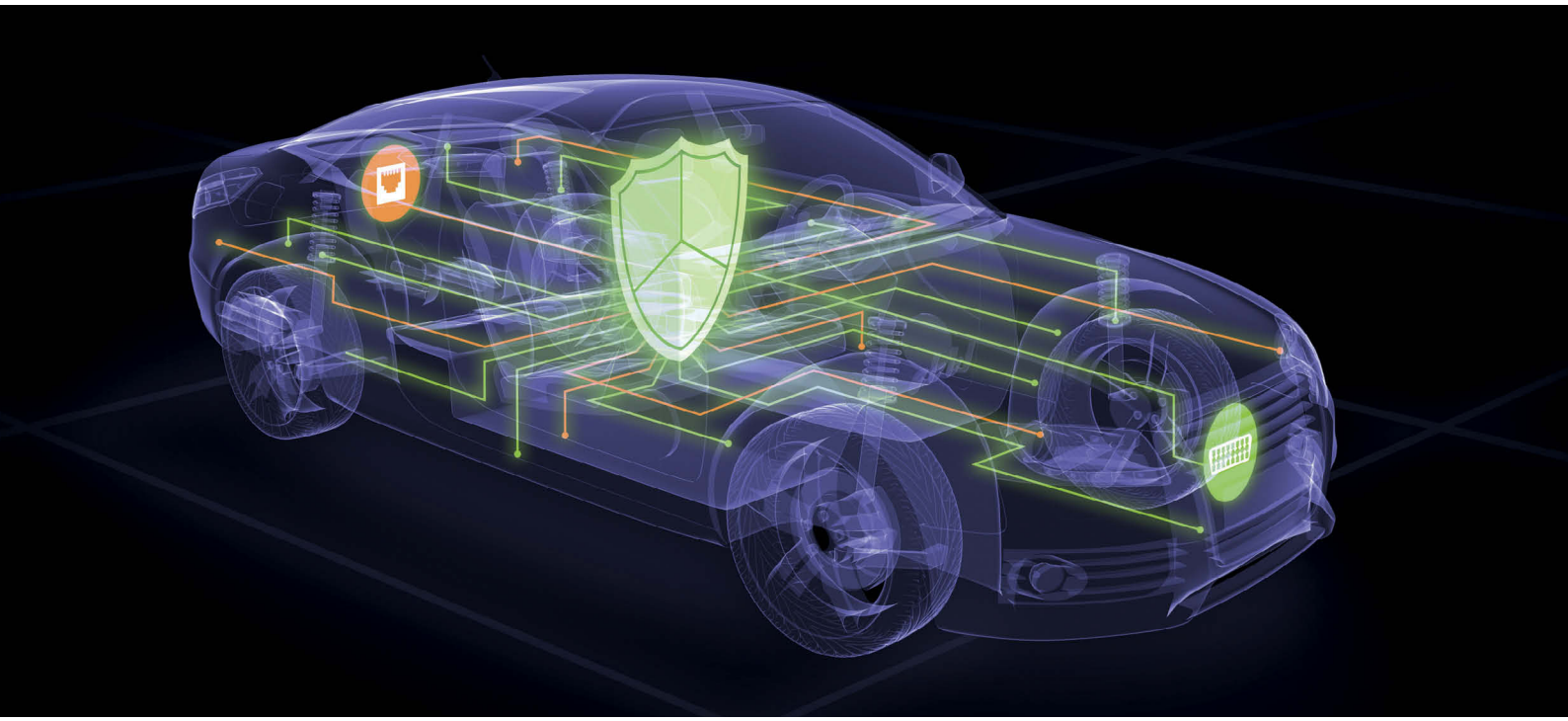
Intrusion detection for hybrid CAN-Ethernet networks

Tailoring security measures to both worlds



Today's decentralized E/E architectures are no longer up to the challenges of connected, automated vehicles, which is why vehicle computers and automotive Ethernet will complement conventional ECUs and CAN buses. These kinds of vehicle networks require protection in the form of tailored attack detection and data traffic monitoring.

The direction of development is clear: vehicle computers (VCs) and broadband automotive Ethernet will complement today's vehicle electrical systems with dozens of ECUs connected by CAN, LIN, and FlexRay data buses. The latter remain in demand where high real-time requirements and cyclically recurring functions need to be implemented. In other instances, microprocessor-based central computers partitioned into virtual machines will take over, because they are better equipped to meet the challenges of connected, automated vehicles.

But how can hybrid CAN-Ethernet architectures and their data processes be effectively secured? Fundamentally, there are two principles: communication shielding and partitioning. Seamless monitoring of communication is required in order to detect cyber attacks at an early stage; domain-specific virtual subnets (VLANs) minimize the penetration depth in the case of an attack. Both are feasible in hybrid electrical systems, but require different methodical approaches for the CAN and Ethernet worlds.

Efficient attack detection for CAN

An intrusion detection system (IDS) can be integrated into gateways or ECUs to monitor the CAN buses. It detects anomalies in CAN data traffic by comparing it with the "normal behavior" specified by the OEM. The embedded security component looks out, for example, for anomalies in cyclical messages and abusive diagnostic requests, which it classifies as potential attacks and logs or reports (Fig. 1).

The performance of the CAN IDS (CycurIDS) depends directly on the quality of its configuration. This is why efficient initial rules from the OEM should be continuously supplemented by new detection mechanisms based on analyses of current attack vectors in order to achieve a high detection rate with as few false alarms as possible. The implementation stands and falls with the quality of the toolbox, which is used for the initial configuration and the continuous development of the rule sets. As ready-to-use software, such an IDS (CycurIDS) can be used as a CAN attack detection system in hybrid electrical systems at any time.

Automotive firewall in the Ethernet switch

In contrast, an automotive Ethernet firewall (CycurGATE) is advisable for secure, smooth Ethernet communication in hybrid electrical systems. This is implemented directly in the Ethernet switch, allowing it to monitor the complete packet flow without risking any interference with ECUs or the host controller. Balanced hardware and software co-design means that the firewall can make use of the hardware acceleration on the switch. As a result, most of the data packets are processed at wire speed. The main task is to defend against denial of service attacks. But by maintaining partitioning in all network layers, the firewall also supports secure data exchange between partitioned domains. To this end, a packet filter filters the incoming and outgoing data, checking each by way of stateful packet inspection and deep packet inspection.

So, the automotive Ethernet firewall (CycurGATE) not only protects the electrical system against unauthorized access and manipulation – it also serves to control onboard communication (Fig. 2). It completely covers the Ethernet/IP including the common automotive protocols (e.g., SOME/IP), and it monitors access to networks and VLANs at MAC level. Communication is filtered by means of whitelists or blacklists that can be updated at any time, which ensures fast, effective reactions to new attack patterns.

```
…
0.010000 1  100  Rx  d 8 8A FF FF 0C 42 5F FD 97
0.011000 1  110  Rx  d 8 03 3E 3E E2 10 FF 4A 3F
0.012000 1  120  Rx  d 8 03 F7 30 27 C7 7E D9 9C
0.020000 1  100  Rx  d 8 11 F4 00 3E E2 60 6C B9
0.021000 1  110  Rx  d 8 1F AA 00 00 00 00 C0 00
0.022000 1  120  Rx  d 8 02 AA 00 00 00 00 C0 00
0.031000 1  110  Rx  d 8 86 4A 2F 01 81 05 80 7F
0.031500 1  110  Rx  d 8 E5 2B 41 0C 00 00 00 00
0.032000 1  120  Rx  d 8 02 04 78 00 FF 00 00 30
0.041000 1  110  Rx  d 8 6E 7B FF FF 3F FF 1F 8B
0.042000 1  120  Rx  d 8 00 5A 00 00 0F 55 02 00
0.043000 1  7DF  Rx  d 8 02 10 03 00 00 00 00 00
0.044000 1  7E8  Rx  d 8 02 50 03 AA AA AA AA AA
0.051000 1  110  Rx  d 8 FE 4B 2F 01 81 07 80 7F
0.052000 1  120  Rx  d 8 68 05 78 00 FF 00 00 30
…
```

Timings
- Frequency deviation
- Message infiltration
- Time-outs

Diagnostics
- Type of service
- Service conditions

Figure 1: The CAN IDS detects anomalies in cyclical messages and any abuse of diagnostic requirements.

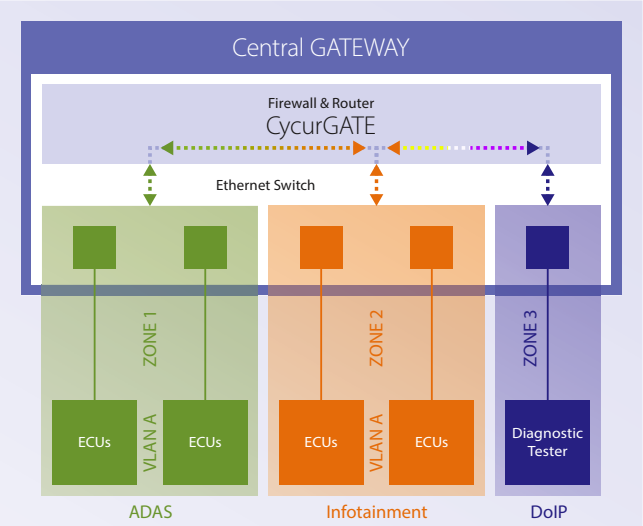


Figure 2: Automotive Ethernet firewall assumes gatekeeper and router functions.

Intelligent load distribution

In addition to implementation in the central Ethernet switch, it is also possible to integrate host-based firewalls directly into ECUs. This requires high-performance solutions. The firewall must be powerful enough to check in real time and decide whether and where to route individual data packets. However, it cannot cover complex attack detection patterns, such as the frequency of stateful SOME/IP communication. Here, an additional Ethernet IDS is required that detects patterns of anomalies based on the message frequency, sequence, payload, data, and services and logs or reports them as attack attempts. For optimum performance, this approach requires intelligent load distribution between switch and microcontroller. Firewalling and intrusion detection can take place partly in the switch and partly in the target controller.

Together, CAN IDS, automotive Ethernet firewall, and Ethernet IDS can protect hybrid E/E architectures reliably and without noticeable latencies. Embedded in integrated security concepts, they are central components of risk prevention and functional safety in the connected and increasingly automated vehicle of the future. ■

Authors

Dr. Jan Holle is Product Manager for Intrusion Detection Systems at ESCRYPT. **M.Sc. Siddharth Shukla** is Product Manager for Automotive Firewall at ESCRYPT.