AUTOSAR include scalability, maintainability and transferability aspects for software between platform variants and across programs.

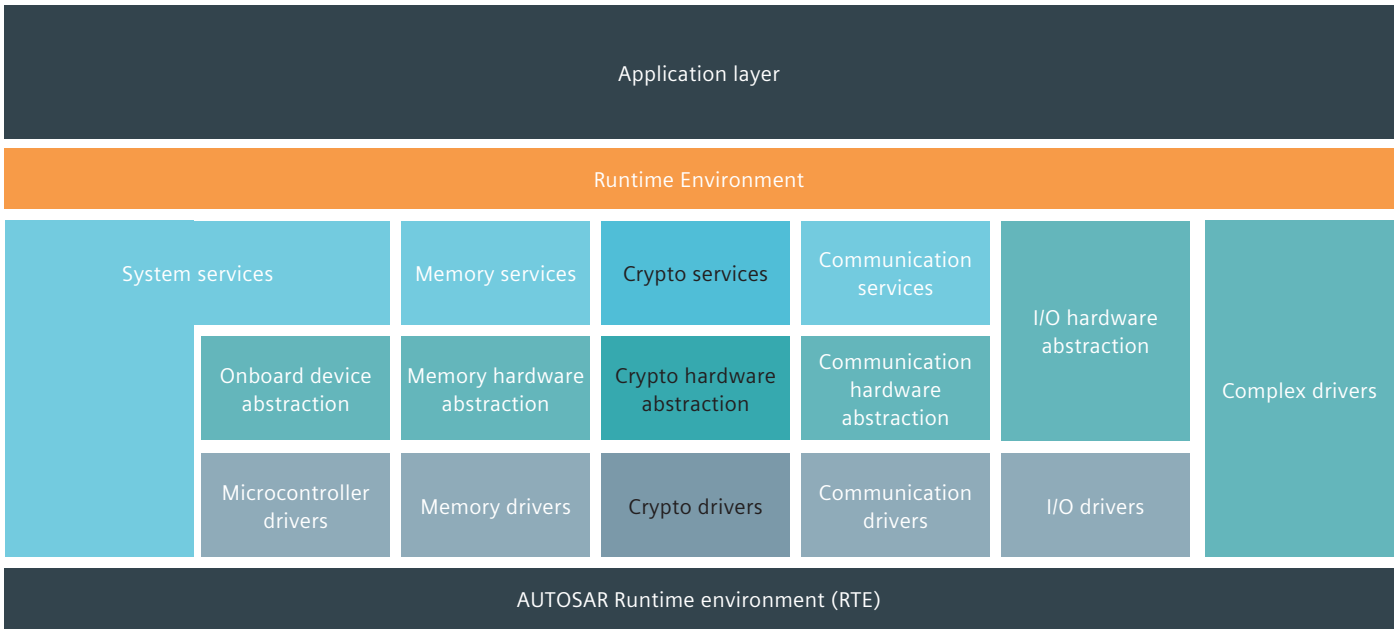
As depicted in the illustration, at the top layer are application software components that interface with the runtime environment through standardized interfaces. The runtime environment interfaces with the software modules, which could be services or communications. Similarly, the software interacts with the underlying hardware through standardized interfaces. The AUTOSAR partnership has a management level or working structure, and on the technical level where the specifications are being worked out, the governing bodies are called working groups, which are responsible for the specifications that are released.



AUTOSAR layered architecture

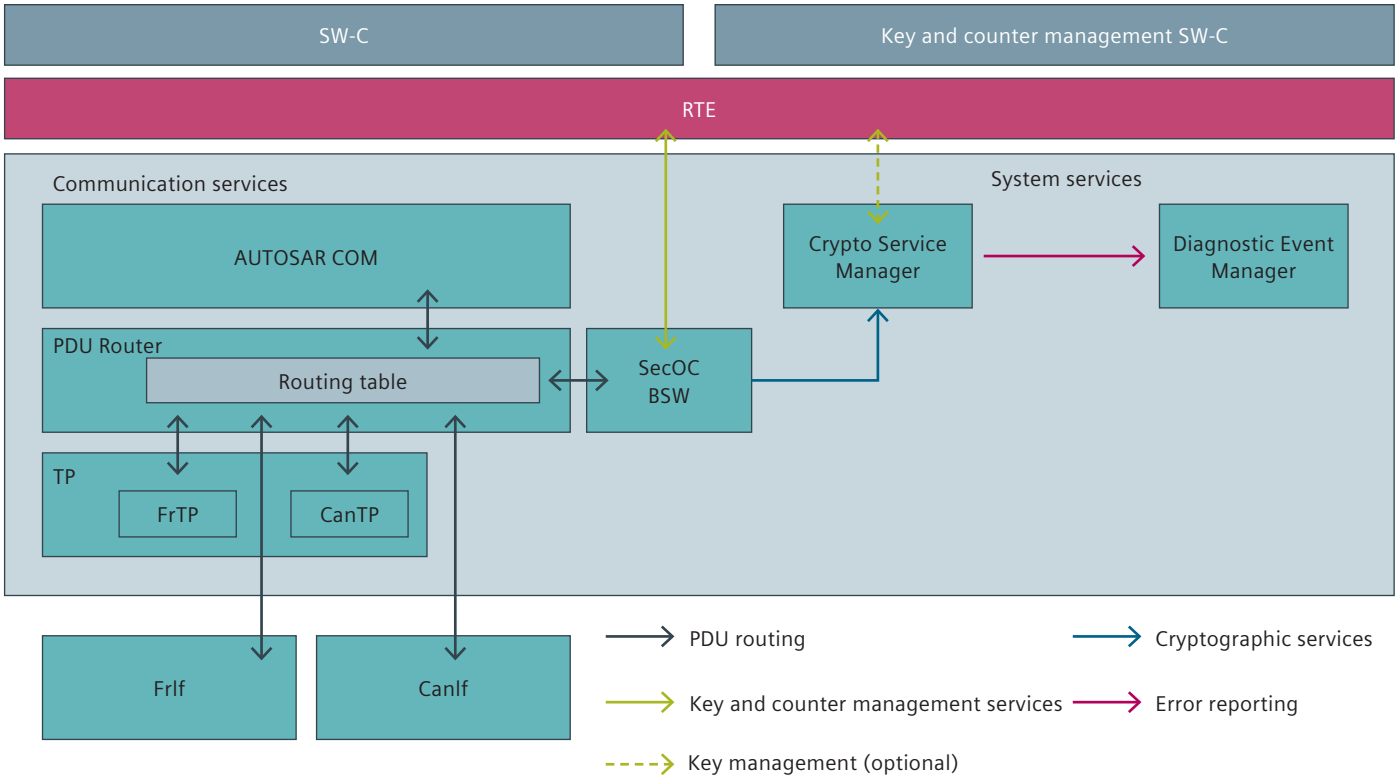
The working group for security, WG-SEC, is in charge of security aspects in the consortium. The security working group was formed in November 2014 with a mission to improve and extend security measures into AUTOSAR and take a holistic approach on a secure, heterogeneous automotive software architecture. AUTOSAR was founded in 2003, but the security working group was not formed until late 2014, when the consortium realized that a separate group working on security was needed.

AUTOSAR has a crypto technology specification. At the hardware abstraction layer, there are crypto interface modules, and then at the service layer the specification includes a Crypto Services Manager. The crypto specification does not provide a security concept; it offers cryptographic services that can be used to support and realize a security concept.



AUTOSAR crypto services (*Source: AUTOSAR*)

In AUTOSAR, the transmission units are protocol data units (PDUs) and the gateway that allows these PDUs is called the PDU Router (PduR). The way AUTOSAR secure communication works is with integration at the level of the PduR. As shown in the illustration, the PduR is responsible for routing incoming and outgoing security-related information PDUs (IPDUs) to the SecOC module. The SecOC then adds or processes the security-relevant information and propagates the results in the form of an IPDU back to the PduR. The PduR is then responsible for routing the IPDUs to their destinations.



AUTOSAR Secure Onboard Communication (SecOC)

Multilayered security approach

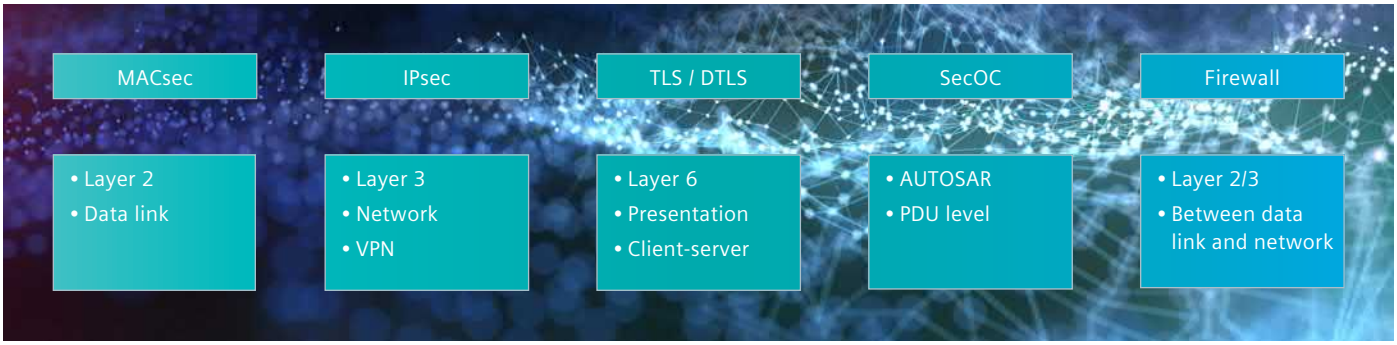
Protecting connected cars requires a multilayered security approach, and a firewall is a vital component. The Open Systems Interconnection (OSI) model standardizes communications functions in seven layers (three media and four host layers), all of which must be secured for an application to be considered safe. The overall security policy must cover prevention at every level or at the level based on the use.

Edge nodes or gateway nodes are the most vulnerable because they are directly exposed to the external world, and need the most protection. The nodes inside the vehicle network are not directly exposed and, these nodes can have basic protection with filtering at the PDU level. At layer two, the data link layer of the OSI model, the industry-standard Media Access Control Security (MACsec) provides point-to-point security on Ethernet links between directly connected nodes and can identify and prevent most security threats, including denial of service, intrusion, man-in-the-middle, masquerading, passive wiretapping, and playback attacks. MACsec defines connectionless data confidentiality and integrity for media access-independent protocol.

At layer three, the network layer, Internet Protocol Security (IPsec) is a suite of protocols that interact with one another to provide secure, private communication across the IP networks, allowing the system to establish and maintain secure tunnels with security gateways; virtual private network (VPN) is an example.

At layer six, the presentation level, Transport Layer Security (TLS) offers cryptographic protocols designed to provide communication security over a network. Websites can use TLS to secure all communications between their servers and the web browsers, and TLS protocols primarily provide privacy and data integrity between two or more communicating computer applications, operating in a client-server mode.

At the AUTOSAR level, the data transmission unit is the PDU. AUTOSAR's specification for Secure Onboard Communication (SecOC) was developed to secure those PDUs. And similarly, between layer two (data) and layer three (network) a firewall can be deployed to block unused ports or prevent the probing of those ports and to filter data use cases.



Multilayered security approach

Firewalling the threats

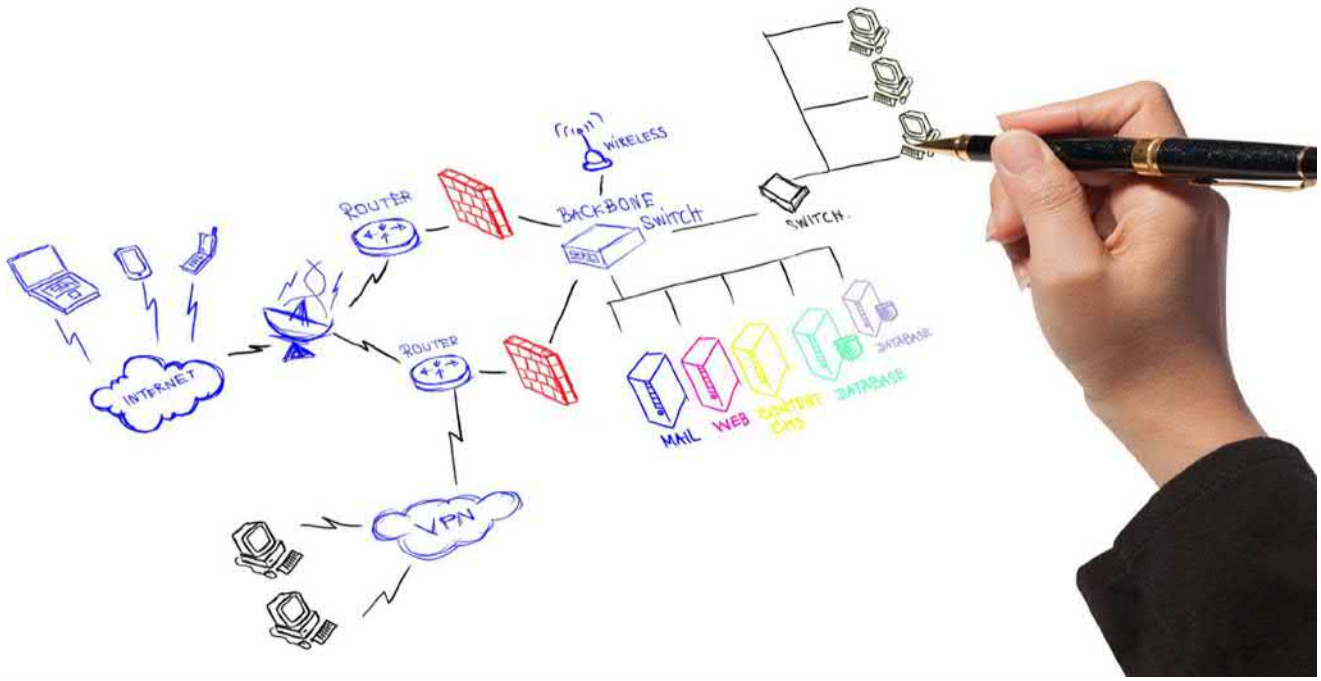
Firewalls are network elements that control the traversal of packets across the boundaries of a secure network based on a specific security policy.

Security policies are lists of filtering rules that define the actions performed on packets.

Filtering rules are composed of a set of filtering fields such as protocol type, source address, destination address, source port, destination ports and an action field.

Filtering fields represent the possible values that a corresponding field in actual network traffic can take for that specific rule. A filtering field can be a single value or a range of values, and can be used to create blacklists or whitelists that block or allow traffic coming from or directed to specific source addresses. Based on this set of rules, the firewall can determine whether to accept the packet for further processing or drop the packet and log the incident.

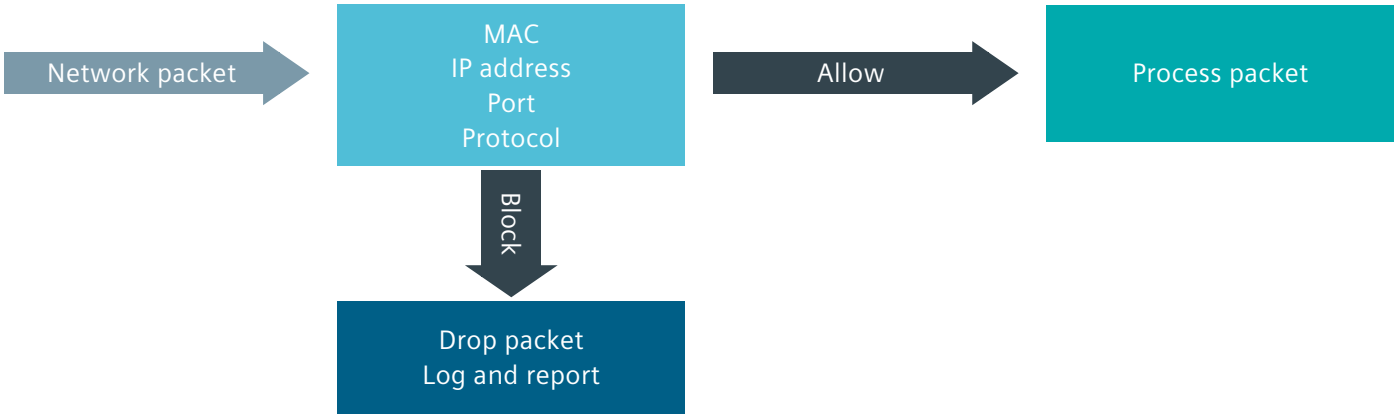
A network layout with a firewall controls the traversal of packets. It not only prevents the internal network from malicious data coming from the outside world, but also protects the outside world from potential malicious data that is generated inside the network. A firewall can secure a portion of the network inside the car, so if a specific ECU is compromised it is not allowed to exploit the weaknesses for the ECU within that secure portion of the network.



Network layout with firewalls

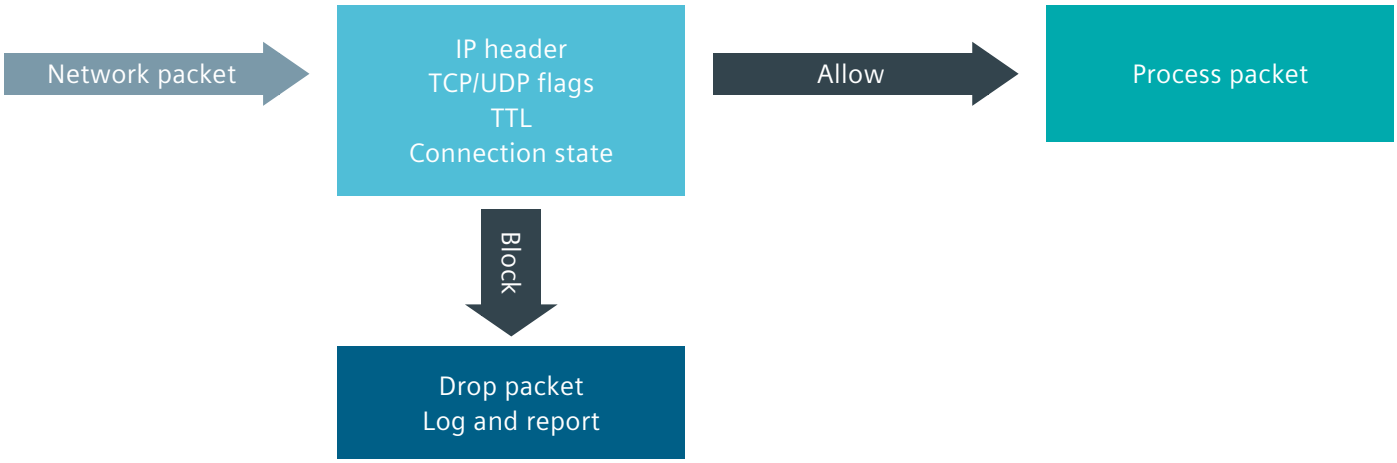
Firewall design considerations

Rule-based filtering, also called packet or static filtering, is the first consideration for firewall design. This type of filtering does not maintain the state of the packets. It is based on configurable rules in the filtering engine that may support protocol, source IP address and MAC address filtering, and it can be used to create whitelist and blacklist filtering.



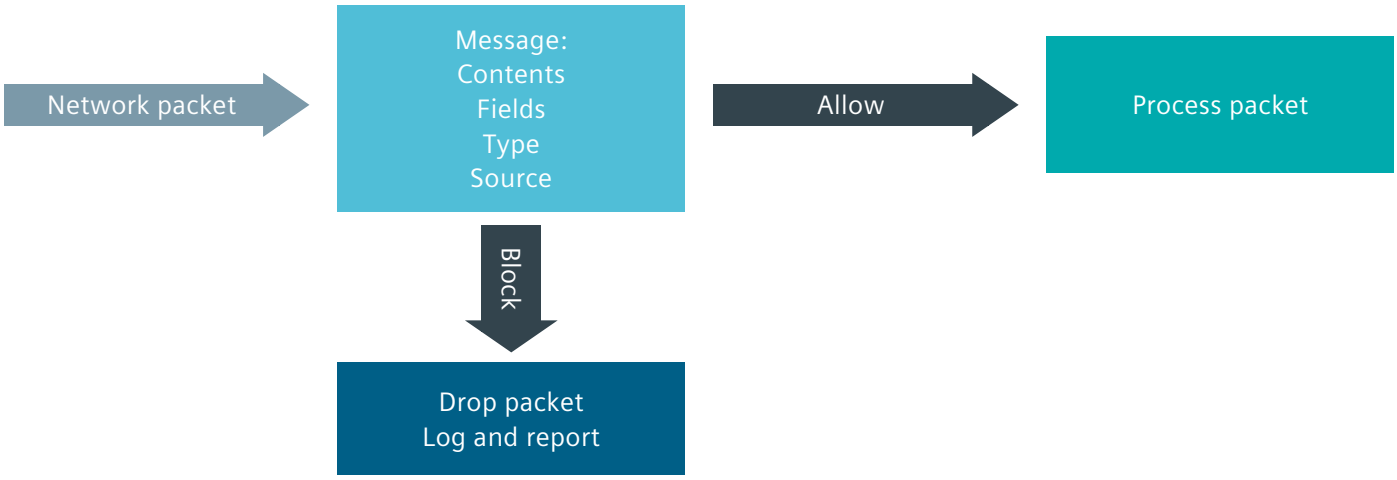
Rule-based filtering

Dynamic filtering. Another type of firewall uses dynamic filtering, also called circuit-level gateway or stateful packet inspection. Dynamic filtering can block packets based on the state of the connection. It can check that the incoming traffic for an unprivileged port with a higher port number is not a compromised response to previous outgoing requests to establish a connection. Dynamic filtering can support IP header options, transmission control protocol (TCP) or user datagram protocol (UDP) flags and configurable time to live (TTL) of packets. The high-level concept is that the filtering engine selects the network packet and performs the specific logic based on the rules to allow the packet to process or drops, logs and reports it.



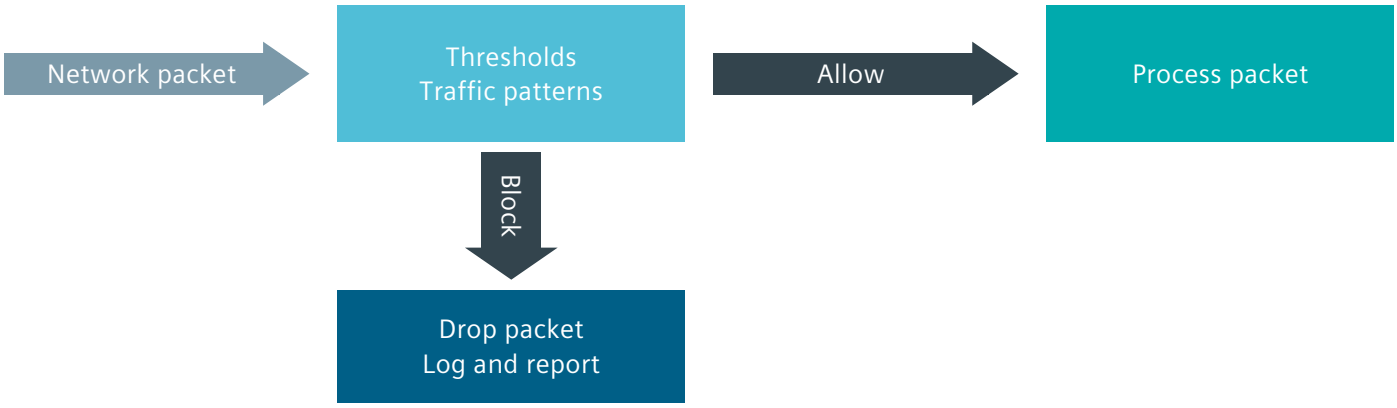
Dynamic filtering

Deep packet inspection, also known as an application-level gateway, allows control and validation of each individual field within the message, and filters messages based on type, contents and source. It is typically used to secure industrial automation and control systems.



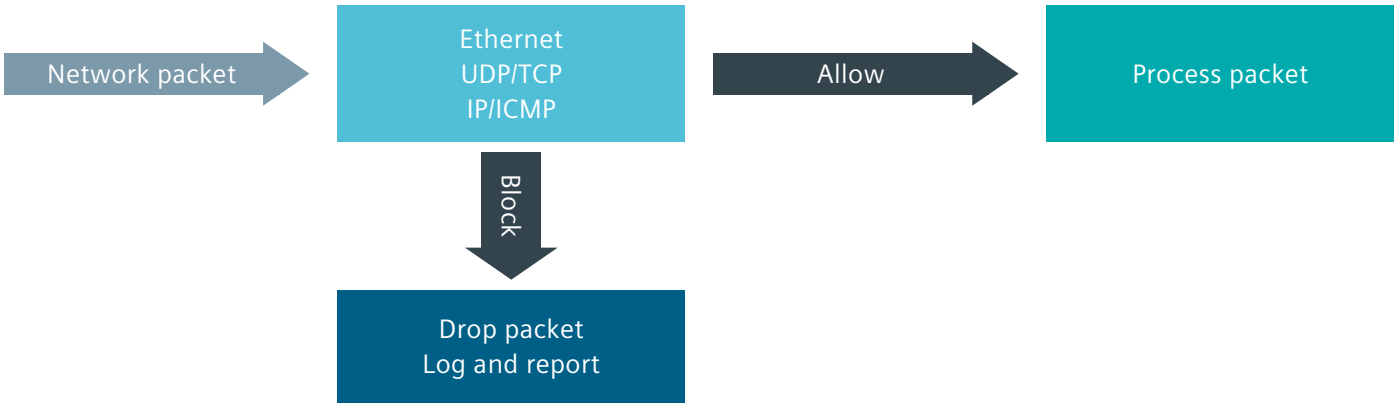
Deep-packet inspection (application-level gateway)

Threshold filtering can block packets based on threshold crossings to protect against denial-of-service attacks, broadcast storms and other types of packet flood conditions. Threshold filtering is based on network traffic patterns. Thresholds are used to determine the level at which the network traffic will be dropped or should be blocked. Static filtering is less efficient as compared to threshold filtering. Threshold filtering determines network traffic patterns in real time, which thresholds are being set, and which decisions should be made and filtering actions taken on specific packets.



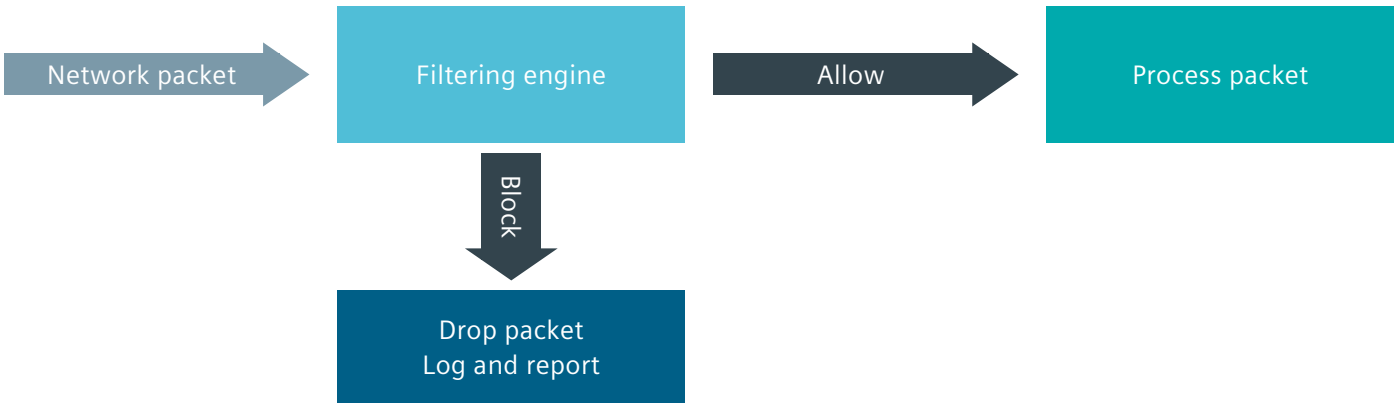
Threshold filtering

Protocol filtering is a firewall approach that drops packets based on a set of rules related to application layer protocols, which can be set for Ethernet, Internet Protocol (IP), Internet Control Message Protocol (ICMP), Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). Protocol filtering can terminate the application layer connection and resend the traffic to a destination if it fulfills the criteria set by the rules.



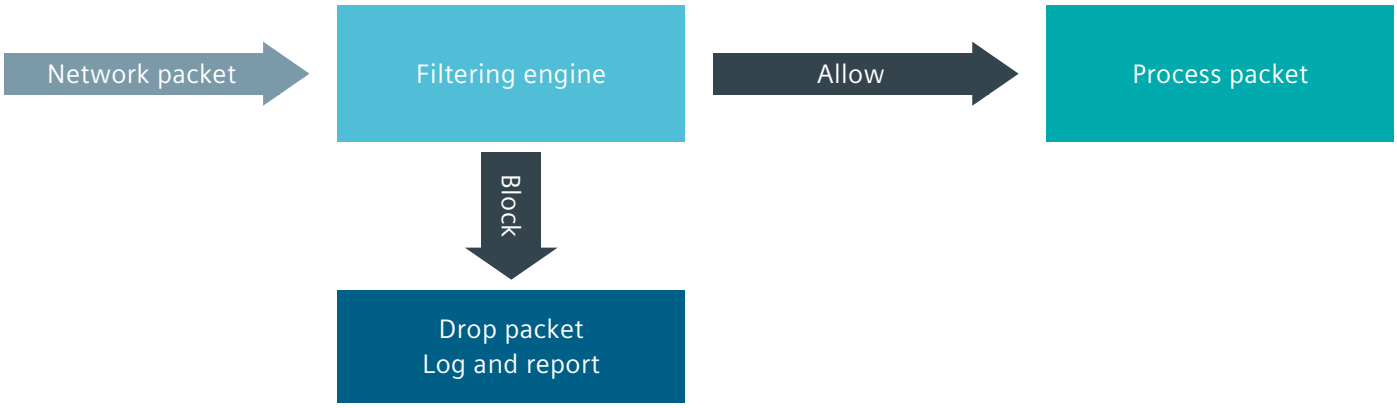
Protocol filtering

Data logging and alerts are also important firewall design considerations. A log of security events and policy violations should be maintained. Changes to firewall policies should also be recorded to enable support for audits and forensics. Event logging can be used for forensic investigations and for determining the sources of attacks and actions for the future. Other advantages include real-time analysis and aiding in development of risk mitigation strategies.

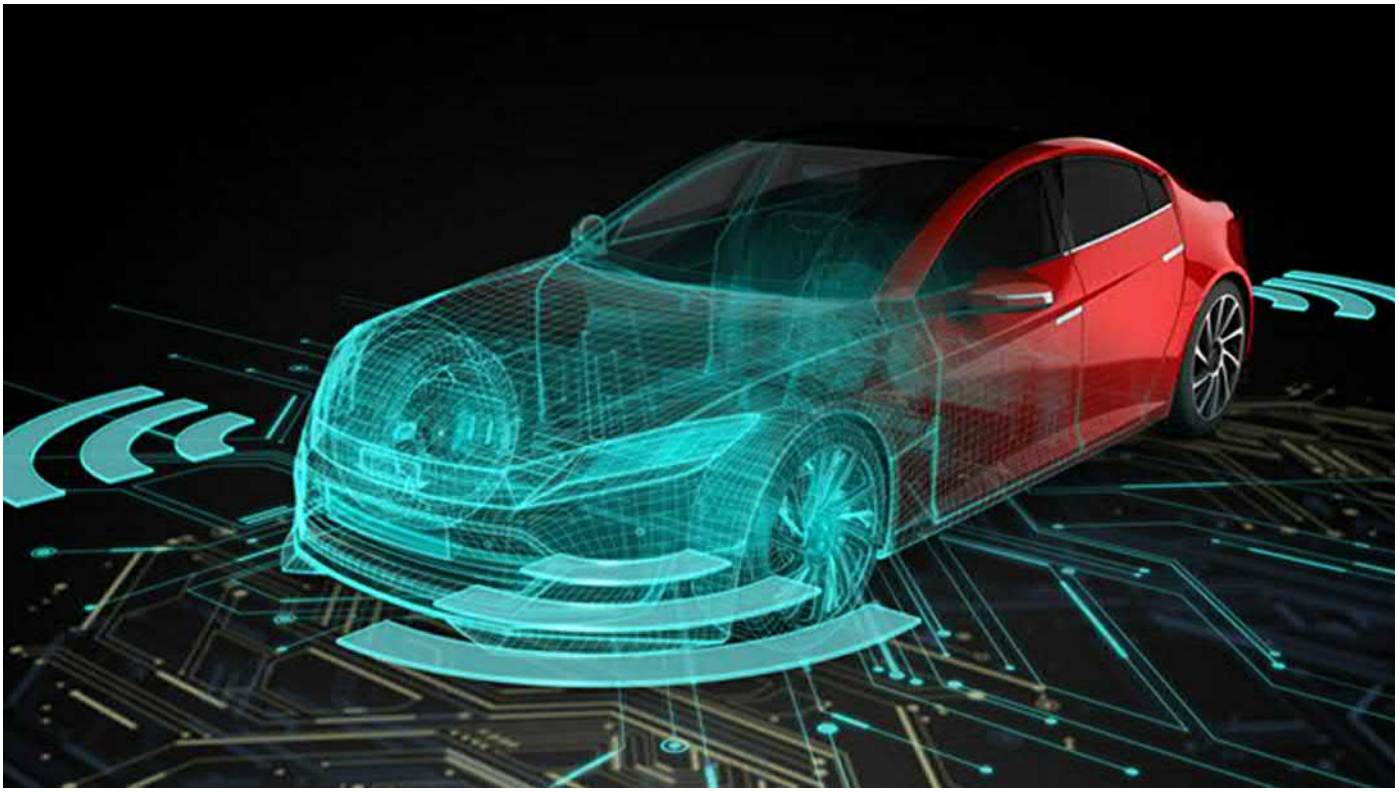


Data logging and alerts

Connected car environment is another firewall design consideration. In contrast to leading-edge, state-of-the-art firewalling that is based on human usage patterns and deployed with artificial intelligence and machine learning, the connected car environment is characterized by small power and memory footprints and ECUs inside the car, and embedded efficiency is very important.



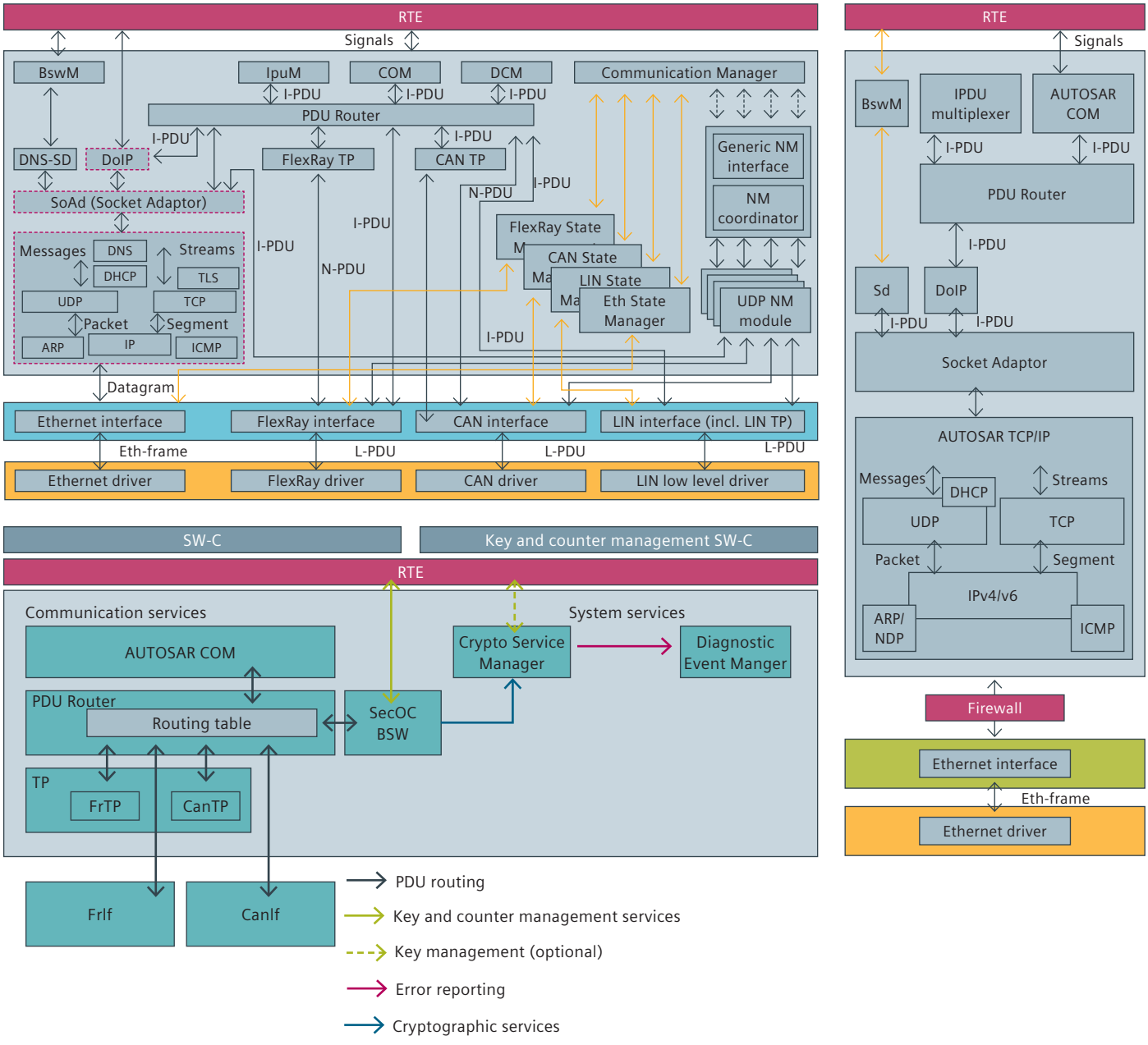
Embedded efficiency – configurability, CPU load, memory



The rules for the filtering engines that process each packet must have sufficient memory and will consume CPU cycles. From a replicability standpoint, it is important to enforce rules. Firewall designers should deploy the firewall that is most suitable for the specific use case. Configurability is the key – it should be allowed to switch on or off the sets of rules that are required under specific scenarios, use cases or situations in which an ECU is deployed.

The final design consideration is to take filtering actions as early as possible, when the packet enters the network. If the filtering is too late, sometimes the damage is already done. Consider denial of service attacks, when the network is being flooded with packets. If the packet is allowed inside the network for a longer period of time, the purpose of the attack is already fulfilled. Devices can become unusable with a flood of packets if they are dropped too late.

Firewalls should be placed between layer two and layer three at the TCP/IP level. TCP/IP has all the information that is required for the firewall to work –source IP address, destination, MAC address and others. If the firewall is deployed that far down inside the network, it can work most efficiently, an important consideration especially for high-risk gateways that are exposed directly to the external network.



Conclusion

Early detection. Early detection is the key to firewalling security threats in connected cars. Because hackers look for open ports to gain access inside the network, it is very important to block all open ports and log packets that violate the rules for those ports.

Configurability. Configurability is very important for embedded efficiency, which requires independent enabling or disabling of filtering rules. It is beneficial if configuration can be done remotely, using an enterprise-level security management system. Some solutions are available that enable centralized management of security policies, and offer other advantages like monitoring the health of the device remotely, and supporting analytics.

Standardization. Standardization is critical; the firewalling concept should be adopted according to the AUTOSAR security policy manager. We recommend that AUTOSAR define a specification for connectivity firewalls.

The automotive industry must prove itself trustworthy enough for humans to trust connected cars. Security is not a competitive offering – it is required for a connected car to work, and the firewall remains a vital component of a multilayer security approach.

References

1. Charette, Robert N., "This Car Runs on Code," *IEEE Spectrum*, February 1, 2009, https://spectrum.ieee.org/transportation/systems/this-car-runs-on-code
2. Burkacky, O., Deichmann, J., Doll, G., and Knochenhauer, C. "Rethinking car software and electronics architecture," McKinsey & Company, February 2018, https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/rethinking-car-software-and-electronics-architecture
3. Fox, Zohar, "How Do We Trust the Software in A Driverless Car," *Forbes*, June 2018, https://www.forbes.com/sites/startupnationcentral/2018/06/05/how-do-we-trust-the-software-in-a-driverless-car/
4. "Hackers Remotely Kill a Jeep on the Highway – With Me in It," *Wired*, July 21, 2015, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
5. Greenberg, Andy, "This Gadget Hacks GM Cars to Locate, Unlock, and Start Them," Wired, July 30, 2015, https://www.wired.com/2015/07/gadget-hacks-gm-cars-locate-unlock-start/
6. "Hackers Can Steal a Tesla Model S in Seconds by Cloning Its Key Fob," Wired, September 29, 2018, https://www.wired.com/story/hackers-steal-tesla-model-s-seconds-key-fob/
7. Upstream Security, Global Automotive Cybersecurity Report 2019, https://www.upstream.auto/upstream-security-global-automotive-cybersecurity-report-2019/.
8. www.autosar.org

Siemens Digital Industries Software

Headquarters
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 972 987 3000

Americas
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 314 264 8499

Europe
Stephenson House
Sir William Siemens Square
Frimley, Camberley
Surrey, GU16 8QD
+44 (0) 1276 413200

Asia-Pacific
Unit 901-902, 9/F
Tower B, Manulife Financial Centre
223-231 Wai Yip Street, Kwun Tong
Kowloon, Hong Kong
+852 2230 3333

About Siemens Digital Industries Software

Siemens Digital Industries Software is driving transformation to enable a digital enterprise where engineering, manufacturing and electronics design meet tomorrow. Our solutions help companies of all sizes create and leverage digital twins that provide organizations with new insights, opportunities and levels of automation to drive innovation. For more information on Siemens Digital Industries Software products and services, visit siemens.com/software or follow us on LinkedIn, Twitter, Facebook and Instagram. Siemens Digital Industries Software – Where today meets tomorrow.

siemens.com/software

81330-C7 3/20 Y