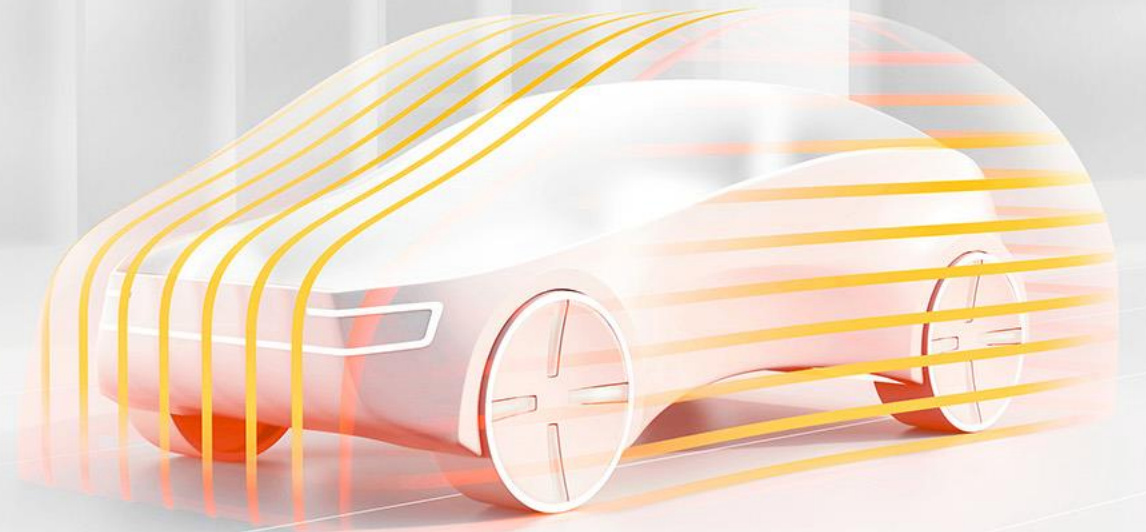


FUTURE CONNECTIVITY & IN-VEHICLE CYBERSECURITY: KNOW YOUR RIGHTS

Fighting on Two Fronts



GILAD BANDEL

VP Product and Marketing

Arilou Automotive Cybersecurity

Gilad.Bandel@nng.com

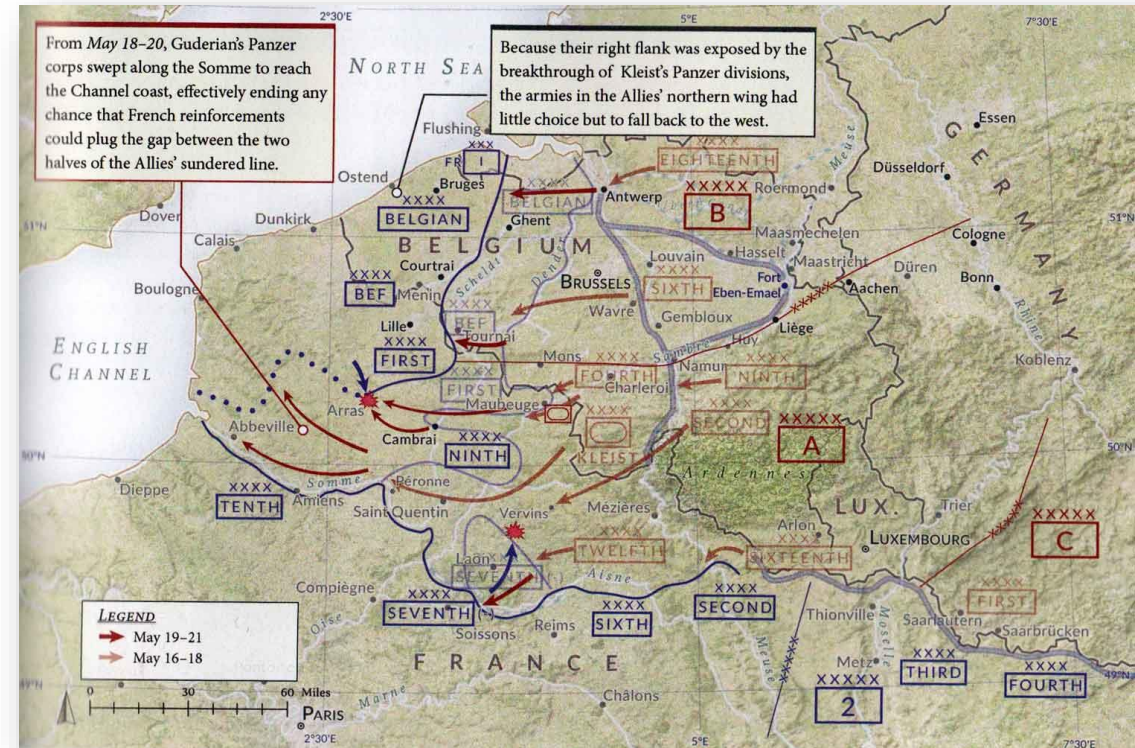


**CENTER FOR
AUTOMOTIVE
RESEARCH**




AGENDA

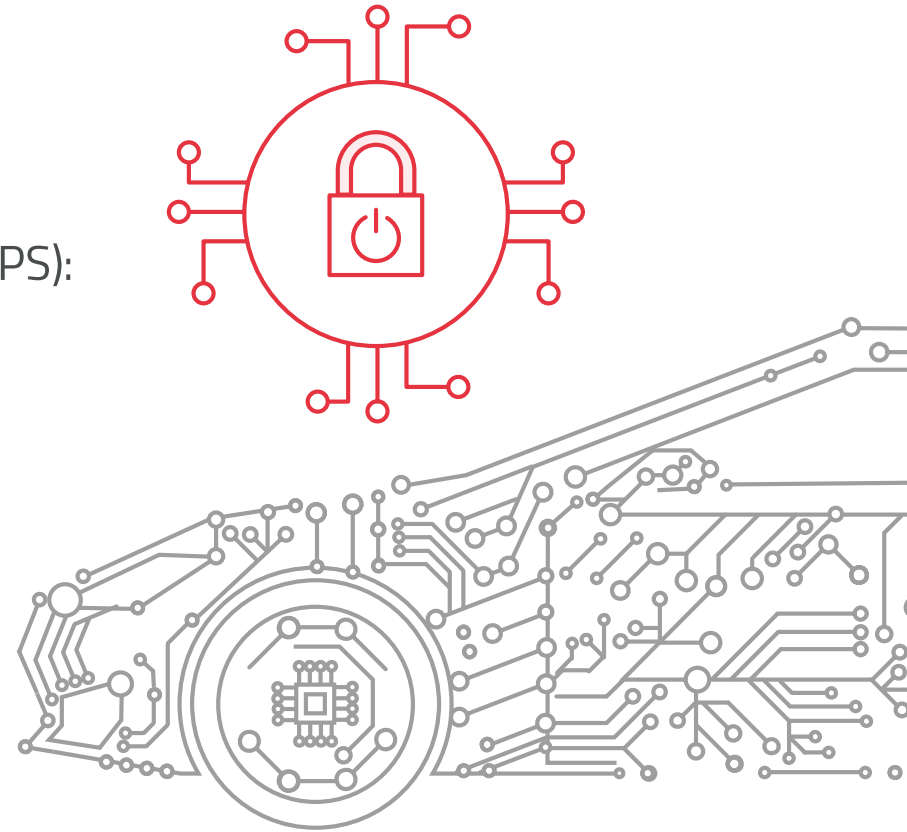
- Influencing factors
- Strategy
- Homeland security
- Fighting on two fronts
- Embedded positions
- Decisive tactics
- Debrief



ARILOU AUTOMOTIVE CYBERSECURITY

Your trusted independent security partner

- Automotive cybersecurity pioneer since 2012
- Independent member of global automotive software supplier,
 Group since 2016
- **SENTINEL** – Firewall & Intrusion Detection/Prevention Systems (IDS/IPS):
 - **SENTINEL-ETH** – IDS/IPS for Automotive Ethernet
 - **SENTINEL-CAN** – IDS/IPS for CANbus and SAE J1939 commercial vehicles
- **Secure Boot for ECUs**
- **Professional services:**
 - **ISO/SAE 21434** – Consulting for compliance
 - **TARA** – Automotive Threat Analysis & Risk Assessment



01

IVI (IN-VEHICLE INFOTAINMENT) CYBERSECURITY

Influencing factors



INFLUENCING FACTORS

Growing concern

INDUSTRY DYNAMICS GENERATE MANY BENEFITS BUT ALSO SHORTCOMINGS

- Connected vehicles create safer and comfortable driving experience
- Cyber risks to safety, reliability, and privacy
- Industry strives to prevent hackers from inflicting damages
- Regulation require OEMs to comply with cybersecurity standards
- Example of IVI (In-Vehicle Infotainment) system protection for homologation



02

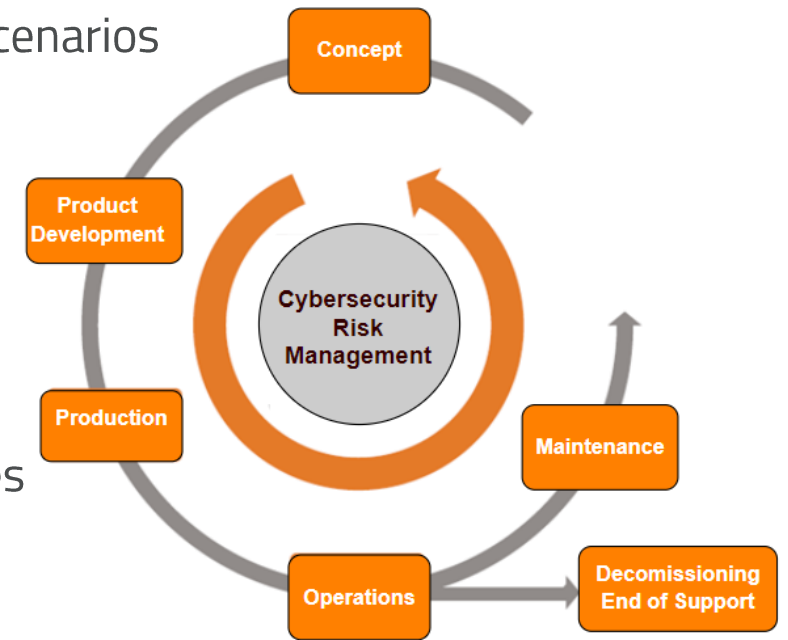
IVI CYBERSECURITY

Strategy



ISO/SAE 21434 COMPLIANCE PROCESS

- Cybersecurity culture – adopt cybersecurity awareness for all processes
- Cybersecurity concept – assets classification, attack paths, damage scenarios
- TARA – **T**hreat **a**nalysis and **R**isk **a**ssessment
- CAL – set the **Cybersecurity Assurance Level** – select risks to handle
- Product development – based on CAL and according to V Model
- Validation – demonstrate cybersecurity implementation
- Production – control plan with all cybersecurity measures
- Operation and Maintenance – support, incident mitigation and updates
- End of support – and decommissioning of the vehicle



ISO/SAE 21434 logical Cybersecurity activities – throughout vehicle lifecycle



AUTOMOTIVE THREAT ANALYSIS AND RISK ASSESSMENT (TARA)

Analyze the current and planned automotive cyber-security posture to evaluate vehicle cyber-security maturity

Document

- Risks
- Weak points
- Vulnerabilities
- Exposures
- Predicted attack vectors
- Kill chains

Sorted by severity and probability

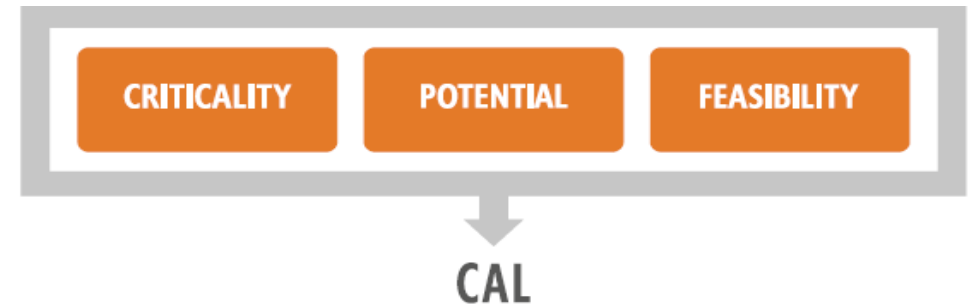
Generate a prioritized and optimized plan for risk reduction using improved

- Cyber-security architecture
- Design
- Components
- Intrusion detection/prevention
- Endpoint protection
- Cloud security

Risk probability	RISK SEVERITY				
	Catastrophic A	Hazardous B	Major C	Minor D	Negligible E
Frequent 5	6A	5B	5C	5D	5E
Occasional 4	4A	4B	4C	4D	4E
Remote 3	3A	3B	3C	3D	3E
Improbable 2	2A	2B	2C	2D	2E
Extremely improbable 1	1A	1B	1C	1D	1E

CAL (CYBERSECURITY ASSURANCE LEVEL) DETERMINATION

- CAL classification determines the level of rigor with which cybersecurity activities are performed
- CAL, need to know an impact, attack vector and feasibility, deriving from the ISO 26262 standard:
 - ✓ Impact rating
 - ✓ Risk-based approach
 - ✓ Independence of cybersecurity assessment
- A CAL can be used to select methods:
 - ✓ For development and verification;
 - ✓ To identify and analyze vulnerabilities;
 - ✓ For cybersecurity assessment.



		Attack Vector			
		Physical	Local	Adjacent	Network
Impact	Negligible	-	-	-	-
	Moderate	CAL1	CAL1	CAL2	CAL3
	Major	CAL1	CAL2	CAL3	CAL4
	Severe	CAL2	CAL3	CAL4	CAL4

03

IVI CYBERSECURITY

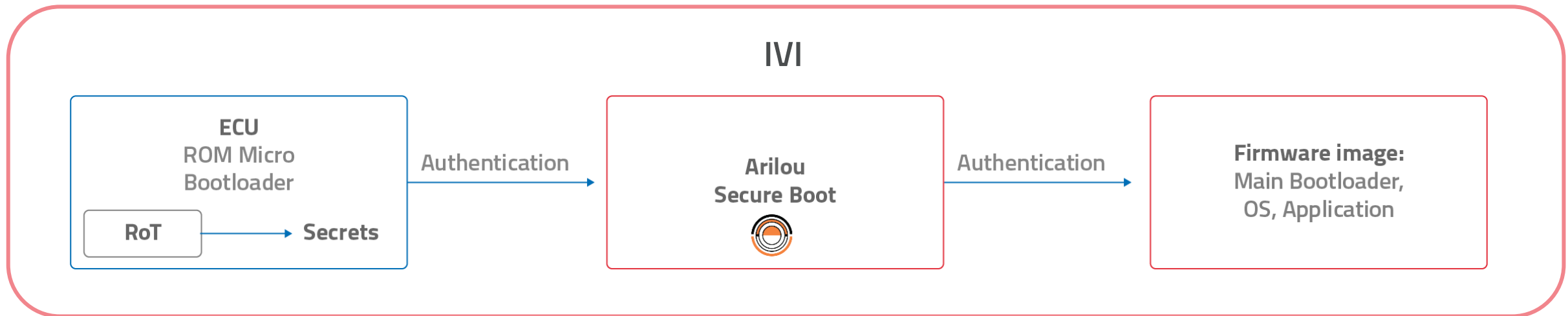
Homeland security



SECURE-BOOT

Chain-of-Trust

- Hackers might attempt to load their rouge software on to the IVI
- Digital rights might be infringed: such as unlicensed pirate software or copied maps
- The ROM micro-bootloader authenticates the Arilou Secure Boot, and boots it
- Arilou Secure Boot authenticates the OS (Operating System) header and image, and boots it



04

IVI CYBERSECURITY

Fighting on two fronts



IN-VEHICLE INFOTAINMENT (IVI) CYBERSECURITY

Fighting on two fronts

THE IVI IS VULNERABLE ON TWO FRONTS

It is a gateway between the external world and the In-Vehicle Network (IVN)



1. Attackable remotely via the cellular network.
2. Attackable via the IVN and attacking the IVN.



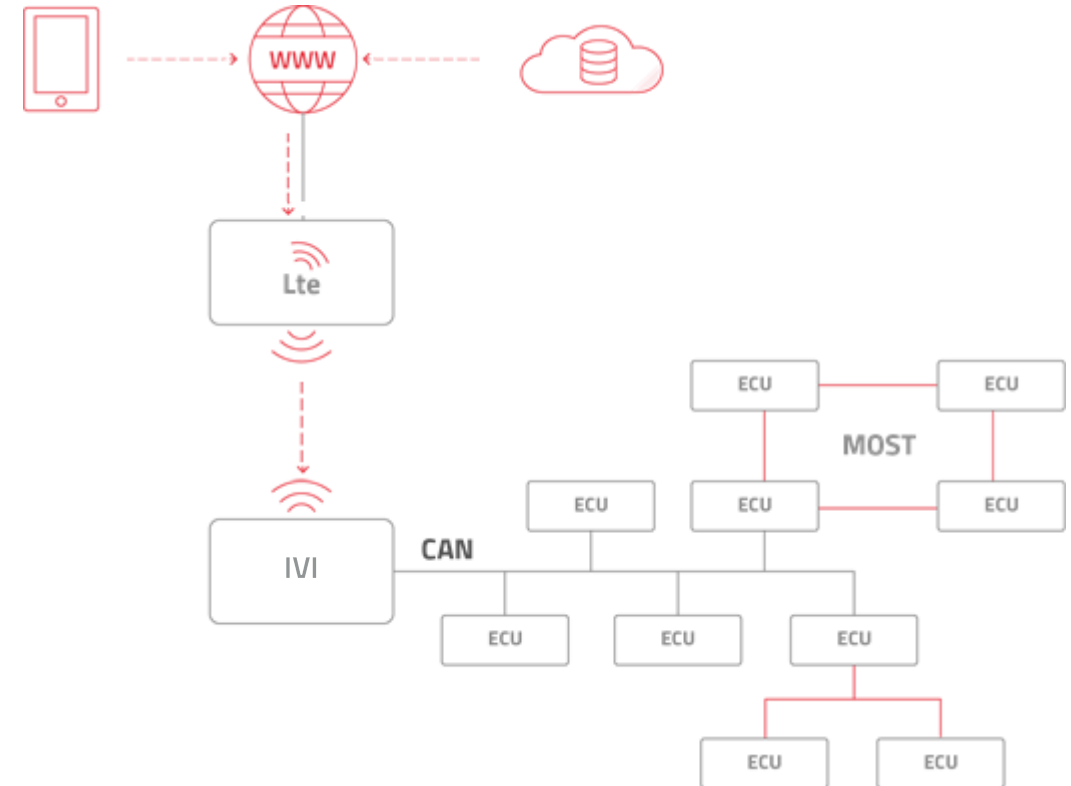
The 28th North Gloucestershire Regiment face off against Napoleonic forces on two fronts

IVI CYBERSECURITY

A Mobile Enemy (First Front)

REMOTE ATTACKS ARE THE MOST SEVERE THREAT TO THE VEHICLE

- External Cellular
 - Incoming traffic from the cellular network
 - Outgoing traffic to the cellular network

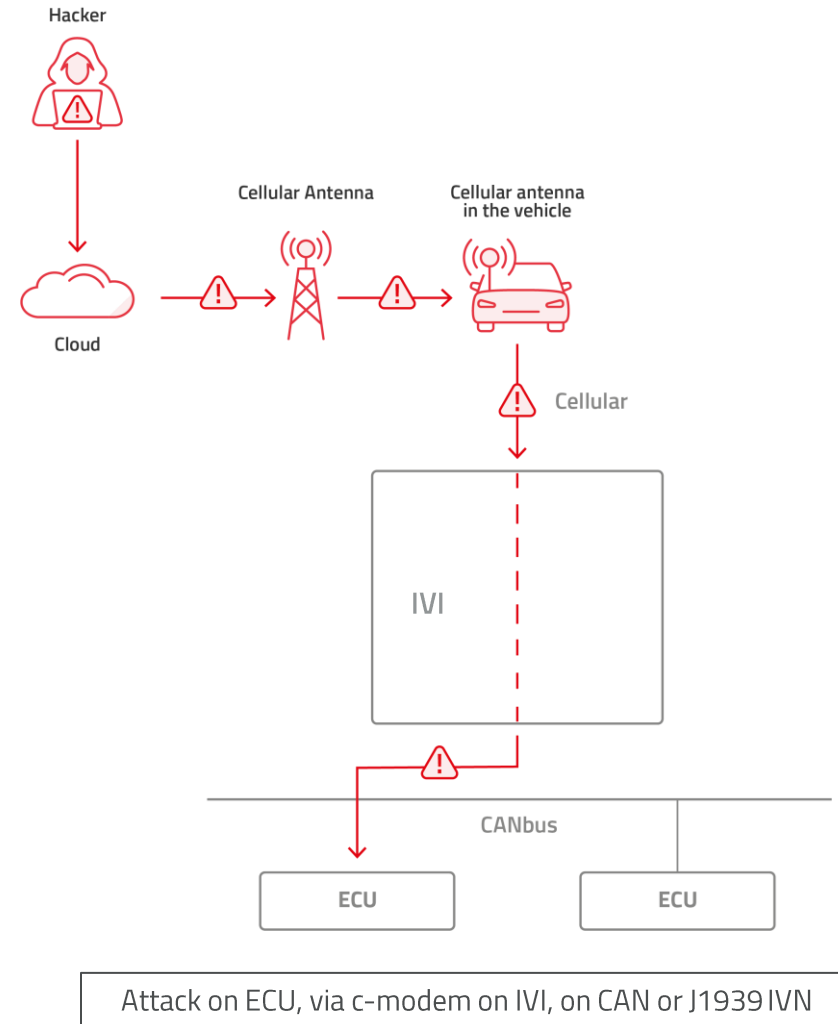


IVI CYBERSECURITY

In the Trenches (Second Front)

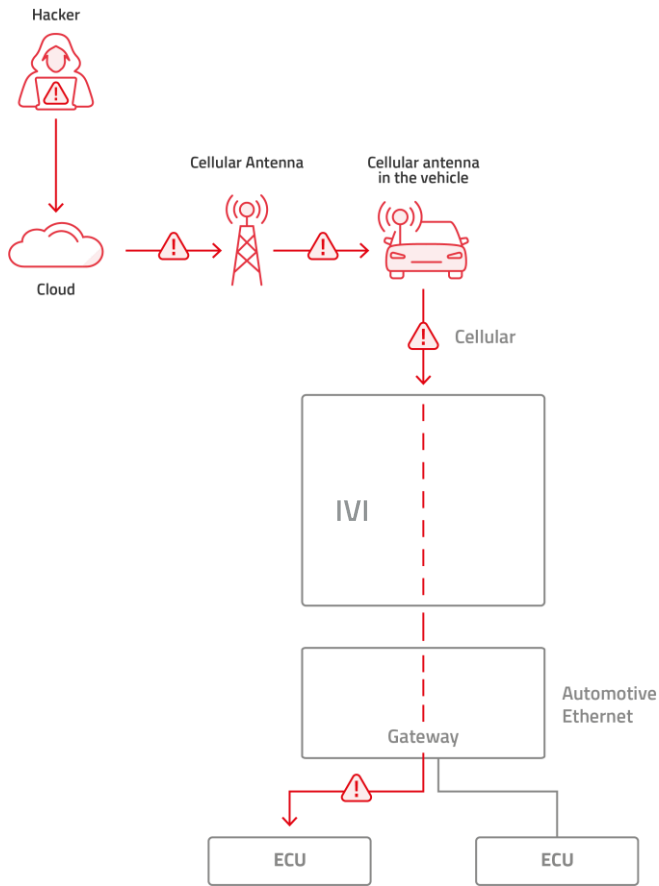
IVNS ARE A COMMON TARGET USED TO ACCESS ECUS (ELECTRONIC CONTROL UNIT)

- Incoming traffic from the IVN
 - IVI is the target
 - A step in the kill chain
 - Using the IVI as a relay
- Outgoing traffic to the IVN
 - Destination is another ECU
 - Central Gateway, rather than IVI has cellular-modem
 - IVI and Central Gateway are combined

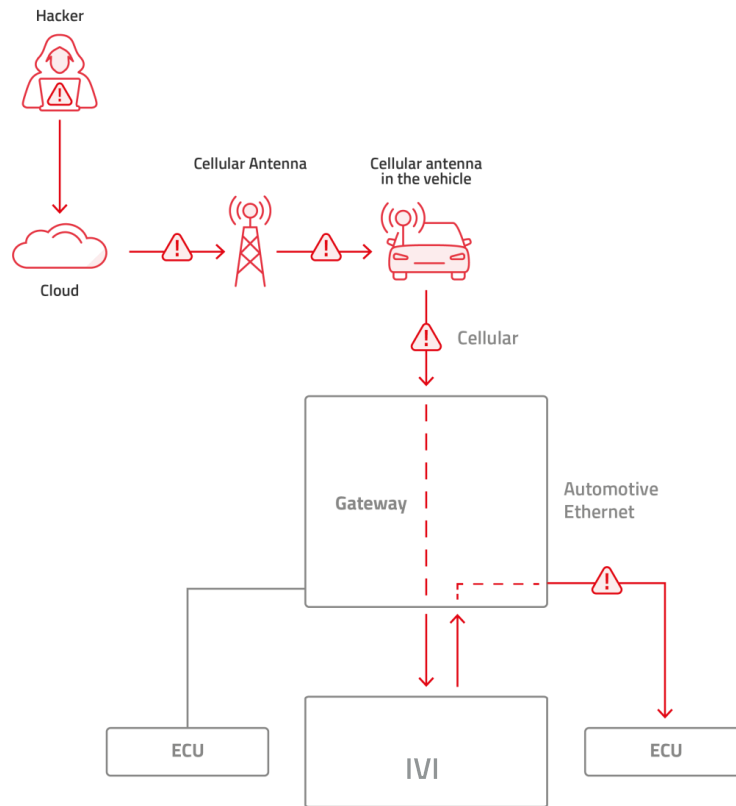


MORE ATTACK VECTORS

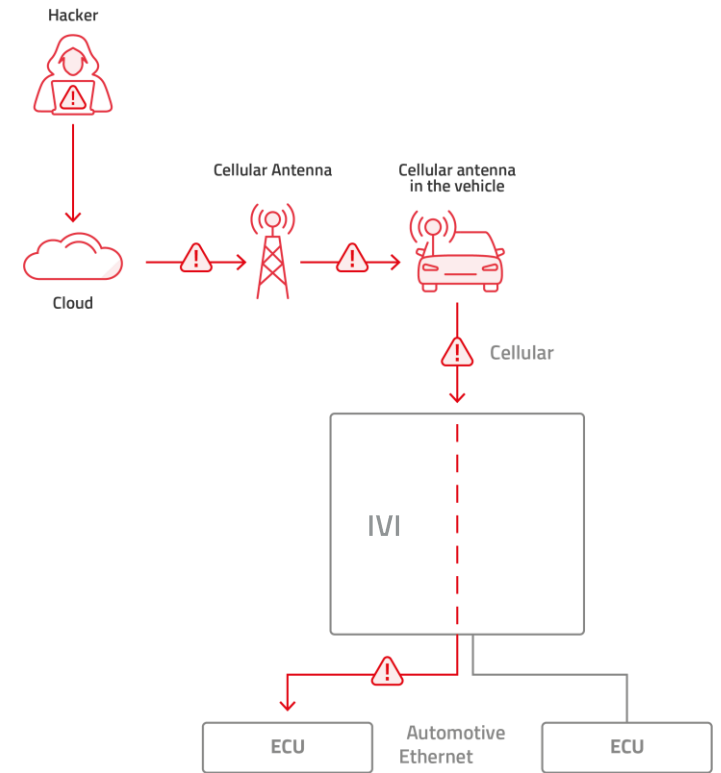
In the Trenches



Attack on ECU, via c-modem on IVI, on Ethernet IVN



Attack on ECU and IVI, via c-modem on GW, on Ethernet IVN

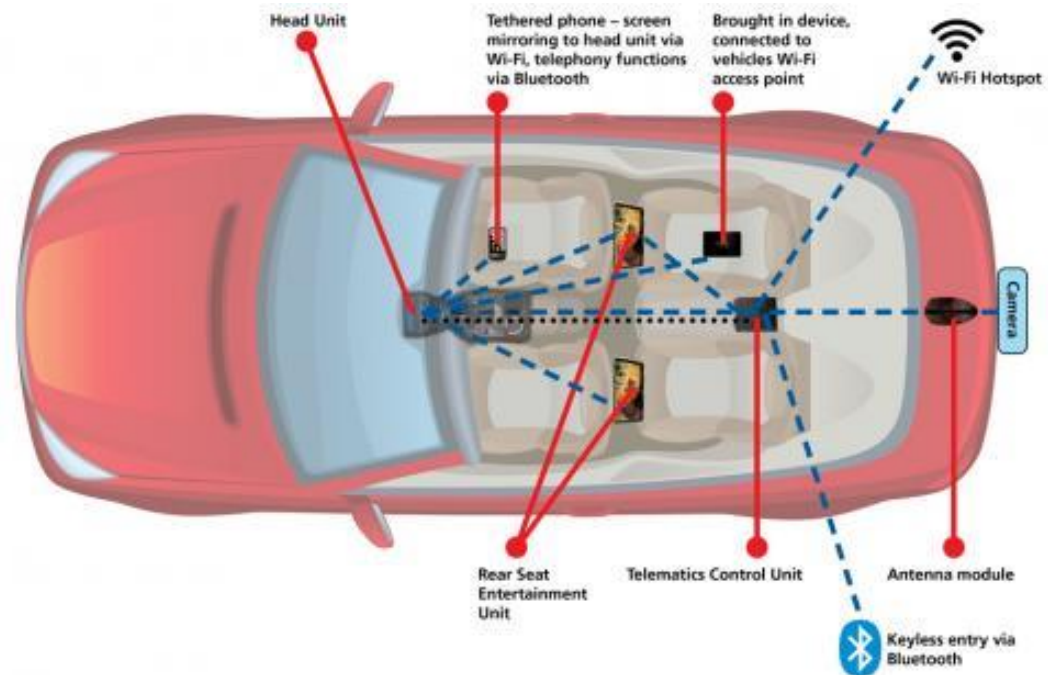


Attack on ECU, via c-modem on IVI, on Ethernet IVN

BLUETOOTH AND WI-FI

In the Trenches

- The IVI has additional connectivity:
 - Bluetooth with mobile phone that can be used as a tool to attack the IVI and the vehicle
 - Wi-Fi as a hotspot can be used as a tool to attack the IVI and the vehicle



EVENTS HISTORY

Chronic of enemy achievements



- 2010 – Using the remotely controlled immobilizer system, over 100 cars were grounded in Texas, US using insider privileges
- 2014 – Arilou gains access to major OEM vehicle network using through the IVI, gaining control over hundreds thousands of vehicles (telnet port, SMS BoF, open AT commands interface and more)
- 2016 – Gaining control over connected car service through vulnerabilities found in the web portal enabling locking, unlocking, taking over the vehicle, etc.
- 2019 - Thousand of user accounts hacked through GPS tracking application using brute force attack enabling location tracing, shutting the engine while the vehicle in on the move, etc.
- 2019 – Hardcoded credentials vulnerability in thousands of cars exposing them to attacks enabling private information retrieval from the vehicle
- 2020 – Leaked credentials of OEM internal systems create channel to inject malware to be later used for malicious activities creating a cascading effect.

05

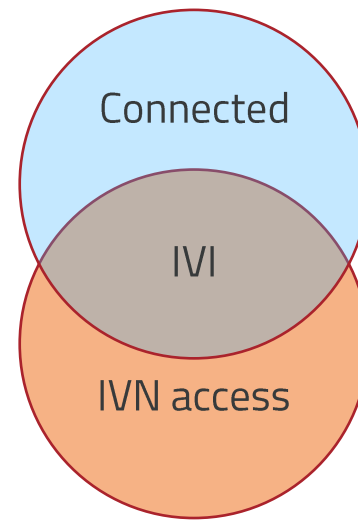
IVI CYBERSECURITY

Embedded Positions



IVI CYBERSECURITY

Embedded Positions



THE IVI IS VULNERABLE TO RISKS RELEVANT TO ANY EMBEDDED DEVICE

- Over 50% of the vehicle vulnerabilities detected in the IVI
- Legacy system developed over many years with multiple layers for code and patches
- Compromised boot sequence
 - Old or unsecure flash image. Embedded malware
- Tampered storage
 - Modified SW modules or data can be loaded
- Firmware update from rogue source
 - Includes code that will cause malfunction or allow remote control
- Vulnerability and exposure opportunism (BOF - Buffer overflow or open port)
 - Causes IVI misbehaviour
- Automotive Ethernet IVN (using IP) increases the chance of remote attacks on connected ECUs
- Aftermarket device in some cases without OEM control

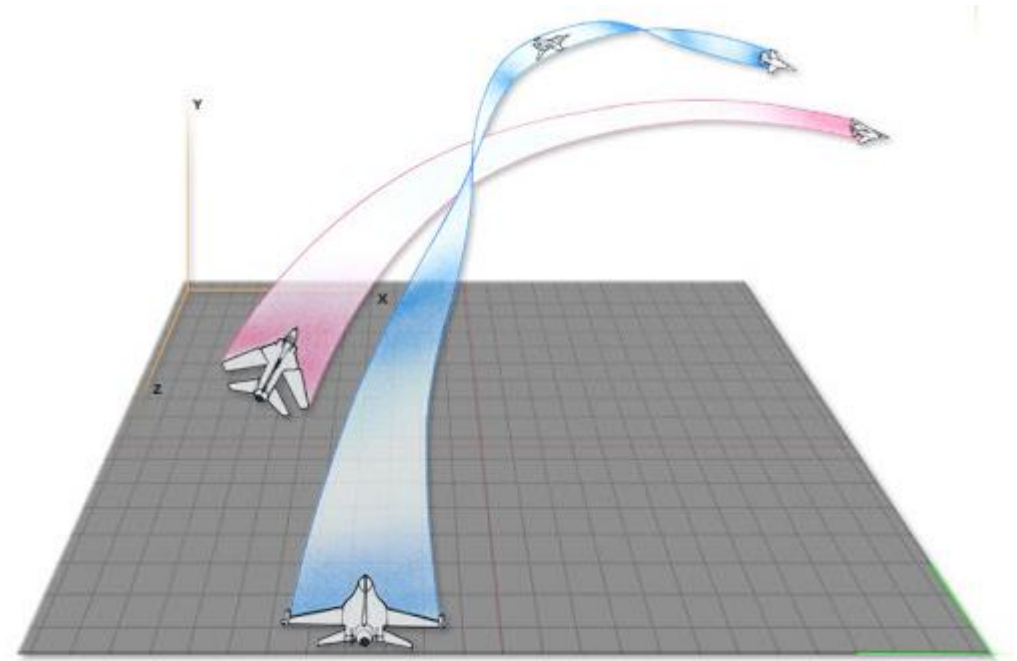
IVI CYBERSECURITY

Embedded Positions

DEFENSIVE MANEUVERS

There are numerous reasons to secure the IVI

- **The most targeted ECU**
 - On CAN, attacker needs to switch protocol
 - On Ethernet, IP is used end-to-end
- **Global Regulation**
 - UNECE WP.29 (UNR 155) and equivalent in non-participating countries
- **Brand/Reputation Damage**
 - Mainly to OEM



IVI CYBERSECURITY

Embedded Positions

A SUITABLE ARSENAL

Use TARA to determine the most effective response.

- **Secure by Design, Development Process and Hardening (SW & HW)**
- **Link protection between server and endpoint, P2P prevention**
- **Endpoint Detection and Response (EDR)**
 - Private APN
 - Secure Boot, Secure Module Loading
 - Host Intrusion Detection System (HIDS)
- **Network Intrusion Detection/Prevention System (NIDS/NIPS)**
 - Message Format, Field Value Range, Change of Rate Values, Periodic Messages, Correlation between signals, Vehicle Context, Authentication Failure, Media Access Control (MAC), Excessive Message Rate



06

IVI CYBERSECURITY

Decisive Tactics

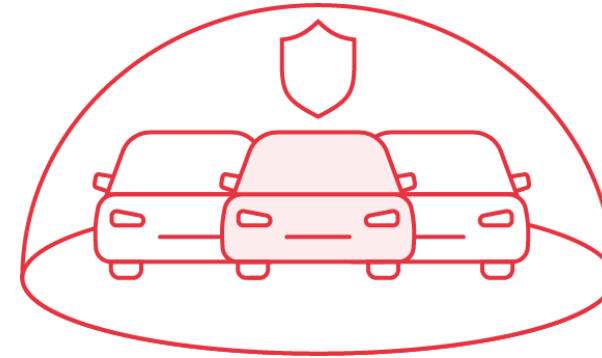


IVI CYBERSECURITY

Decisive Tactics

IDS/IPS IS VITAL TO VEHICLE CYBERSECURITY

It is the only vehicle component dedicated to cybersecurity protection.



- **IDS (Intrusion Detection System)**

- **Detection and reporting (only)**

- **SIEM** (Security Information and Event Management) ==>
 - **VSOC** (Vehicle Security Operations Center) ==>
 - **CERT** (Cyber Emergency Response Team)

- **IPS (Intrusion Prevention System)**

- **Stop attacks by taking intrusive actions**

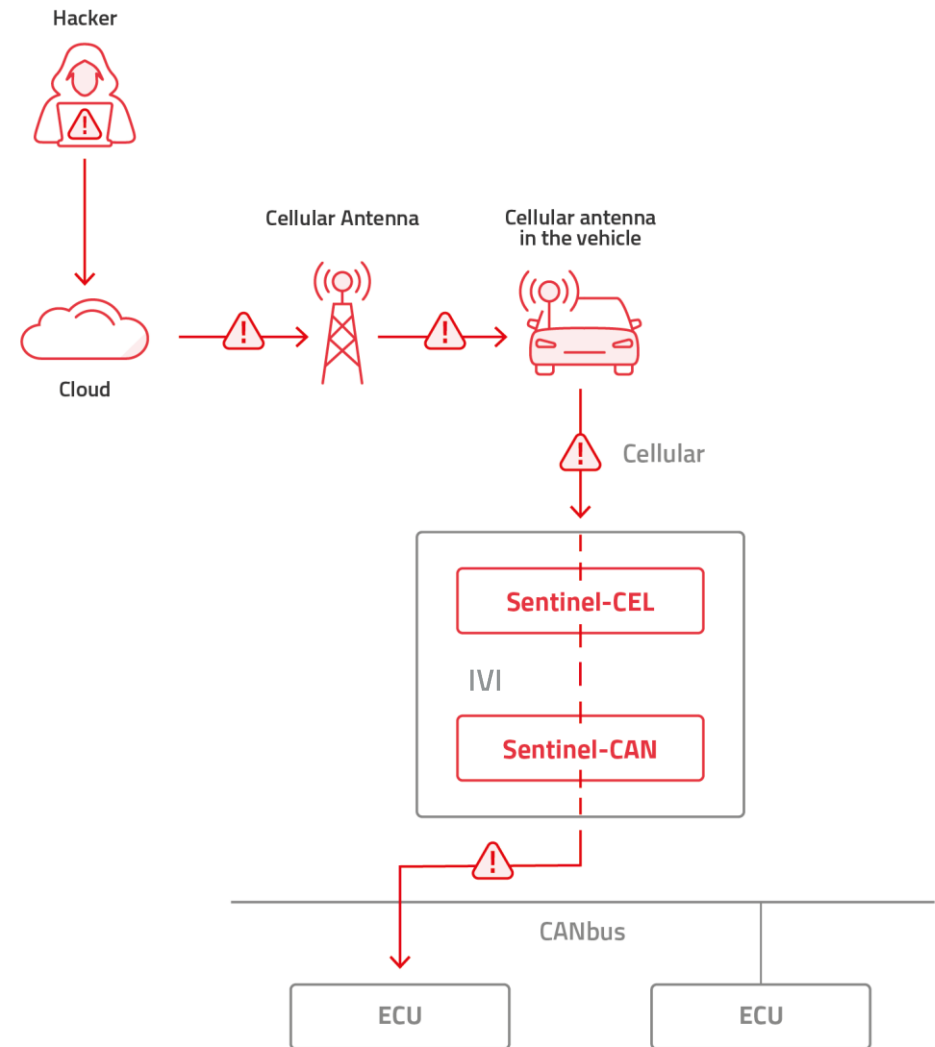
- Dropping frames
 - Disabling offending components
 - Excluding non essential components

IVI CYBERSECURITY

Decisive Tactics

INSPECTING THE CELLULAR – INCOMING TRAFFIC

Incoming traffic from the cellular to the IVI should be inspected, in case the IVI is the target or used as a bridge to the IVN.

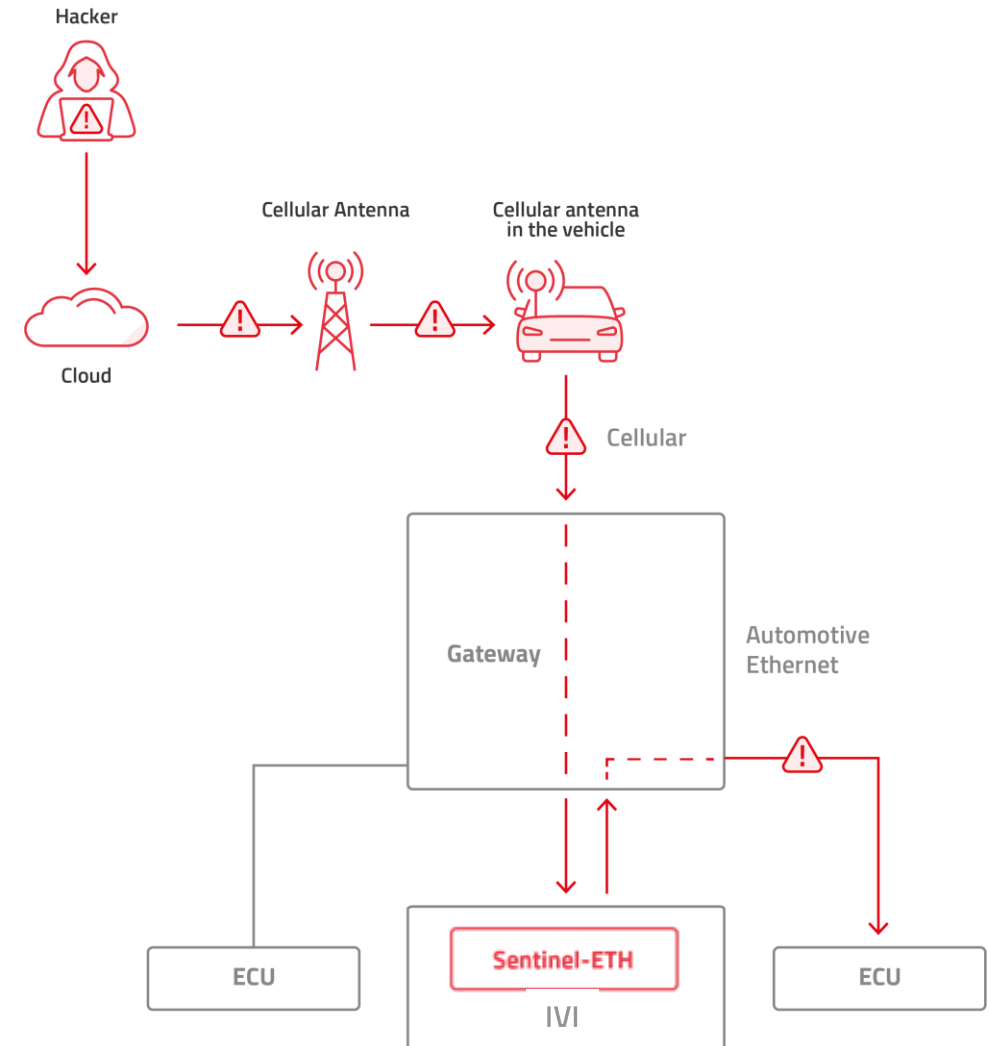


IVI CYBERSECURITY

Decisive Tactics

INSPECTING THE IVN TRAFFIC – INCOMING AND OUTGOING TRAFFIC

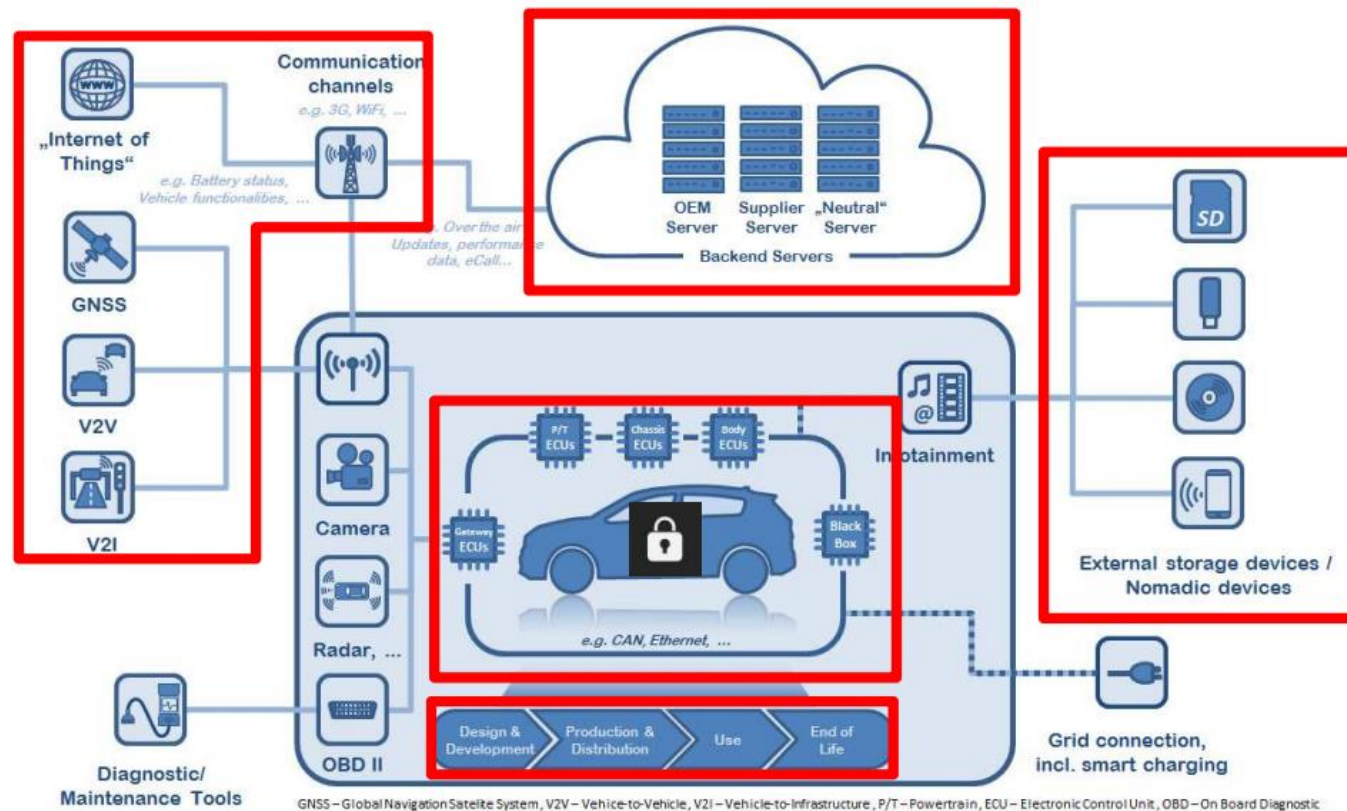
Incoming and outgoing traffic from between the IVI and the IVN should be inspected.



BLUETOOTH AND WI-FI PROTECTION

Decisive Tactics

- Bluetooth incoming traffic inspection for attack attempts detection
- Wi-Fi incoming traffic inspection for attack attempts detection



GNSS – Global Navigation Satellite System, V2V – Vehicle-to-Vehicle, V2I – Vehicle-to-Infrastructure, P/T – Powertrain, ECU – Electronic Control Unit, OBID – On Board Diagnostic

06

IVI CYBERSECURITY

Debrief



IVI CYBERSECURITY

Debrief

THE IVI IS A CONNECTED DEVICE

The IVI interfaces both the outside world and the in-vehicle network.

- It should be well protected!

Interface	CANbus/ Ethernet	Direction	Cellular Modem	Detection/ Prevention	Implementation	Importance
Cellular	Not relevant	Incoming	Yes	Both	IVI	Very High
Cellular	Not relevant	Outgoing	Yes	Both	IVI	Low
Cellular	Not relevant	Incoming	No	Both	IVI/GW	Critical
Cellular	Not relevant	Outgoing	No	Both	IVI/GW	Low
In-Vehicle	CANbus	Incoming	Both	Detection	IVI/GW	High
In-Vehicle	CANbus	Outgoing	Both	Detection	IVI/GW	Very High
In-Vehicle	CANbus	Incoming	Both	Prevention	IVI	High
In-Vehicle	CANbus	Outgoing	Both	Prevention	IVI	Very High
In-Vehicle	Ethernet	Incoming	Yes	Both	IVI/GW	High
In-Vehicle	Ethernet	Outgoing	Yes	Both	IVI/GW	Very High
In-Vehicle	Ethernet	Incoming	No	Both	IVI/GW	Critical
In-Vehicle	Ethernet	Outgoing	No	Both	IVI/GW	Very High

LIVE DEMO



For a live demo please contact us at

Gilad.Bandel@nng.com

TAKE HOME MESSAGES

Debrief

- Tier-1's and OEMs need to implement proper security measures if they are to protect the vehicle and IVI from dangerous attacks
- Several methods needs to be employed for a robust, defense in depths multi layer protection approach
- Methodologies such as secure by design, network segregation, secured software development process, supply chain assurance, etc.
- Secure boot protects the authenticity of the software and data used
- The IDS/IPS is the only dedicated, devoted and independent component aimed at the vehicle cybersecurity protection
- **For more information, please see our web site <https://ariloutech.com/>**
- **Please follow us on LinkedIn <https://www.linkedin.com/company/arilou/>**





ARILOU

Automotive Cybersecurity
Part of NNG Group

THANK YOU FOR YOUR ATTENTION

GILAD BANDEL

VP Product and Marketing

Email: Gilad.Bandel@nng.com

Tel: +972 (54) 246-0006

Website: www.ariloutech.com

