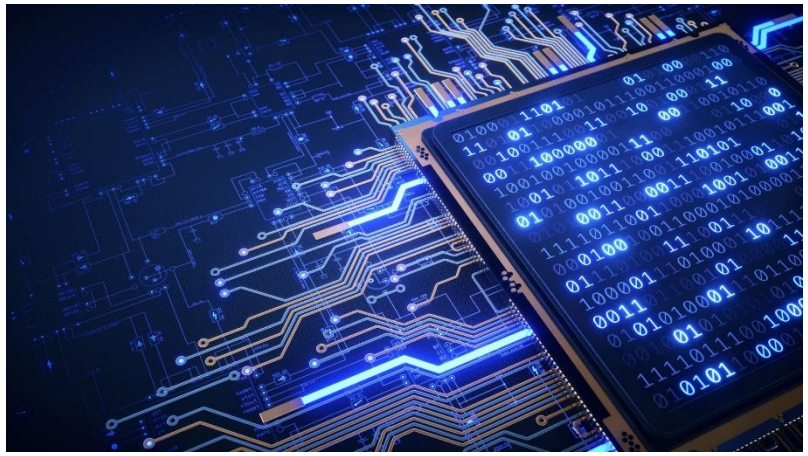
Driving Compliance – Global Automotive Cybersecurity Standards and Indian Regulations

ISO 21434, UNECE WP.29, ARAI 189/190

M M Desai-Deputy Director
ARAI, Pune

Agenda

- Introduction to ARAI
- Regulatory Mechanism in India
- Government of India’s Mission-CASE
- Auto Electronics, Connectivity & ITS in India
- CSMS & SUMS AIS standards
- India Specific Discussion
- Challenges



ARAI at a Glance

- Established in **1966** in Pune as a Society
- Affiliated to Ministry of Heavy Industries **(MHI), GoI**
- Recognized by DSIR as a Scientific Industrial Research Organization (**SIRO**)
- **16** specialized Auto Engg. Labs/ Depts
- **4** CoEs
- **1800 + B2B** Customers every year
- **675+** strong team
- Accredited for ISO **9001, 14001, 45001, 27001, 17025**

Service Portfolio

Regulatory Mechanism in India

Government of India

MORTH
Ministry of Road Transport & Highways

MOHI
Ministry of Heavy Industries

MOEF
Ministry of Environment & Forests

Ministry of Consumer Affairs

DGFT
Director General of Foreign Trade

State Ministries

Standardization

CMVR - Technical Standing Committee

Automotive Industry Standards Committee-AISC

Standing Committee on Emission Legislation – SCOE

Bureau of Indian Standards – BIS

Type Approval / Certification Agencies

ARAI
Automotive Research Association of India

Other testing agencies identified by Govt. of India

ARAI® Progress through Research

Automotive Electronics "Past and Present"

…Automobile is one of the fastest growing sectors in the world

Diodes, transistors, analog integrated circuits, and digital integrated circuits started to gain in vehicle applications
1960-1970

Electronic fuel ignition, came to meet tighter emission norms and to improve fuel economy.

Addition of Integrated circuits(IC) and microprocessors enabled vehicle features such as ABS, ECM, and climate control
1980

DSP & 32-bit µP added intelligent sensors, and large memory which enables powertrain/traction control, braking, steering and suspension, navigation, and OBD
1990

Computing power is now 40 times greater than what is was in 1975
2014

Today's vehicles contain three centuries of technology…19th century internal combustion engines…combined with 20th century electrical systems…and 21st century electronics….

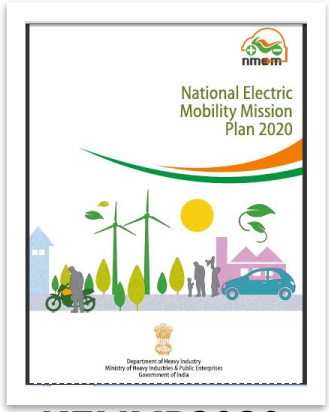
Today, from the front bumper to the back bumper, every system on a vehicle has electronics on it"

E-mobility-Government Initiatives

Ministry of Heavy Industries (MHI)

2011
National Mission on Electric Mobility (NMEM)

2013
National Electric Mobility Mission Plan 2020



NEMMP2020

2014
India becomes member country of Electric Vehicles Initiative (EVI)

2015
FAME India - Faster Adoption and Manufacturing of (Hybrid & Electric) Vehicles in India

Phase I

FAME-I

2017
NITI Aayog Roadmap

2019
FAME-II

Phase II

2021
FAME-II Extension
PLI-ACC
PLI-Auto

Extn. Phase II

2024
PM E-DRIVE

PM E-DRIVE

FAME-India
(National Mission on Electric Mobility)

Early Penetration: E-rickshaw, E-auto, Taxis, Buses

ARAI
Progress through Research

Intelligent Transport System (ITS) Efforts in India (1)

ITS enable Urban Bus Specifications finalized by MoUD

2013 MoUD covered ITS system for buses in UBS-II Specifications for JnnURM Scheme

Key Features – ITS

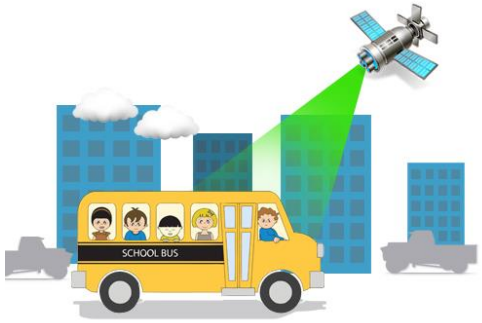
- Multiplex wiring
- Communication with Command Center : Wifi and GPRS
- Vehicle Health Monitoring and Diagnostics System (VHMD)
- Single Driver Console
- **PIS inside and outside integrated with audio announcement system of approaching bus stop**
- Security Camera Network

ITS Efforts in India (2)

Tracking Device in School Buses of CBSE

In 2014, to ensure safe transportation of children, **Central Board of Secondary Education** (CBSE) has made it compulsory to install GPS in all school buses. The Global Positioning System which will help track school buses will be approved by ARAI according to the new guidelines issued by CBSE.

Again, issued guidelines in 2017



ITS Efforts in India (3)

Transportation of hazardous goods requires Vehicle Tracking

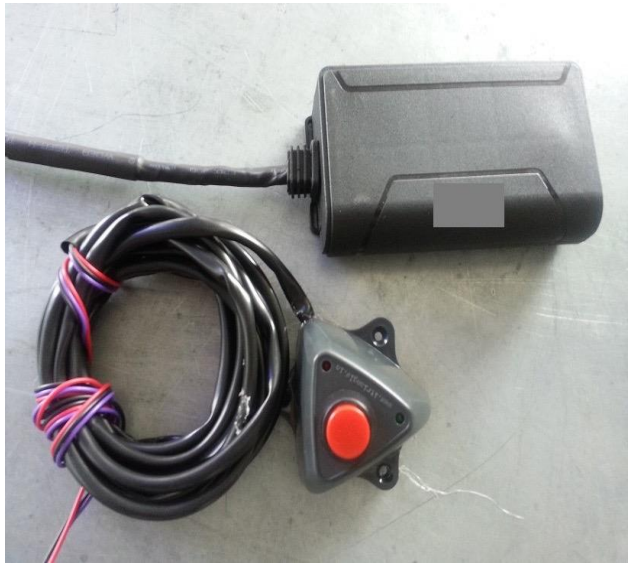
Now Oxygen Cylinder Carrying vehicles must be fitted with Tracking Device (VTS)

Digital Tachographs are planned for vehicles carrying Dangerous Goods

ARAI Progress through Research

ITS Efforts in India (4)

AIS140/ IS 16833: Intelligent Transport System (ITS) -Requirements for Public Transport Vehicle Operation



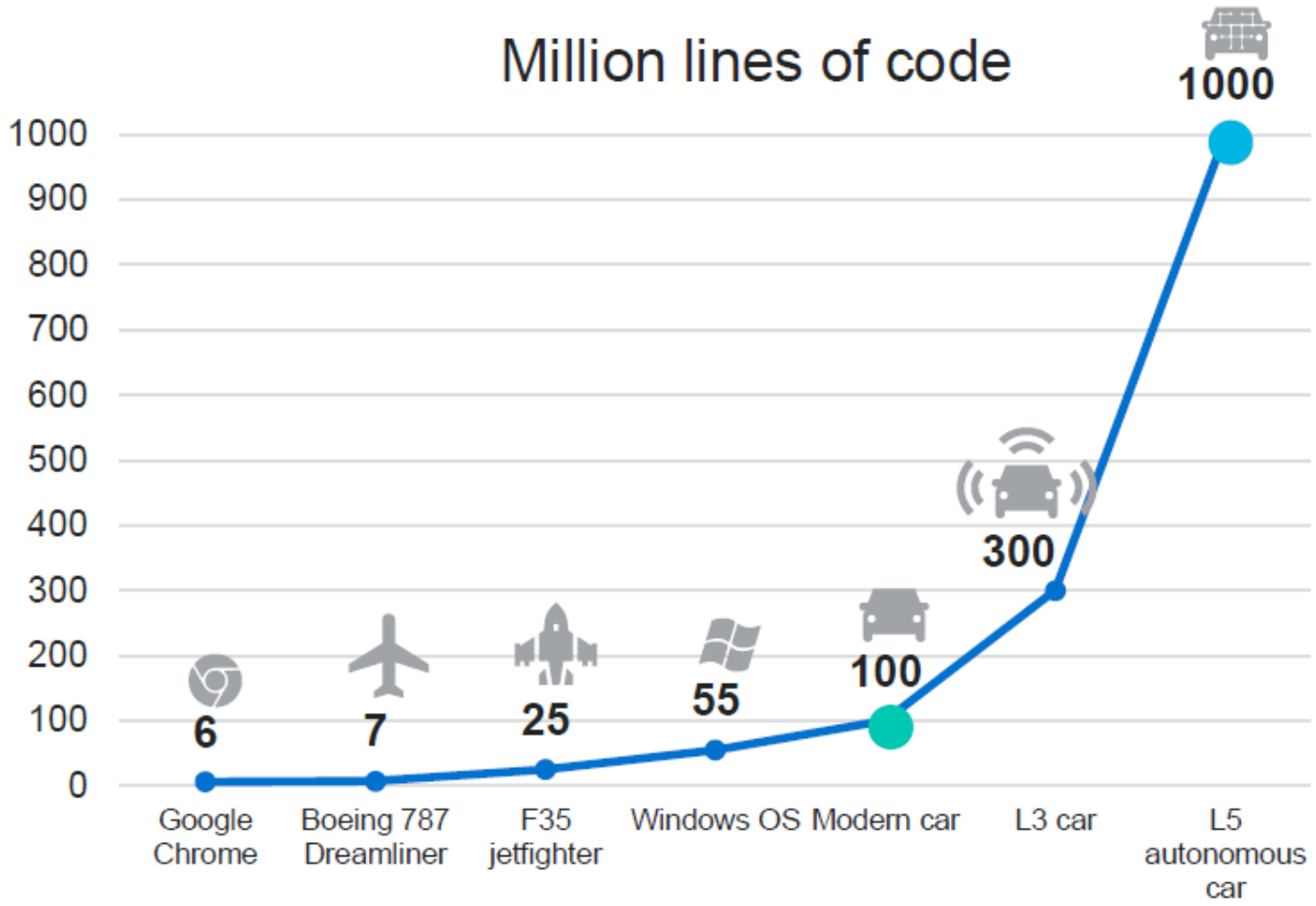
IRNSS Support is Mandatory

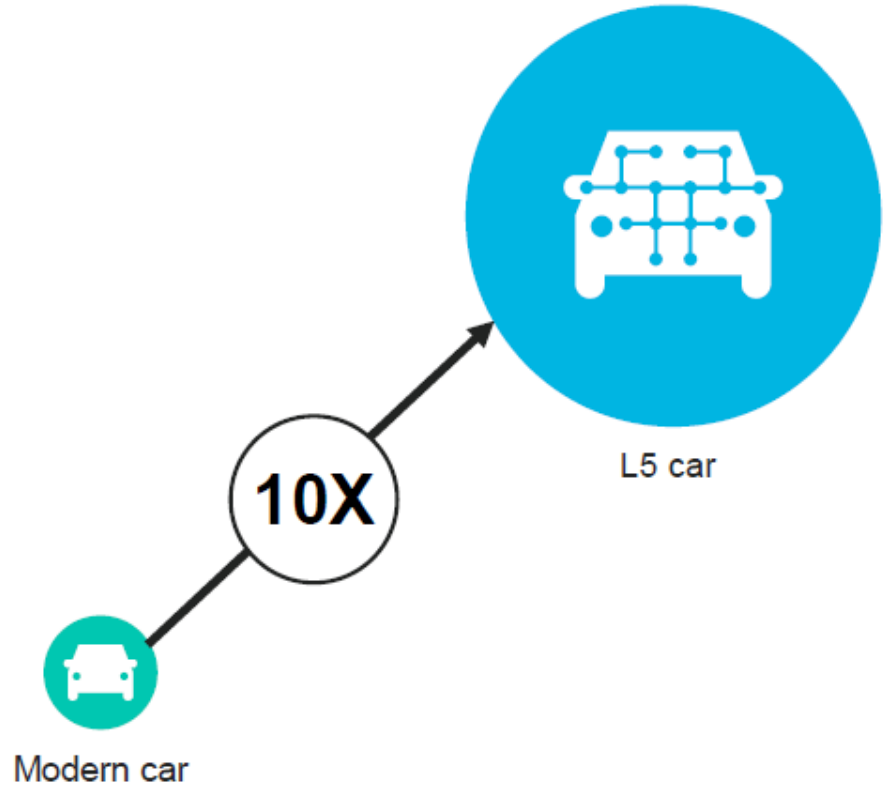
ITS Efforts in India (5)

Proposal for Electronic Toll Collection

- On Highway by **RFID implemented**
- Plan to have **GPS based Toll Collection**

Transition to software-defined vehicles

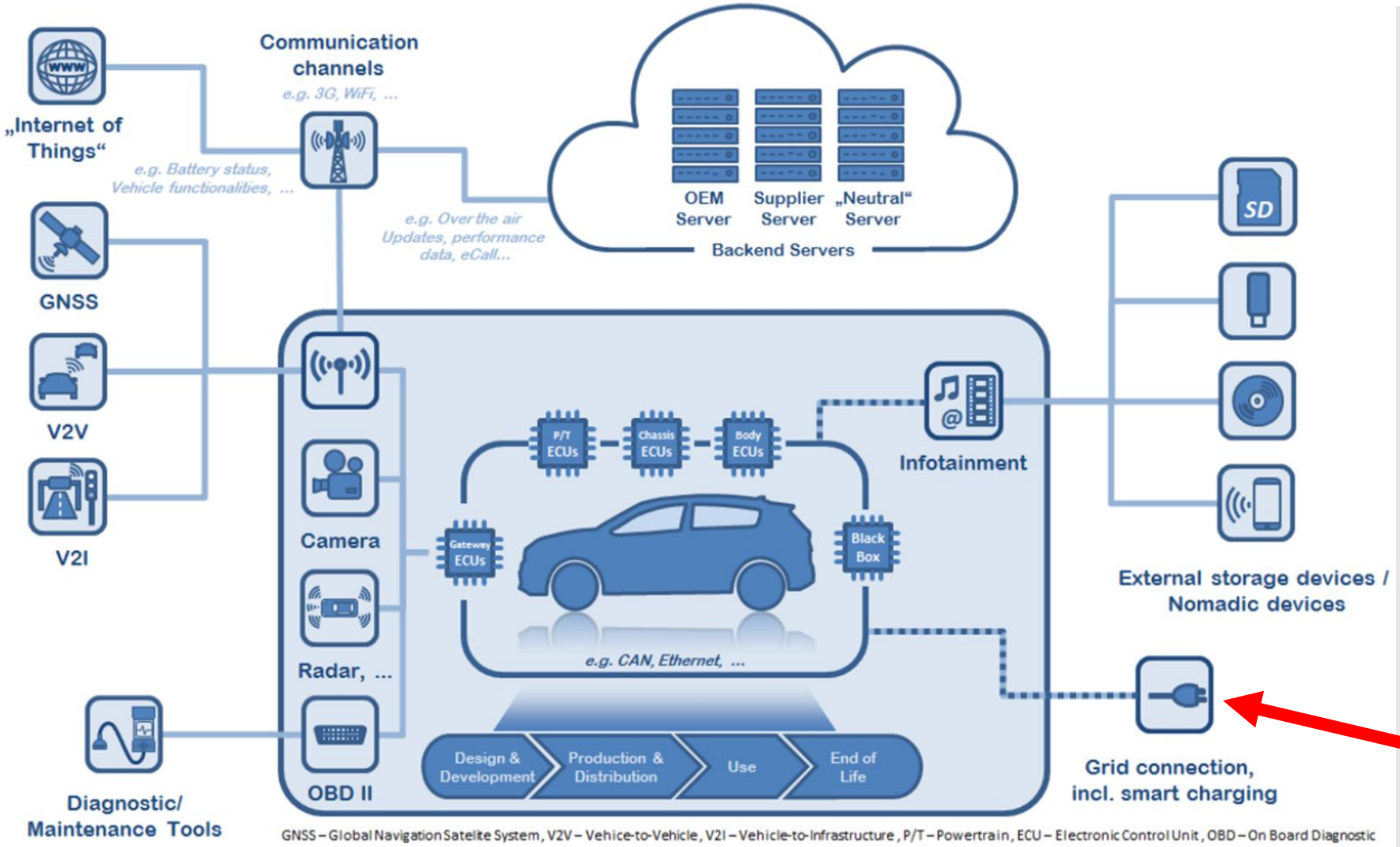




More software + connectivity → greater security threat surface

Source: VW

Vehicle Threat Landscape: Possible attack vectors



Threats against

- External vehicle interfaces
- E/E topology
- In-vehicle networks
- Sensors, Radar, Lidar, Camera
- Common ECU threats
- EV Charger

Penetration Testing, Fuzz Testing, Vulnerability Scanning

WP29 : 1958 and 1998 Agreement

UNECE

- India has signed 1998 agreement.
- Hence, we participates in GTR and **WP 29** meetings

मानकः पथप्रदर्शकः

- In India, BIS is APEX standardization body

AIS

- Automotive Industry Standards Committee (AISC) formulates AIS standards.

WP29 : 1958 and 1998 Agreement

UNECE

1958 Agreement:

- "UN Regulations"
- Directly applicable by the stakeholders/industry
- Mutual recognition of Type Approvals

1998 Agreement:

- "UN Global Technical Regulations"
- Requires transposition in national law
- No administrative procedures -> suitable for:
  - Self Certification
  - Type Approval

#Courtesy: UN ECE

WP29 : GRVA

UNECE

- WP 29
  - ...
  - GRVA
    - TF-CS/OTA

World Forum for Harmonization of Vehicle Regulations

Sub-Working Party on Automated/Autonomous and Connected Vehicles

UN Task Force on Cyber security and OTA issues

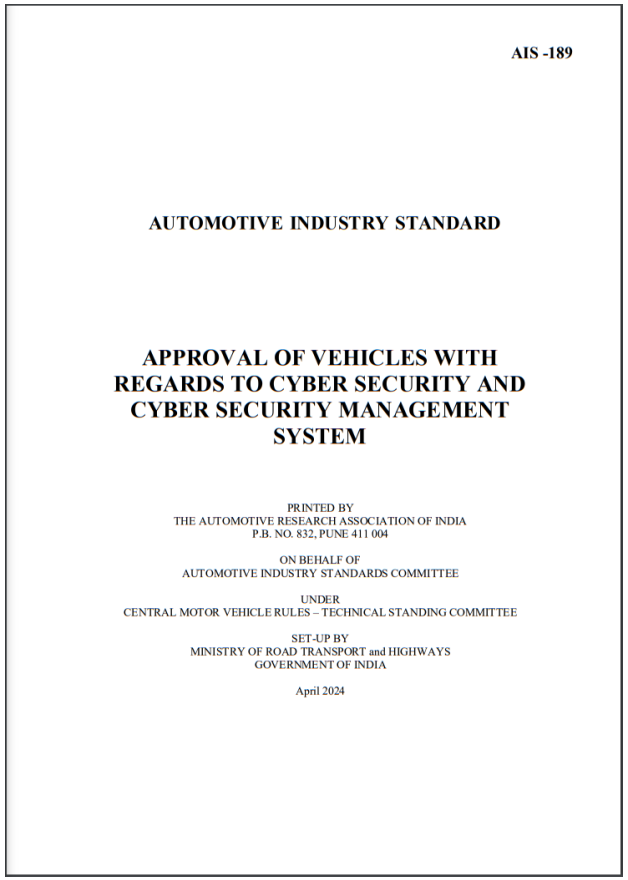
adopts under 1958 agreement

*UN R 155:Uniform provisions concerning the approval of vehicles with regards to **cyber security and cyber security management system***

*UN R 156:Uniform provisions concerning the approval of vehicles with regards to **software update and software updates management system***

Implementation by contracting parties' of 1958 agreement

Cyber Security & CSMS: AIS 189



AIS -189

AUTOMOTIVE INDUSTRY STANDARD

APPROVAL OF VEHICLES WITH REGARDS TO CYBER SECURITY AND CYBER SECURITY MANAGEMENT SYSTEM

PRINTED BY
THE AUTOMOTIVE RESEARCH ASSOCIATION OF INDIA
P.B. NO. 832, PUNE 411 004

ON BEHALF OF
AUTOMOTIVE INDUSTRY STANDARDS COMMITTEE

UNDER
CENTRAL MOTOR VEHICLE RULES – TECHNICAL STANDING COMMITTEE

SET-UP BY
MINISTRY OF ROAD TRANSPORT and HIGHWAYS
GOVERNMENT OF INDIA

April 2024

- New Panel Formulation in 66th Meeting of AISC (14thJuly 2021)
- Multiple Panel Meetings are done
- **Present Status :** AIS 189 on CSMS is formulated

Corresponding UN R	UN Regulation No. 155 - Cyber security and cyber security management system
Scope of AIS 189	Applicable for M and N (passenger cars, vans, trucks and buses) T-trailers if fitted with at least one electronic control unit L7- light four-wheeler vehicles if equipped with automated driving functionalities from level 3 onwards **Discussion for L1/L2/L5 category**

Introduction to CSMS & Vehicle Type Approval

Cyber Security Management System (CSMS)

- Processes for up-to-date risk identification, treatment, management, security testing, incident/attack detection and handling, threat intelligence and vulnerability monitoring
- Entire life-cycle
- Entire supply chain

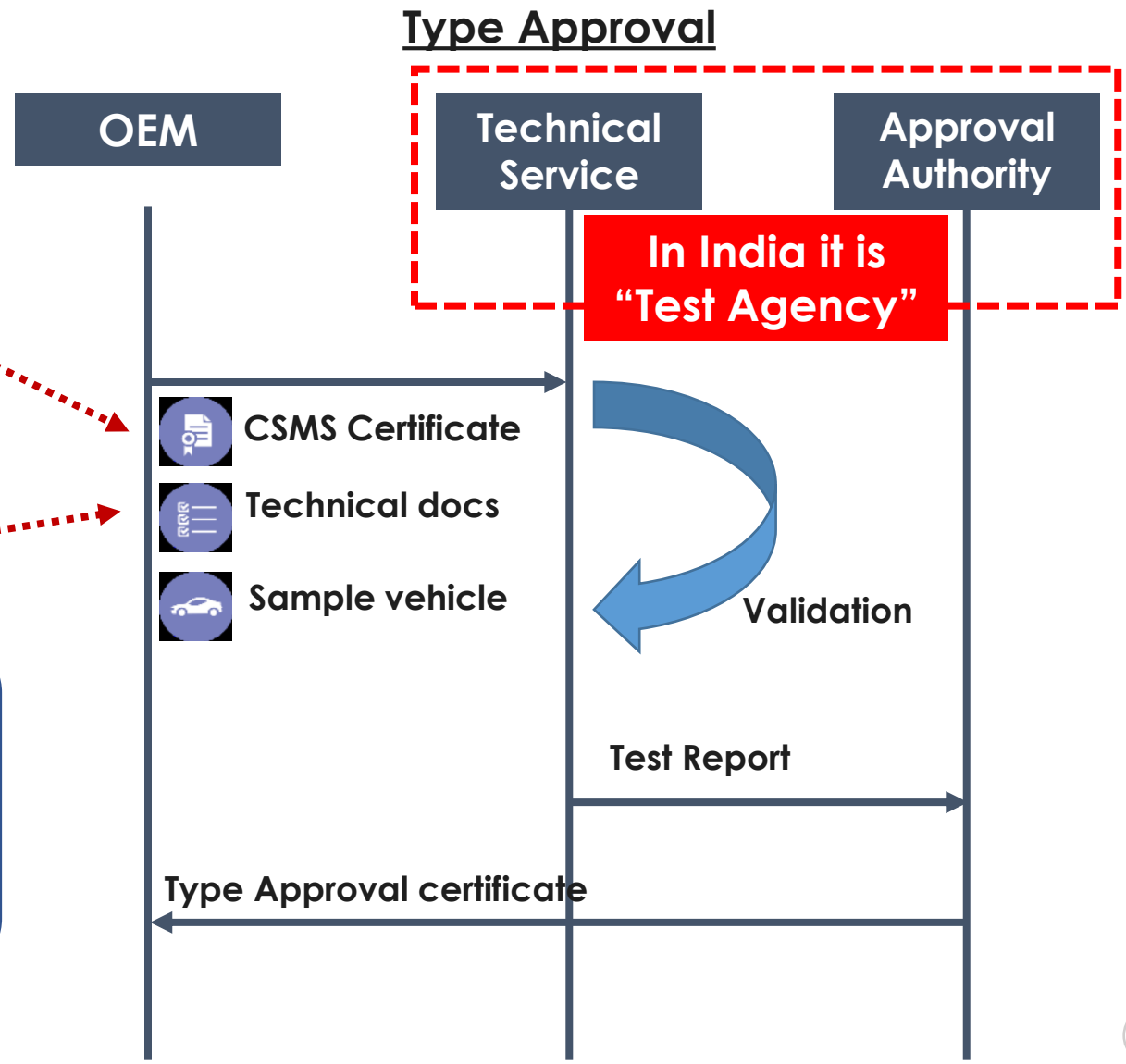
Vehicle Security

- "Application of CSMS to complete vehicle type approval"

OEMs Need to go for

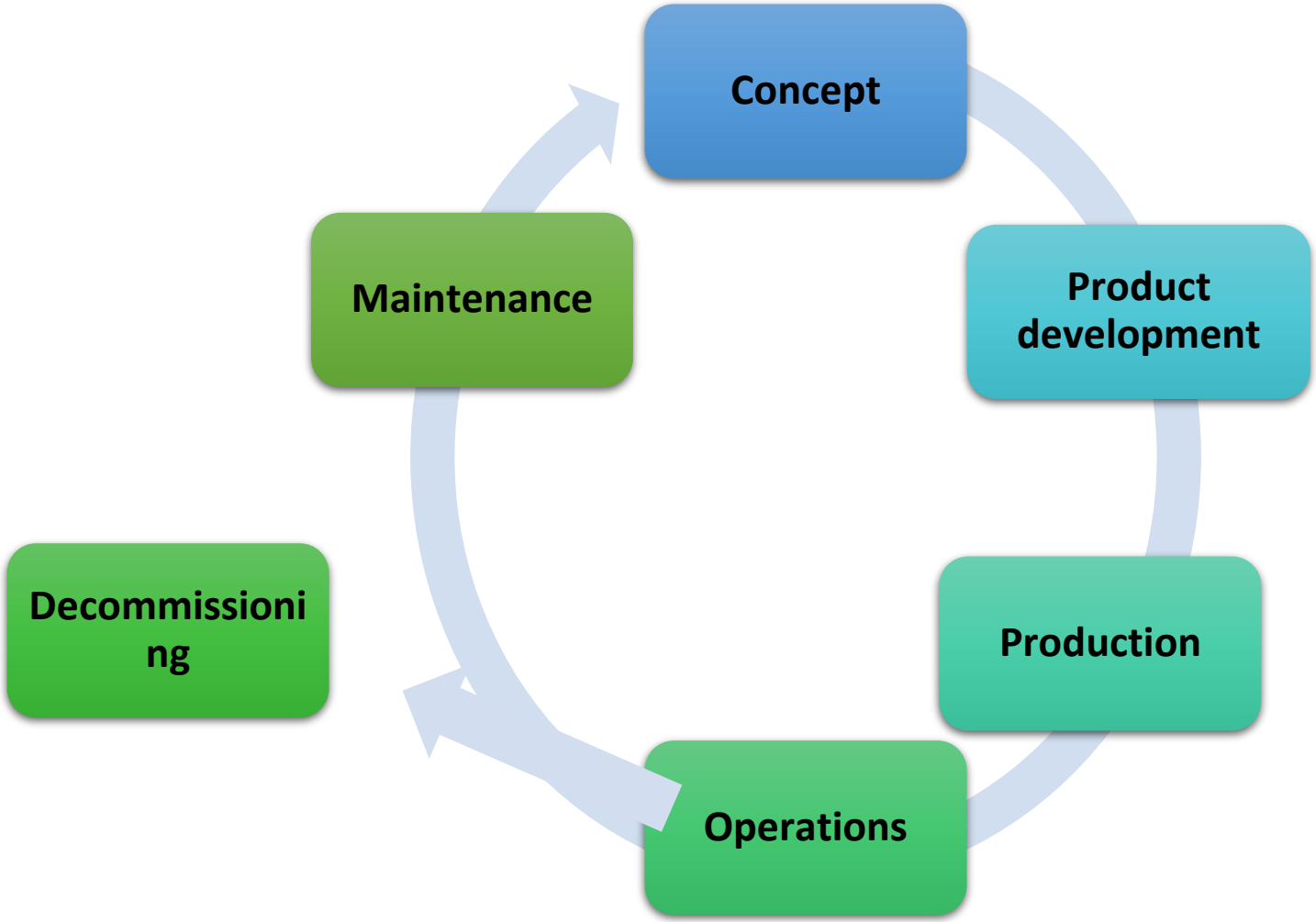
1) Cyber Security Management System (CSMS) Certificate- Organization

2) Cyber Security -Vehicle Type Approval



Cybersecurity throughout the Life Cycle of Vehicle

Overall Cybersecurity risk management



ISO/SAE 21434 Road Vehicles - Cybersecurity Engineering

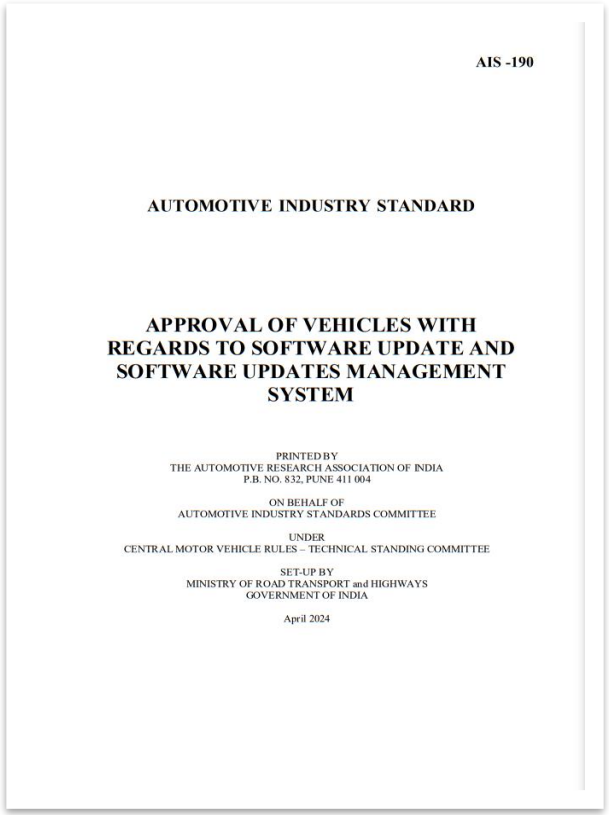
1. ISO 21434 addresses the cybersecurity perspective in engineering of **electrical and electronic** (E/E) systems within **road vehicles**.

2. A framework is defined that includes requirements for cybersecurity processes and a common language for communicating and managing cybersecurity risk.

   - **Define cybersecurity policies and processes;**
   - **Manage cybersecurity risk; and**
   - **Foster a cybersecurity culture.**

3. ISO 21434 can be used to implement a **cybersecurity management system(CSMS)** including cybersecurity risk management.

Software Update including Over-The-Air(OTA) Update: AIS 190



AIS -190

AUTOMOTIVE INDUSTRY STANDARD

APPROVAL OF VEHICLES WITH REGARDS TO SOFTWARE UPDATE AND SOFTWARE UPDATES MANAGEMENT SYSTEM

PRINTED BY
THE AUTOMOTIVE RESEARCH ASSOCIATION OF INDIA
P.B. NO. 832, PUNE 411 004

ON BEHALF OF
AUTOMOTIVE INDUSTRY STANDARDS COMMITTEE

UNDER
CENTRAL MOTOR VEHICLE RULES – TECHNICAL STANDING COMMITTEE

SET-UP BY
MINISTRY OF ROAD TRANSPORT and HIGHWAYS
GOVERNMENT OF INDIA

April 2024

- New Panel Formulation in 66th Meeting of AISC (14th July 2021)
- Multiple Panel Meetings are done
- **Present Status :** AIS 190 on Software Update & SUMS is formulated

Corresponding UN R	UN Regulation No. 156 - Software update and software update management system
Scope of AIS 190	Applicable for M and N (Passenger cars, vans, trucks and buses) A-Agricultural vehicles T-Trailers, … that permit software updates **C- Construction Equipment, L category -> Under Discussion**

AIS 190: Software Update and Software Update Management System (SUMS)

Software Identification Number RxSWIN or AIS[IS]xSWIN

A **dedicated identifier**, defined by the vehicle manufacturer, representing information about the type approval relevant software of the Electronic Control System.

- Software Update Management System with vehicles for updating vehicle firmware by over-the-air updates (OTA) as per AIS 190 standard.

- **Software Defined Vehicle** (SDV) is reshaping the Automotive Landscape providing
  - Customization and Personalization
  - Improved User Experience
  - AI Integration
  - Operational Efficiency
  - Innovation
  - Enable Over-The-Air Updates

Discussion points w.r.t India

Proposal under discussion for Applicability to category of vehicles

- Many Electric Vehicles are being launched in India
- Premium 2W-EVs offer OTA update and OTA configurable subscription model
- Panel members are discussing to bring 2W (L1/L2) category under the ambit of CSMS & SUMS

Challenges in Implementation w.r.t India

Implementation of AIS 189 (CSMS) and AIS 190 (SUMS)

(1) Competency for Cyber Security in Automotive

→

- Competent personnel with Specific Automotive risk assessments knowledge

- Competency for Cyber Security in Automotive
  - OEMs,
  - Tire-1's,
  - Test Agency

- Penetration Testing
  - Required resources

(2) TS and TAA

- In UN ECE as per 1958 agreement
  - Technical Service (TS)
  - Type Approval Authority (TAA)

  are different

- In India, Test Agency (Like ARAI) plays both roles.

(3) Database for Exchange of Type Approval (DETA)

- Contacting Parties (CP) applying this UN R 155, shall notify and inform other approval authorities of the contracting parties applying UN R 155 about the **method and criteria** taken as basis to assess the appropriateness of the measures taken in accordance with this regulation.

- In EU, Approval Authorities to exchange information via the **Database for Exchange of Type Approval (DETA)** on the assessment method used for R 155.

- In India, no such practices of Data Exchange.- **Need to establish.**

At present in AIS 189, this clause is deleted

Implementation Timelines

Europe Implementation of Cybersecurity and OTA

1. Year July 2022- New Models
2. Year 2024- Existing models

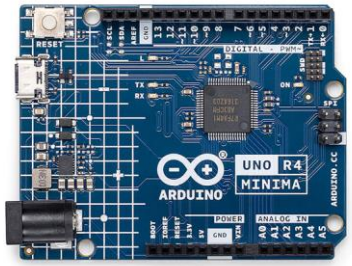
India Proposed Implementation of Cybersecurity and OTA

1. OTA capable: Oct 2027 (New Model)/ Oct 2028 (Existing Model)
2. All OTA Capable Vehicles: Oct 2029
3. All other Vehicles: Oct 2030

ARAI Preparation: Pen Testing Lab

In-Vehicle Network

- USB, Wi-Fi, or Bluetooth
- CAN
- FlexRay
- LIN
- UART
- SENT (Single Edge Nibble Transmission)
- GMSL (Gigabit Multimedia Serial Link)
- I2C (Inter-Integrated Circuit)
- Ethernet
- SAE J1939
- SAE J2497 -Power line communication (PLC)



Hardware Tools

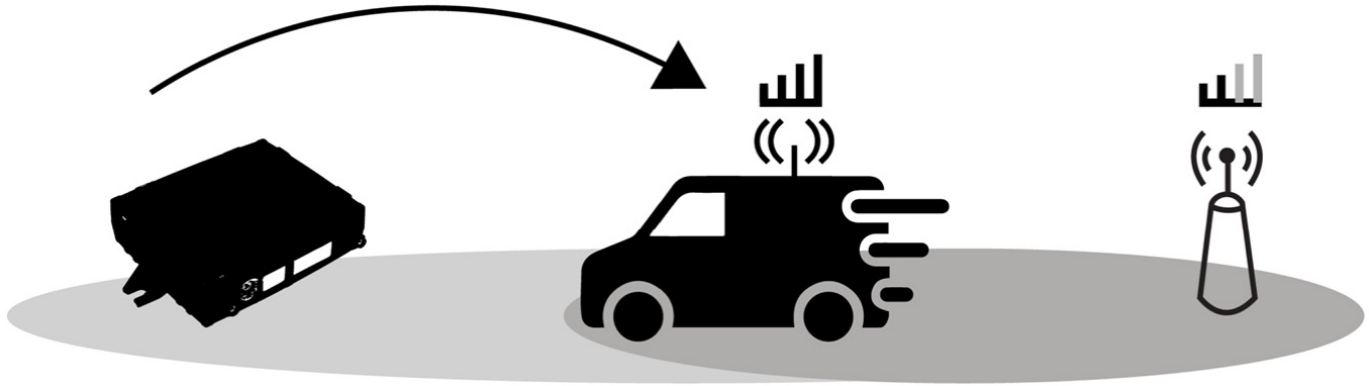
- Arduino Shields for CAN communication
  - CANdiy-Shield
  - ChuangZhou CAN-Bus Shield
  - DFRobot CAN-Bus Shield
  - SeeedStudio SLD01105P CAN-Bus Shield
  - SparkFun SFE CAN-Bus Shield
- CANtact
- Raspberry Pi
- PICAN CAN-Bus Board
- ChipKit Max32 Development Board and NetworkShield
- Freematics OBD-II Telematics Kit

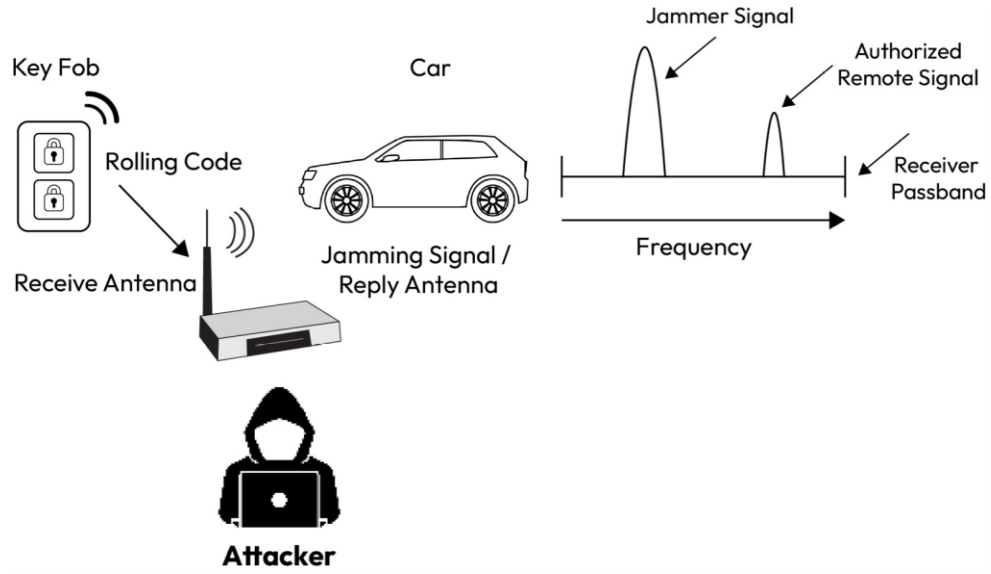
ARAI Preparation : Connectivity threats

- **Cellular**
  - **Location tracking**
  - **Communication interception**
  - **Service downgrade**
- **Wi-Fi**
- **Mobile -application-based attacks- API**
- **Bluetooth**
- **Universal Serial Bus (USB)**
- **OBD**
- **Radio frequency-RKE**

Tool: Cell-site simulators (CSSs)

2G, 3G and LTE, 4G and 5G

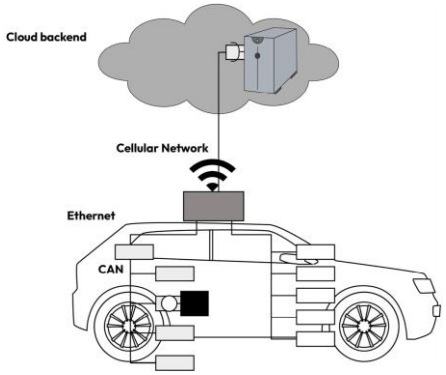




ARAI Preparation : Software Tools/Fuzz Testing

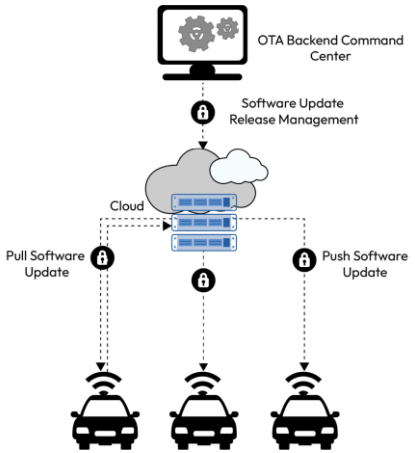
Backend-Server related threats

- Insider threat
- Social engineering
- Spoofed vehicle ID
- Service disruption
- Vehicle data loss or exfiltration
- Malicious software updates

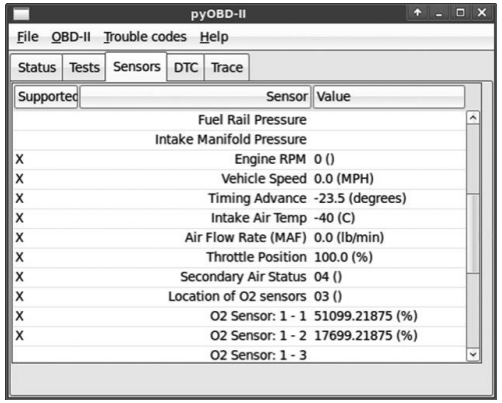


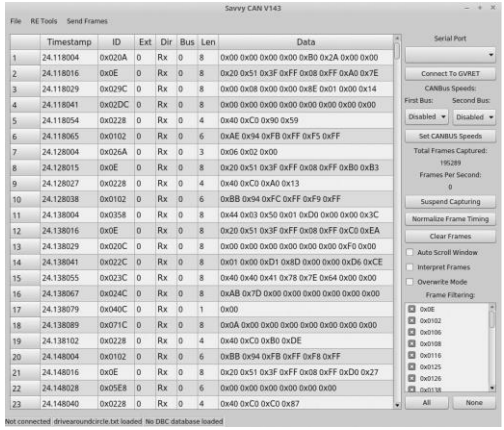
Attack methods against OTA

- Eavesdropping attacks
- Denial of software updates
- Rollback and freeze attacks
- Resource exhaustion
- Mix and match



- **Wireshark**
- **PyOBD Module**
- **CANiBUS Server**
- **Linux Tools**
- **Kayak**
- **SavvyCAN**
- **O2OO Data Logger**
- **UDSim ECU Simulator**
- **Octane CAN Bus Sniffer**





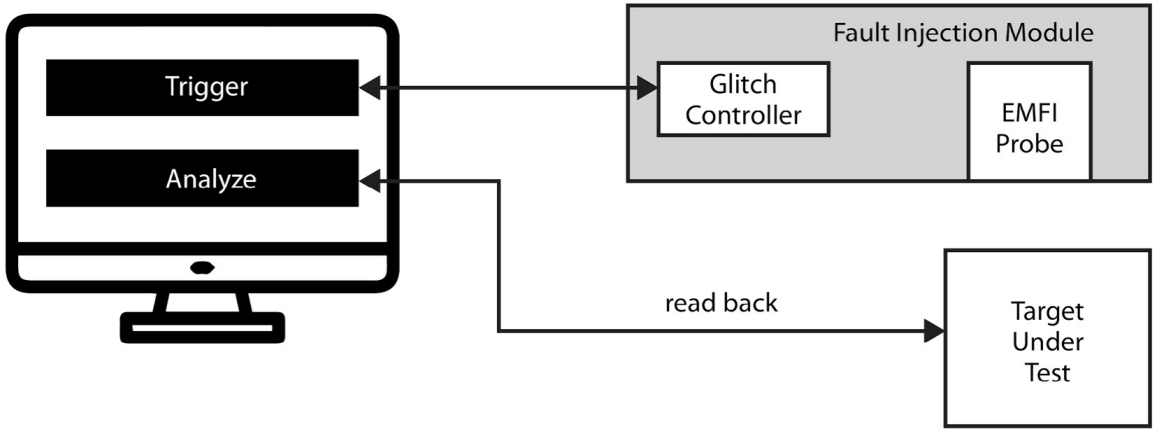
ARAI Preparation: Fault injection attacks: Glitch attacks setup

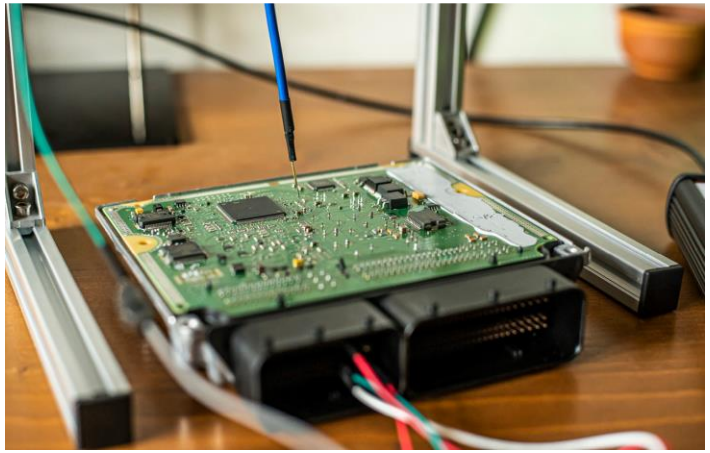
A **fault injection attacks**, called **glitch attacks**, can alter the **CPU** state, causing changes in the **software control flow** to bypass critical security code sections.

E.g bypassing the **boot authentication checks**, enabling an attacker to execute non-genuine software on the ECU source.

Electromagnetic fault injection (EMFI)

Setup where DUT is subjected to **electromagnetic wave pulses** through a **glitch controller**



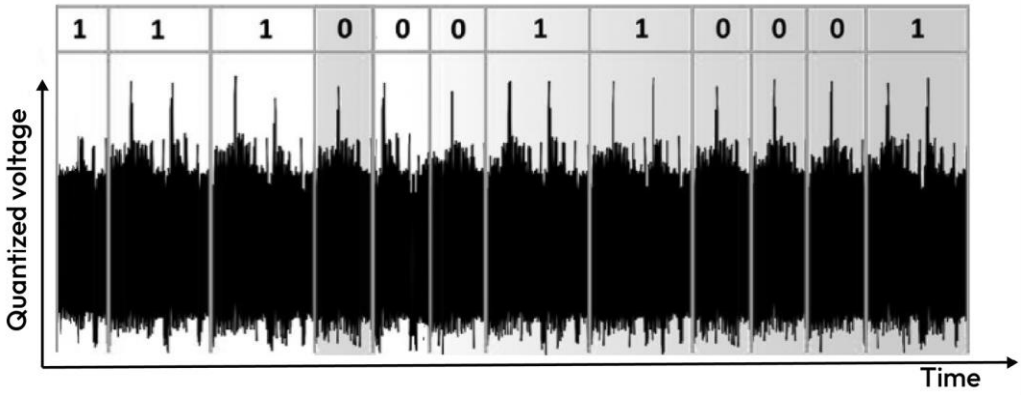


ARAI Preparation : Side channel attacks setup

To exfiltrate sensitive data through covert channels, also known as **side channels**.

- Timing
- Temperature
- Power consumption
- Shared cache memory.

To discover the contents of cryptographic keys inside an ECU or a smart sensor by observing variations in the side channel.



Simple power analysis (SPA)

Figure shows trace of the power variations of an ECU while a key is in use with the **RSA algorithm**.

for taking care of

Security