ARGUS
CYBER SECURITY

TechShow 2021

Securing Connected Modules

Monique Lance, Argus Cyber Security

June 2021

No One is Safe From Cyber Attacks

TechShow 2021

Government

- NASA
- FORMIN.FINLAND.FI — MINISTRY FOR FOREIGN AFFAIRS OF FINLAND
- THE PENTAGON WASHINGTON D.C.
- सत्यमेव जयते — Government of India

International

- INTERNATIONAL OLYMPIC COMMITTEE
- United Nations
- G - 20
- INTERNATIONAL MONETARY FUND

Technology

- Yahoo!
- Google
- Adobe
- Microsoft
- ebay

Infrastructure

Technology

- Apple
- SONY
- NORTEL

Automotive

- MITSUBISHI
- HONDA
- BMW
- UBER
- RENAULT
- NISSAN
- AUDI
- VW
- TESLA

Financial

- EQUIFAX
- Morgan Stanley
- MT.GOX
- WELLS FARGO

Media

- AP Associated Press
- THE WALL STREET JOURNAL.

Cyber Security

- RSA
- KASPERSKY lab
- FireEye
- symantec.

Defense

- BOEING
- LOCKHEED MARTIN

ARGUS CYBER SECURITY

What Can a Hacker Do?

Steal sensitive data from connected components

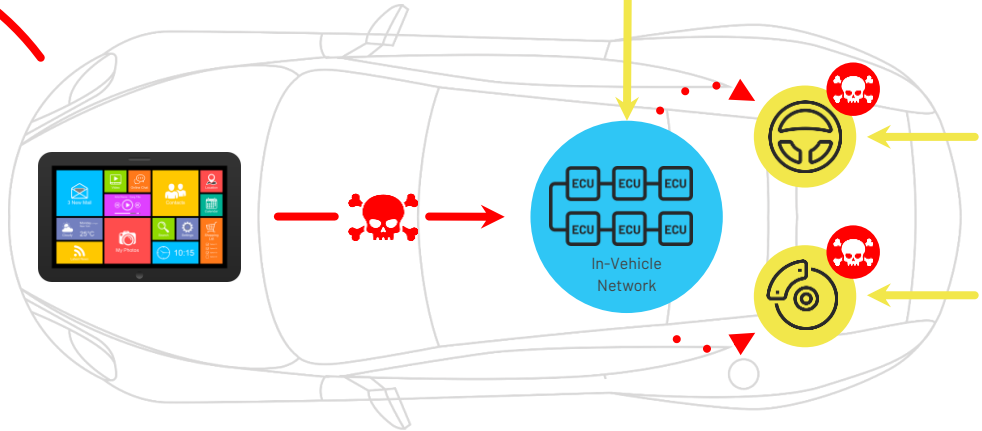
Access in-vehicle network to disrupt vehicle operation

Scan for open ports

Perform man in the middle attack

Exploit a vulnerability (logical or implementation)

...



Manipulate steering

Manipulate brakes

Tesla Hacked by a Drone

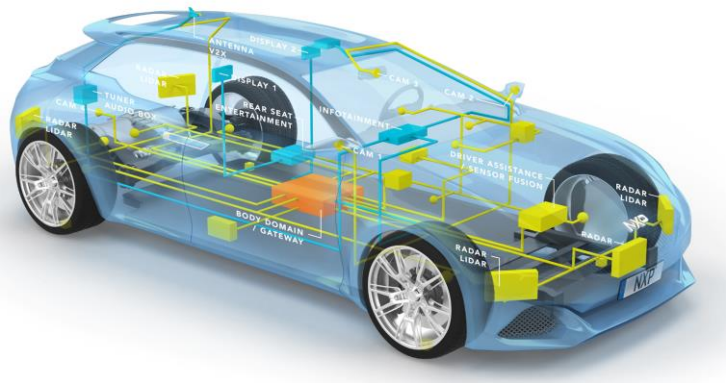
Attack via Wi-Fi from a distance of up to 100 meters (roughly 300 feet)

- From a drone a hacker could:
  - Open doors
  - Change seat positions
  - Play music
  - Control the air conditioning
  - Modify steering and acceleration modes

Source

Modern Vehicles Becoming Increasingly Vulnerable

- More and more software than ever before
- Connectivity on the rise
  - Telematics, GW, ADAS, Infotainment, in-vehicle service based communication
  - Increase in Android systems
- High Performance Computer (HPC) Architecture
- Trend to autonomous vehicles



Changes Introduce New Risks!!!

OEMs Speak Out: CEO, GM

TechShow 2021

> ...Cybersecurity is a systemic concern for our industry...this collaboration among carmakers is important because a critical breach at one company will impact the entire industry.

Mary Barra, February, 2020

ARGUS CYBER SECURITY

In Recognition of Seriousness of the Threat

June 2020, UNECE passed regulation mandating automotive cyber security, also known as UNR 155.

United Nations ECE/TRANS/WP.29/2020/79 REVISED

Economic and Social Council

Distr.: General
23 June 2020

Original: English

Economic Commission for Europe

Inland Transport Committee

World Forum for Harmonization of V[illegible]

Proposal f[illegible] Regulation [illegible] form provisions concer[illegible] regards to cyber se[illegible] and [illegible] management system

Submitte[illegible] the W[illegible] on Automated/autonomous and [illegible]nected vehicle[illegible]

[illegible] reproduced below is consolidated version of the draft UN Regulation on Cy[illegible]ity and Cyber Security Management Systems. This informal version is meant pure[illegible] as documentation tool. The authentic text submitted for adoption is contained in the three documents ECE/TRANS/WP.29/2020/79, ECE/TRANS/WP.29/2020/94 and ECE/TRANS/WP.29/2020/97.

APPROVED

"ECE-TRANS-WP29-2020-079-Revised"

UNR 155 Implementation Milestones

Apr: UN Regulations applied to L3 & L4 vehicles** into force*

Nov: UN Regulations applied to all OTA capable vehicles in Japan** into force*

Jan: UN Regulation entry into force*

Jul: Japan & EU entry into force**

Jul: End of transition (no more "adequate CSMS" or appropriate "annex 5 alternatives")

JUNE 2020 | 2021 | 2022 | 2023 | 2024

* Industry expectation
** Japan Ministry of Land, Infrastructure, Transport and Touring (MLIT)
** European Union "General Safety Regulation" (GSR) (Regulation (EU) 2019/2144)

UNR 155 Key Provisions

- 7.2.2.2. (d): "...the risks identified ***are appropriately managed***."
- 7.2.2.2. (g): "...***monitor for***, detect and ***respond*** to cyber-attacks, threats and vulnerabilities..."
- 7.2.2.3: "...vulnerabilities which require a response...shall be mitigated ***within a reasonable timeframe***."
- 7.3.7 (a): "...and ***prevent cyber-attacks*** against vehicles..."
- 7.4.1: "...mitigations implemented are ***still effective***..."
- 7.4.2.: "...require the vehicle manufacturer to ***remedy any detected ineffectiveness***."

The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that, based on categorization referred to in paragraph 7.2.2.2 (c) and 7.2.2.2 (g), cyber threats and vulnerabilities which require a response from the vehicle manufacturer shall be mitigated within a reasonable timeframe.

(g) The processes used to monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities on vehicle types and the processes used to assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified.

(h) The processes used to provide relevant data to support analysis of attempted or successful cyber-attacks.

The vehicle manufacturer shall report at least once a year, or more frequently if relevant, to the Approval Authority or the Technical Service the outcome of their monitoring activities, as defined in paragraph 7.2.2.2.(g)), this shall include relevant information on new cyber-attacks. The vehicle manufacturer shall also report and confirm to the Approval Authority or the Technical Service that the cyber security mitigations implemented for their vehicle types are still effective and any additional actions taken.

The Approval Authority or the Technical Service shall verify the provided information and, if necessary, require the vehicle manufacturer to remedy any detected ineffectiveness.

If the reporting or response is not sufficient the Approval Authority may decide to withdraw the CSMS in compliance with paragraph 6.8.

(b) The processes used for the identification of risks to vehicle types. Within these processes, the threats in Annex 5, Part A, and other relevant threats shall be considered;

(c) The processes used for the assessment, categorization and treatment of the risks identified;

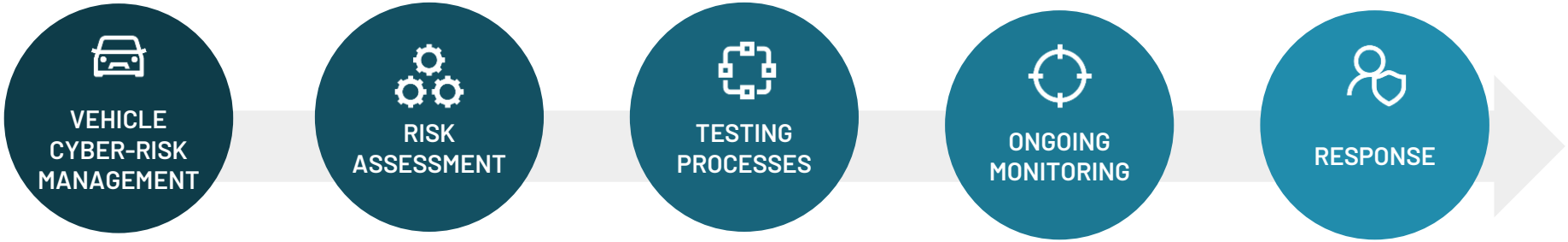
(d) The processes in place to verify that the risks identified are appropriately managed;

The vehicle manufacturer shall implement measures for the vehicle type to:

(a) detect and prevent cyber-attacks against vehicles of the vehicle type;

What does it mean for the OEM

CSMS Main Processes



Risk management throughout the product lifecycle

Exhaustive process of identification, assessment, categorization and treatment of risks

Cybersecurity resilience through validation testing

Supply-chain, development, production and in the field

Capabilities detection, monitoring and rapid response and recovery

Consulting Services & Technology

TechShow 2021

Development
The period before the vehicle type is approved for registration and use in road traffic

Production
The period in which the vehicle type is manufactured and there are new registrations for use in road traffic

Post-production
The period in which a vehicle type is no longer produced and there are no operational vehicles of a specific vehicle type

Overall & Project Dependent CS Management

- Cyber security planning
- Cyber security governance, training & culture
- Self-assessment audit

CS Management System

- Gap analysis
- Process definition & implementation
- Cyber security monitoring, event assessment & incident response
- Strategy & management consulting
- Vulnerability management

Risk assessment, security concept & security validation

- Threat analysis & risk assessment
- Security concept & requirements
- Technology solutions
- Technology consulting & engineering services
- Validation testing - penetration testing, code review

ARGUS CYBER SECURITY


Safe and Dynamic Driving
towards VISION ZERO
ZERO CRASHES
ZERO INJURIES
ZERO FATALITIES
Plan
Sense
Act

Argus at a Glance

TechShow 2021

65+ million vehicles will be secured with Argus technology starting 2021 across **14 production projects, 10 manufacturers**

Reducing cyber security cost and complexity with **reusable software and direct OEM engagement**

300 man years invested to date in Argus technologies

70 granted and pending automotive cyber security patents

Seamless integration across product portfolio

Partnerships with leading industry players

Deloitte. NXP Microsoft T··Systems·

~200 employees with Worldwide officers in: **Korea, Japan, Germany, France, USA**

Automotive grade - **ASIL-B ready** and developed in alignment with **ASPICE Level 2** requirements

ARGUS CYBER SECURITY

Demand for End-to-End Cyber Security

TechShow 2021

ARGUS
CYBER SECURITY

Prevent

Make it as hard as possible to attack

Detect & Understand

Detect when you are being hacked and how, in real time

Respond

Mitigate the damage and immunize the fleet

End-to-End Automotive Cyber Security

TechShow 2021

1 PREVENTION, DETECTION & RESPONSE

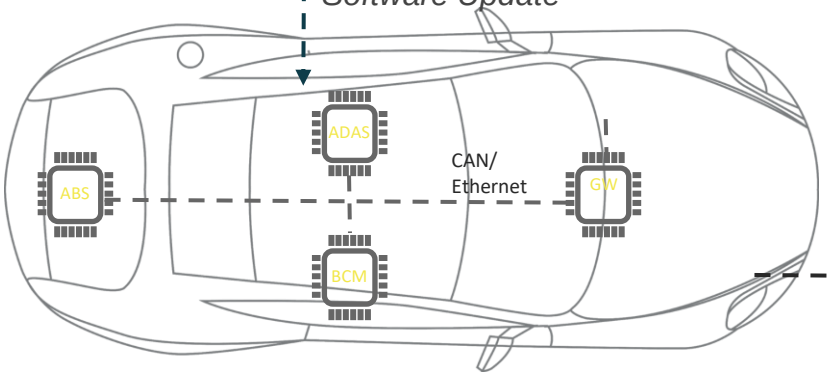
4 RESPONSE

Optional immediate response to attacks using master IDS

Security configuration update to hardening measuresor OTA Software Update

3 DETECTION, INVESTIGATION, MANAGEMENT

Vehicle SOC analysts analyse and manage the incident



2B

Vehicle data enriched with external data from connected ecosystem

2A LOGS & ALERTS

ARGUS CYBER SECURITY

Argus Services for UNR 155 Across the Vehicle Lifecycle

TechShow 2021

01 Cyber Security Management System (CSMS)

- CSMS Gap Analysis
- CSMS Process Definition

02 Vehicle Type Approval

- Type Approval Gap Analysis
- Threat Analysis & Risk Assessment (TARA)
- Recommended Security countermeasures
- Pentesting
- Security Testing (Validation)

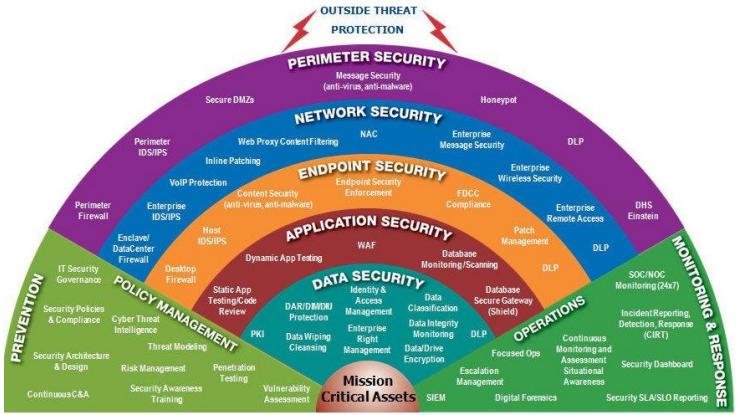
03 Cyber Security Governance

- Cybersecurity Training
- Technology Consulting
- Incident Response

ARGUS CYBER SECURITY

Staying Ahead of the Hackers

One of the first times in history of dynamics between attackers and defenders cyber security experts have the opportunity to establish **a Major Head Start**.



IT - Reactive

Automotive - Proactive

ARGUS CYBER SECURITY

TechShow 2021

THANK YOU

www.argus-sec.com

contact@argus-sec.com

ARGUS
CYBER SECURITY