Hardware-based Cyber Security for Connected Vehicles

Lee Harrison, Director Product Marketing

SIEMENS

Tessent Embedded Analytics - Example Markets Verticals we serve

AI

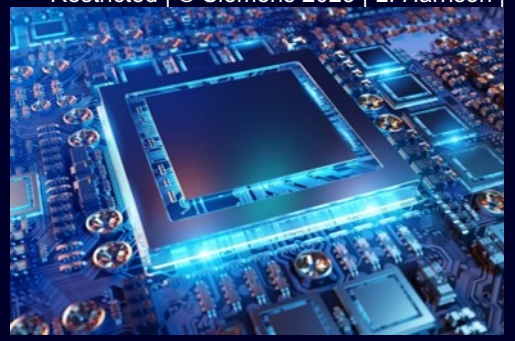
Data Center

Automotive

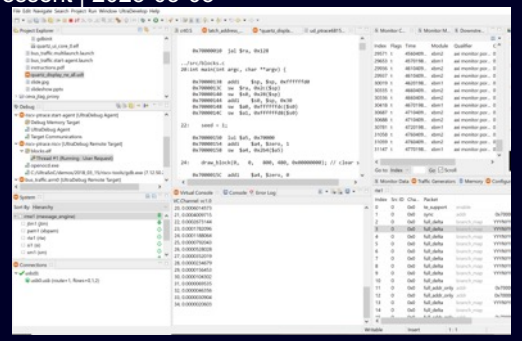
5G

Storage

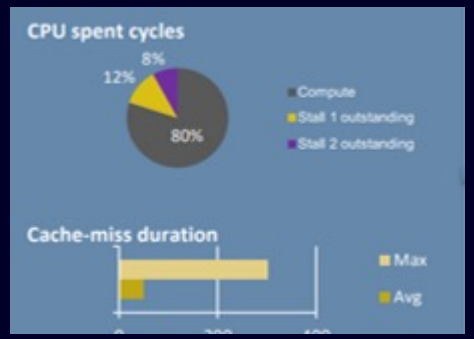
Common Characteristics of Previous Designs



Complex Designs



Debug Functionality



System Performance

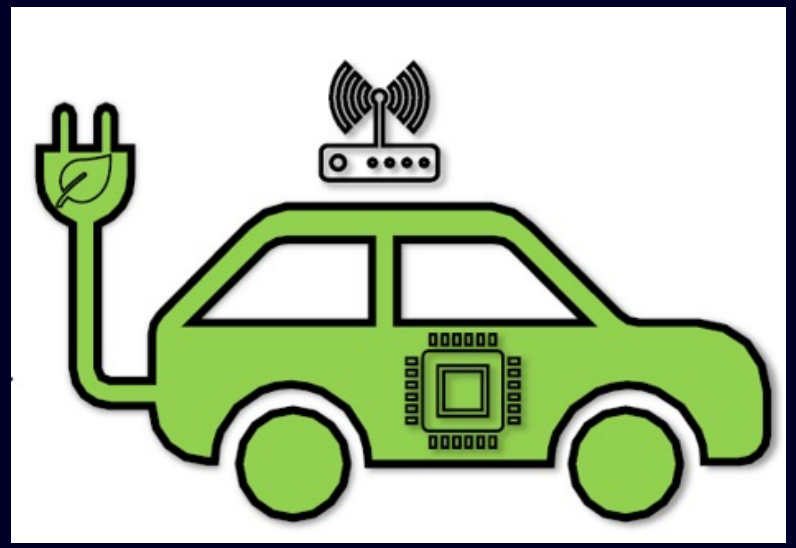
Hardware/Software Optimisation

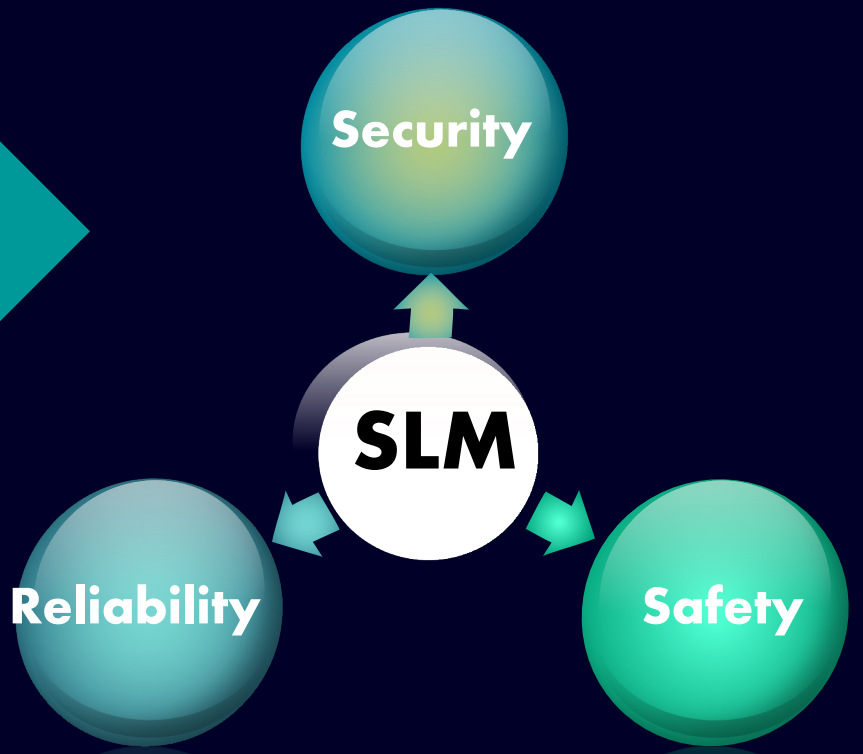
RISC-V Adoption

SIEMENS

Background

ISO 21434



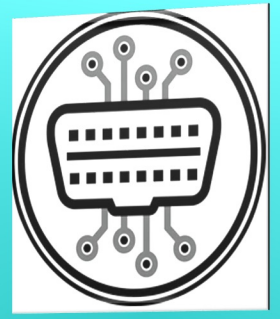


UNECE

ISO 26262

SIEMENS

Threat Categories



Automotive Control Systems

- OBD-II
- CAN
- ECUs

Vehicle Sensors

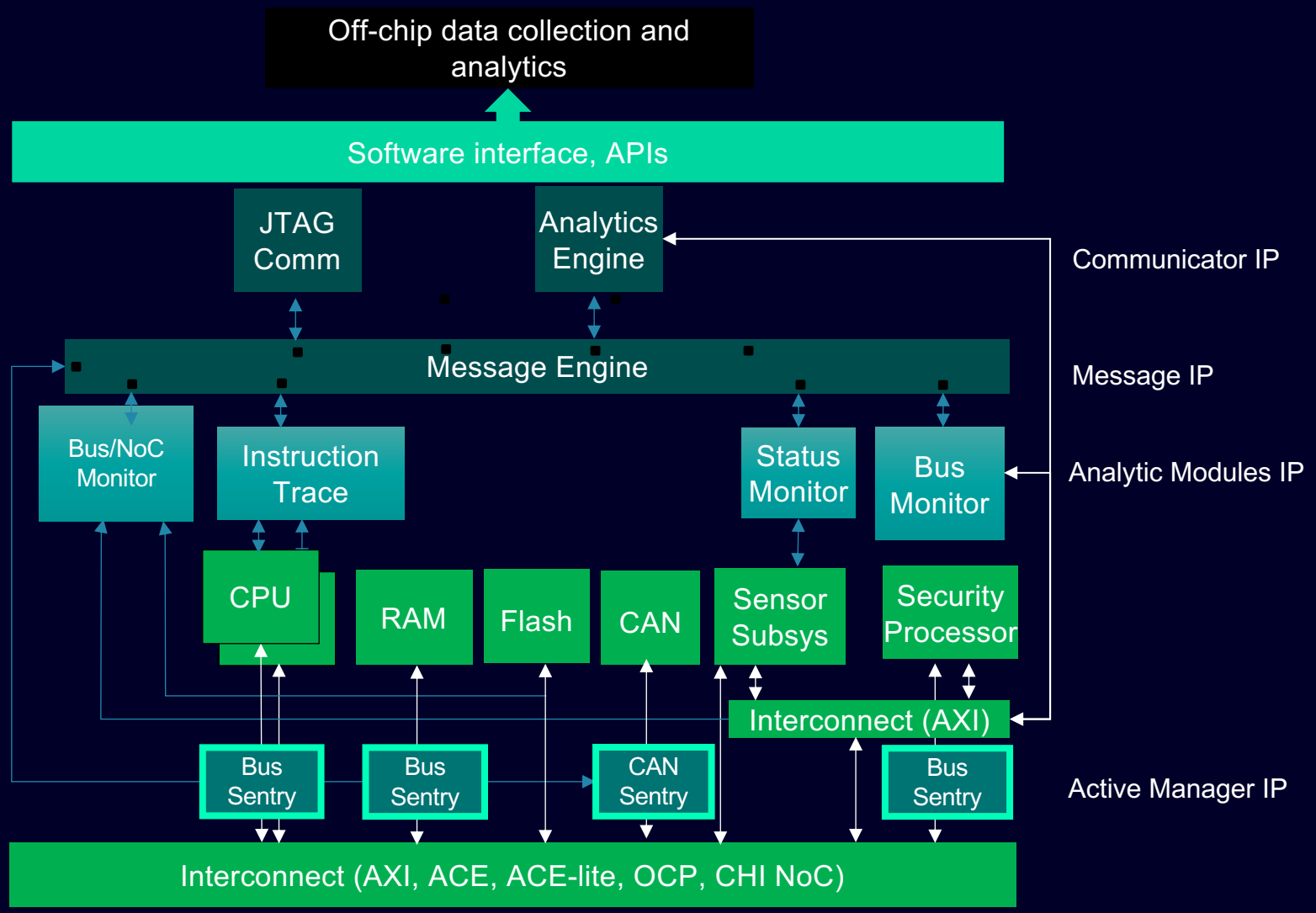
- LiDAR
- Radar
- GPS
- Cameras

V2X Communication

- Mobile Apps
- OTA Updates
- Infotainment Systems / Head Units
- Automotive Key
- VANETs

SIEMENS

An embedded security subsystem – Siemens Tessent Embedded Analytics



System IP

Embedded Analytics Monitor IP

Embedded Analytics Sentry IP

Embedded Analytics Messaging IP

Embedded Analytics E-SDK Embedded SW

SIEMENS

Attack Examples

ABUSE CASE DATASHEET

Mobile Network Attack

In this scenario attacker tries to infect Telematic Control Unit with tampered firmware. Using a man in the middle type of attack to make an over the air firmware update.

DAMAGE SCENARIO

- Hackers can intercept telematics traffic using GSM.
- Hackers can spoof the SMS commands, sending direct commands to the device

THREAT SCENARIO

- Attack to infect Telematic Control Unit with tampered firmware
- Attack to gain access to infotainment unit
- Remote provisioning of embedded SIM by unauthorized party
- Denial of service attack against emergency services
- Premium rate fraud – vehicle TCU used to send SMS or dial premium rate services
- Unauthorized vehicle function control via app compromise
- Unauthorized vehicle function control via false basestation (attack could be made more feasible through open source LTE projects)

IMPACT RATING

MAJOR

Vehicle occupants and other road users could be harmed if vehicle suffers engine, transmission or brake failure while travelling at high speed

SOLUTION

If the Tessent Embedded Analytics solution (using a bus monitor) detects suspicious activity in TCUs firmware it will block all outgoing frames from this module

SECURE CAV Advanced cybersecurity for connected and autonomous vehicles

Copper Horse · Coventry University · University of Southampton · SIEMENS

www.securecav.com

ABUSE CASE DATASHEET

Insecure Telemetrics Control Unit (TCU)

Simple example

In this scenario we assume that TCU is compromised and starts sending harmful frames. Attacker through TCU tries to influence inner workings of vehicle which may endanger the safety of the driver and passengers.

DAMAGE SCENARIO

- Remote control or loss of vehicle ECU functionality potentially endangering vehicle occupants and road users.
- Depletion attack targeting vehicle battery/fuel.
- Driver data is extracted from the vehicle or external servers.

THREAT SCENARIO

- Attacker reverse-engineers authentication between the vehicle and Telematic Control Center.
- Attackers remotely take-over vehicle by re-engineering TCU firmware.
- Attacker exploits vulnerability in the vehicle manufacturer's telematics web portal.
- Attacker discovers hard-coded admin credentials by examining smartphone app.
- Attacker gains access to OEM repository allowing software components to be downloaded to access live vehicle data.
- Deauthentication attack on head unit/TCU wireless access points (APs).
- Driver and vehicle info extracted by connecting to infotainment unit through wireless access point.

IMPACT RATING

SEVERE

Remote vehicle take-over. Attacker is in a position to crash vehicle, causing harm to occupants and other road users.

SOLUTION

The Tessent Embedded Analytics solution monitors current speed by looking on CAN traffic and uses it to validate service frames on CAN bus. If it observes a frame that could cause harm to moving vehicle, aborts it and signals an event.

SECURE CAV Advanced cybersecurity for connected and autonomous vehicles

Copper Horse · Coventry University · University of Southampton · SIEMENS

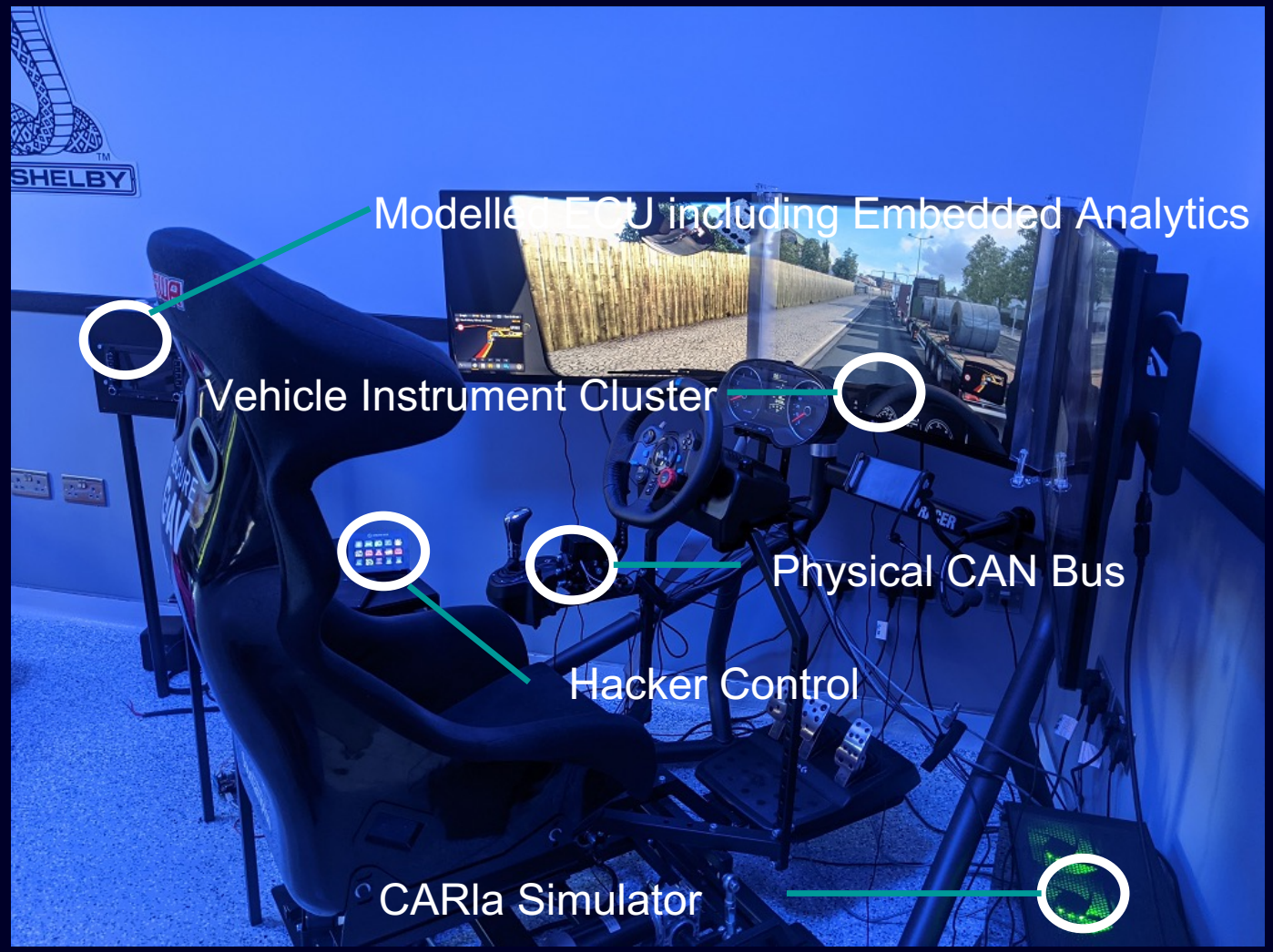
www.securecav.com

SIEMENS

Physical Demonstrator

SecureCAV

http://www.securecav.com



SIEMENS

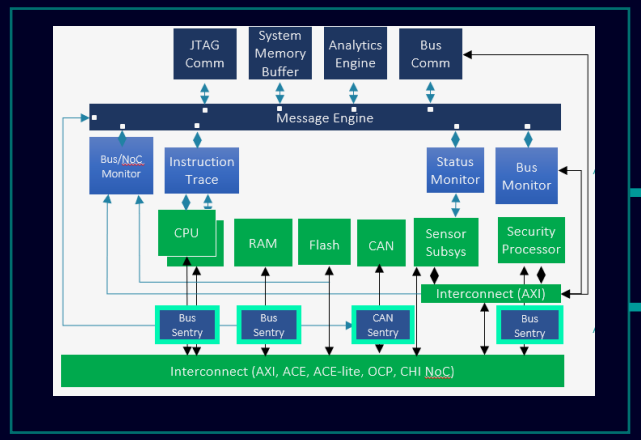
SecureCAV Demonstrator Architecture

Vehicle Simulator

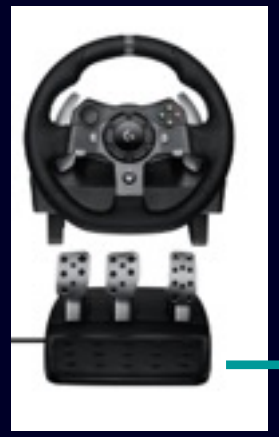
Ethernet to CAN

Example ECU's

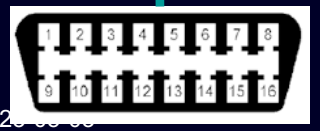
Cloud Data Storage

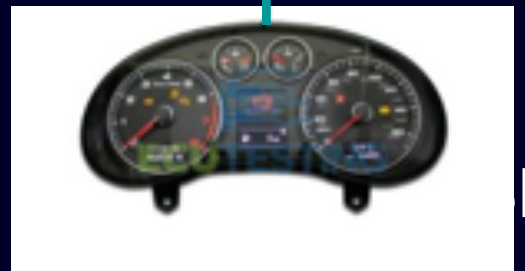


FPGA based ECU Including Embedded Analytics



CAN Network





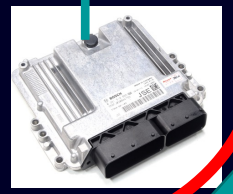
SIEMENS

SecureCAV Demonstrator Architecture

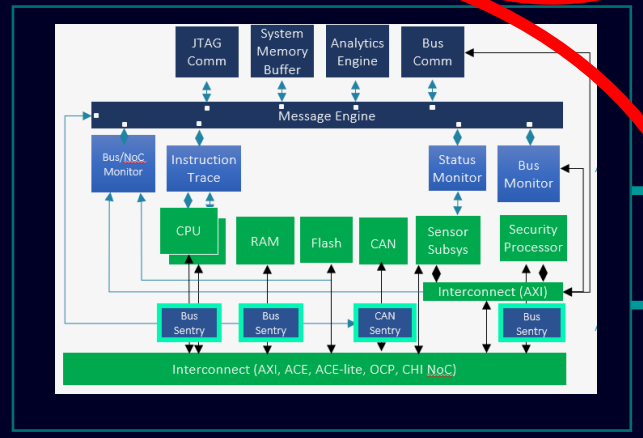
Vehicle Simulator

Ethernet to CAN

Example ECU's



Cloud Data Storage

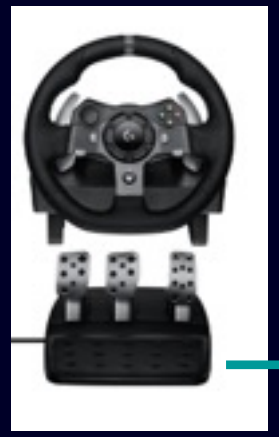


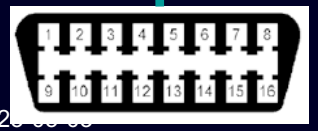
AI Based analysis

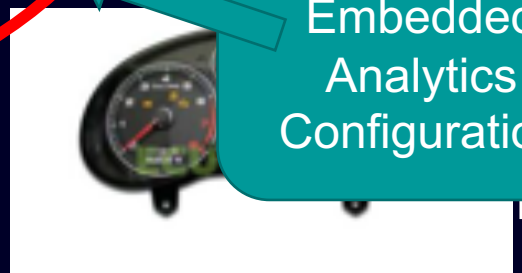
FPGA based ECU Including Embedded Analyti

Updated Embedded Analytics Configuration

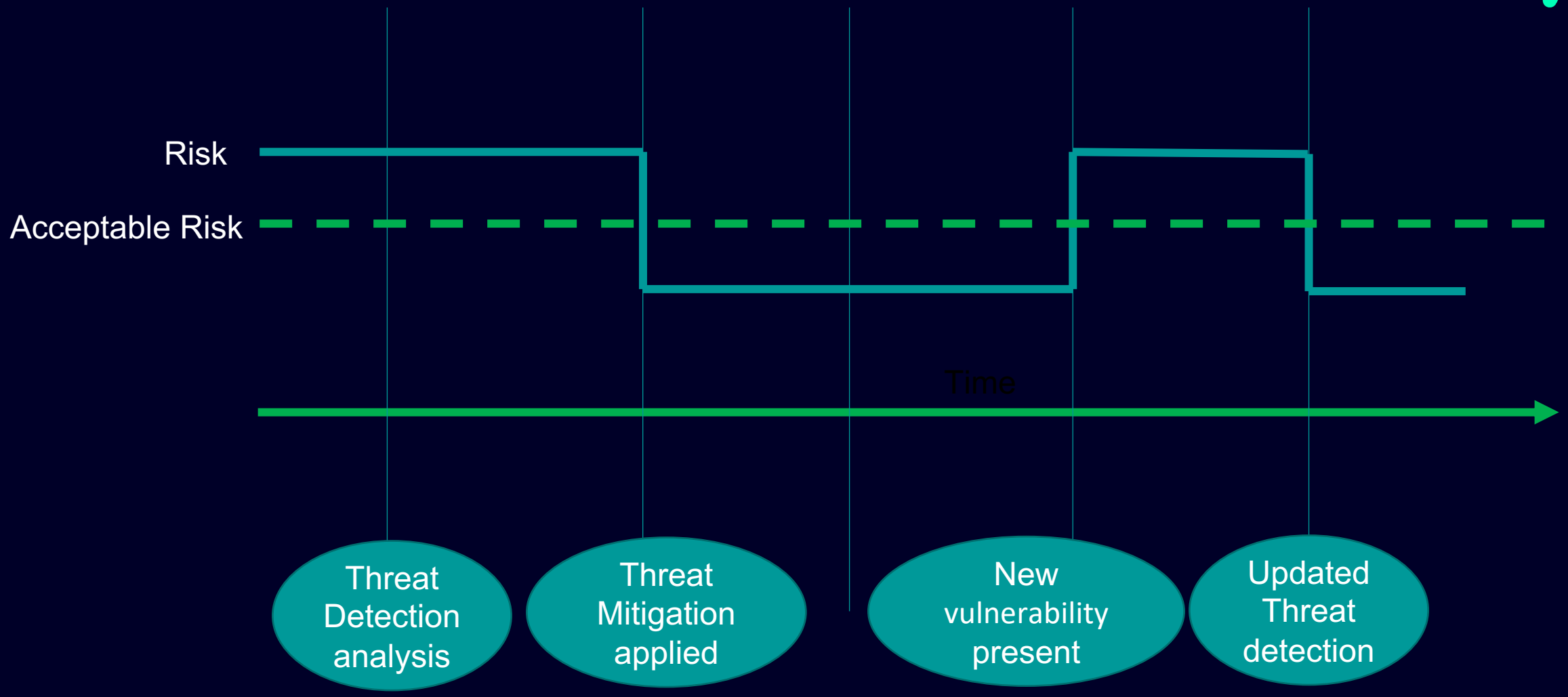
CAN Network







ISO 21434 Threat Detection



SIEMENS

Cloud based data analysis

Problem

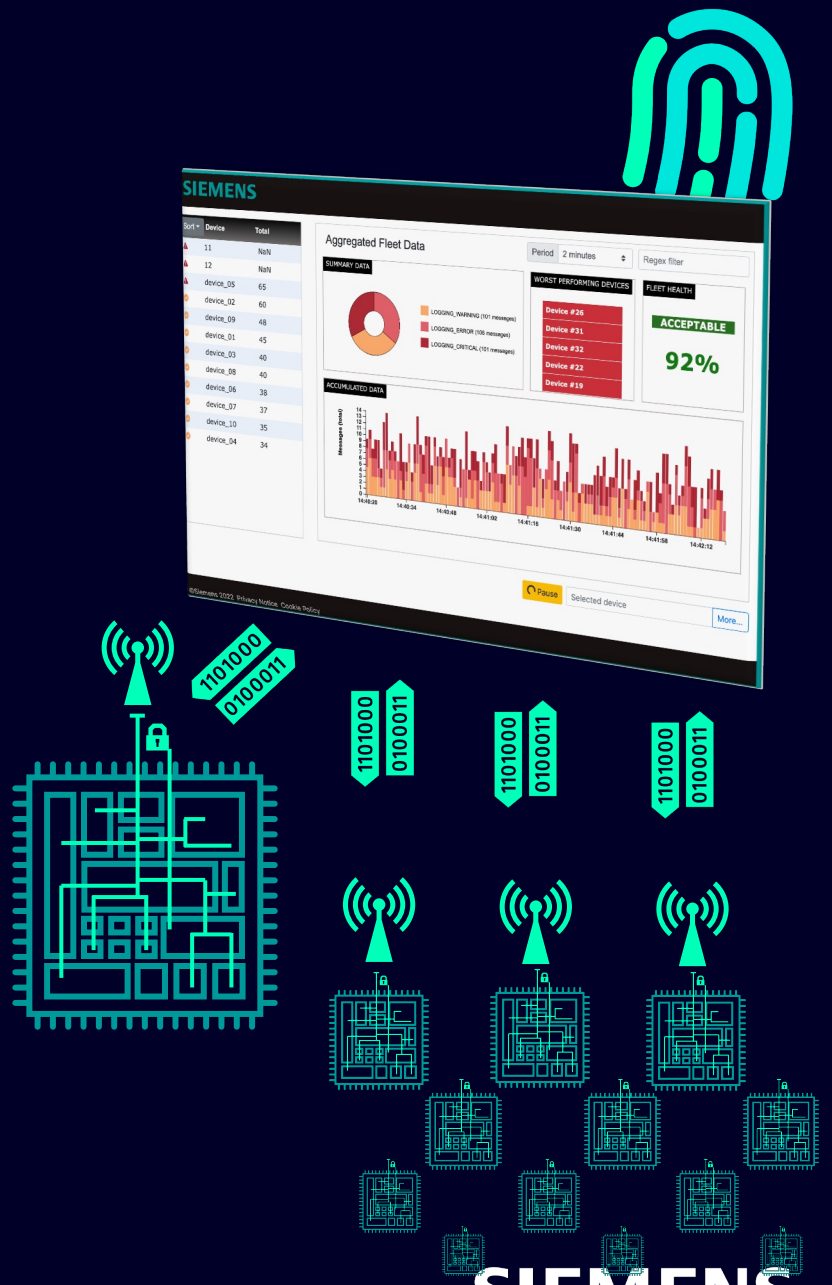
Once deployed it is required to continue the online monitoring of devices for their entire life cycle.

Solution

Full visibility into deployed systems enabling optimisations and debugging throughout the entire system lifecycle

Benefits

- Fleet data collected to enable more advanced offline analysis
- Optimise software to achieve better performance and efficiency
- Faster root-cause analysis of attacks and bugs improve customer satisfaction
- Use historical performance data to inform designs of next-gen chips



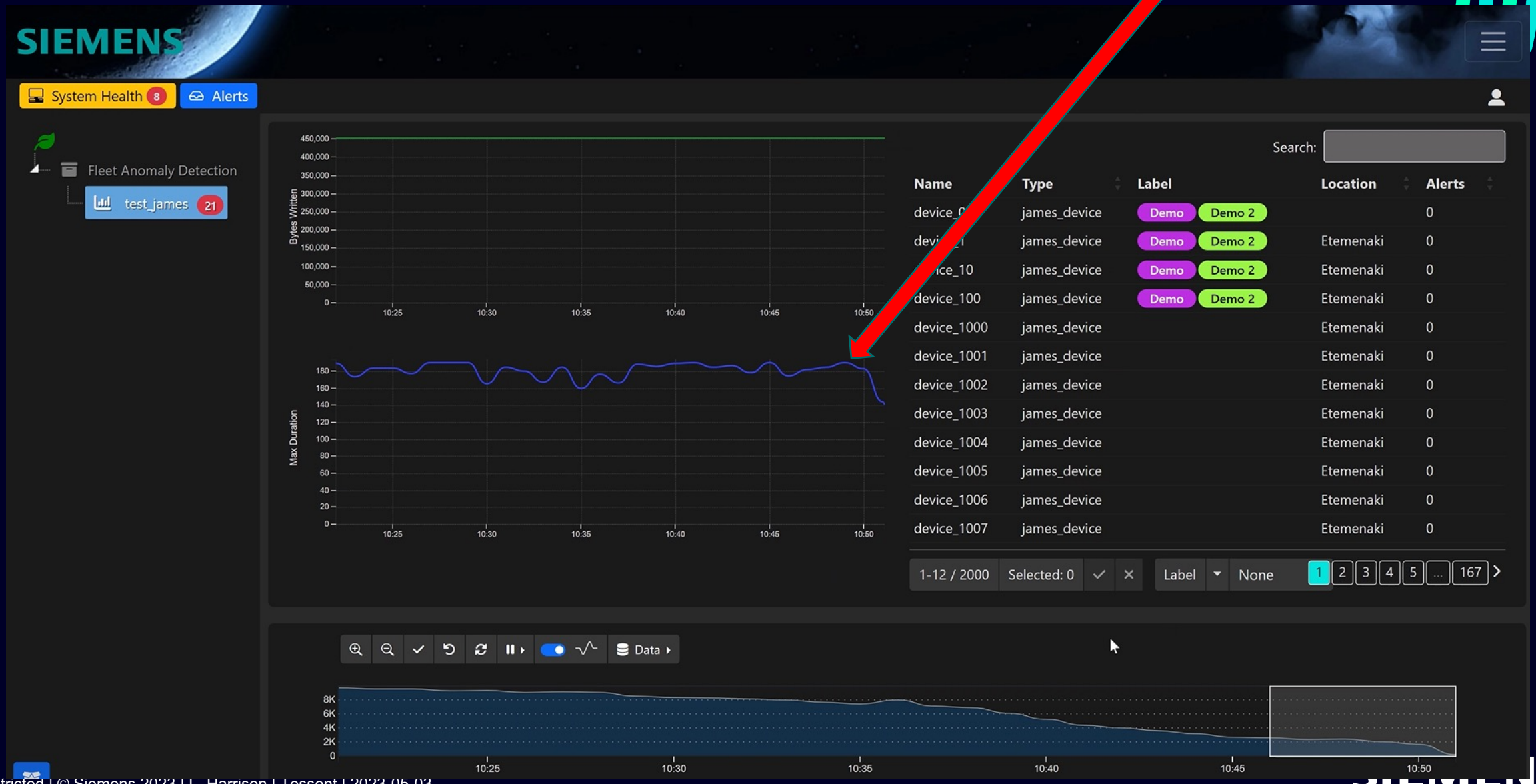
SIEMENS

Detection of individual attacks

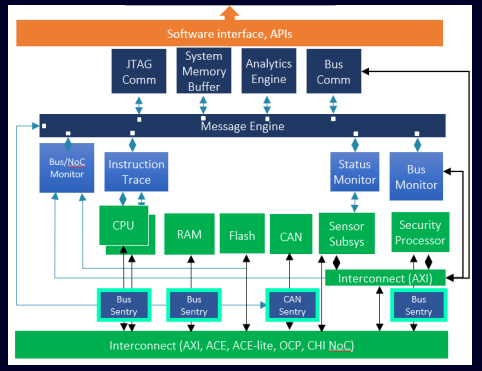
Anomalous device

Analysis of fleet impact

Fleet variation

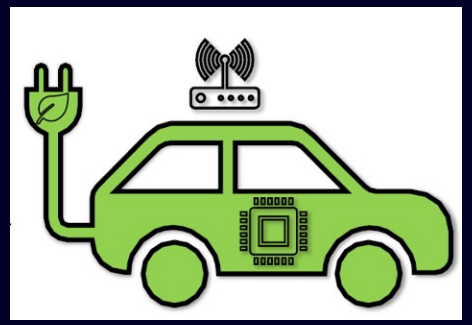


Data feedback and OTA

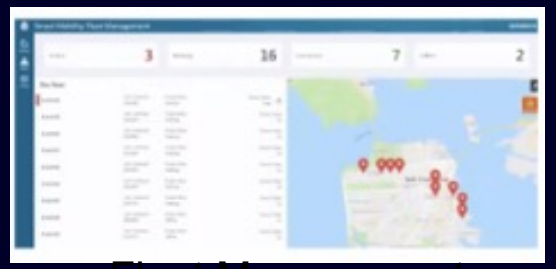


Embedded Analytics
On-Chip Data Collection

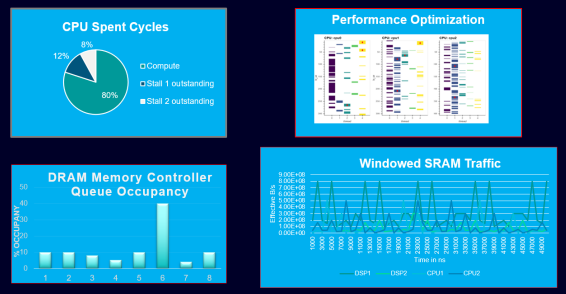
Sokol Embedded Linux
debian or yocto PROJECT
Embedded Solutions



Data Analytics



Fleet Management



SIEMENS

Some of the patents we hold for the IP

- Detecting anomalous latent communications in an integrated circuit chip - allows classifying read latencies seen by a CPU as anomalous or normal
- Identifying causes of anomalies observed in an integrated circuit chip - finding commonalities in measurement windows preceding a known anomalous window
- Error detection within an integrated circuit chip - monitoring errors in data transactions in flight (CRC) + actively performing memory region scans (in hardware) to generate hashes to detect errors
- Monitoring accesses to a region of an integrated circuit chip - monitoring internal chip transaction to spot security access right breaches
- Performance profiling - signature analysis algorithm
- Hardware based sensor analysis - method of monitoring messages from sensors, comparing hashes and taking corrective action if required.

SIEMENS

Thank You

SIEMENS

Contact

Published by Siemens Lee Harrison

Lee Harrison
Tessent
Rivergate, Newbury
Berkshire
UK

Phone +447810757413

E-mail lee.Harrison@siemens.com

SIEMENS