Intelligent **software-update** technologies for **safe and secure mixed-criticality** and **high performance** cyber physical systems

Irune Agirre (IKERLAN)

THE AUTONOMOUS - Safety, Research & Innovation: EC funding and autonomous mobility

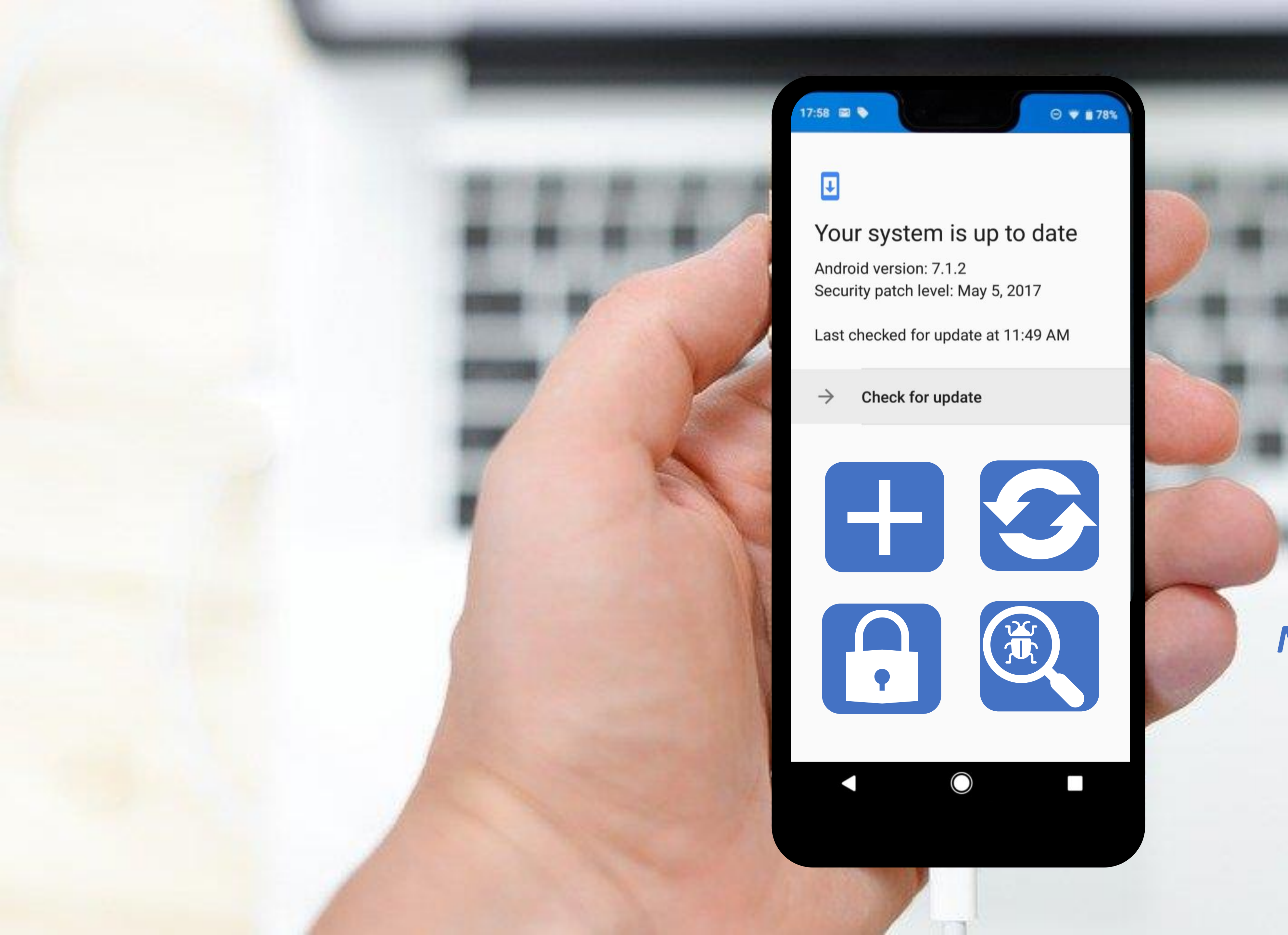
29th of September 2021, Vienna

www.h2020up2date.eu

This project and the research leading to these results has received funding from the European Community's Horizon 2020 Programme [H2020-ICT-2019-2] under grant agreement 871465

European Commission

HORIZON 2020



Your system is up to date

Android version: 7.1.2
Security patch level: May 5, 2017

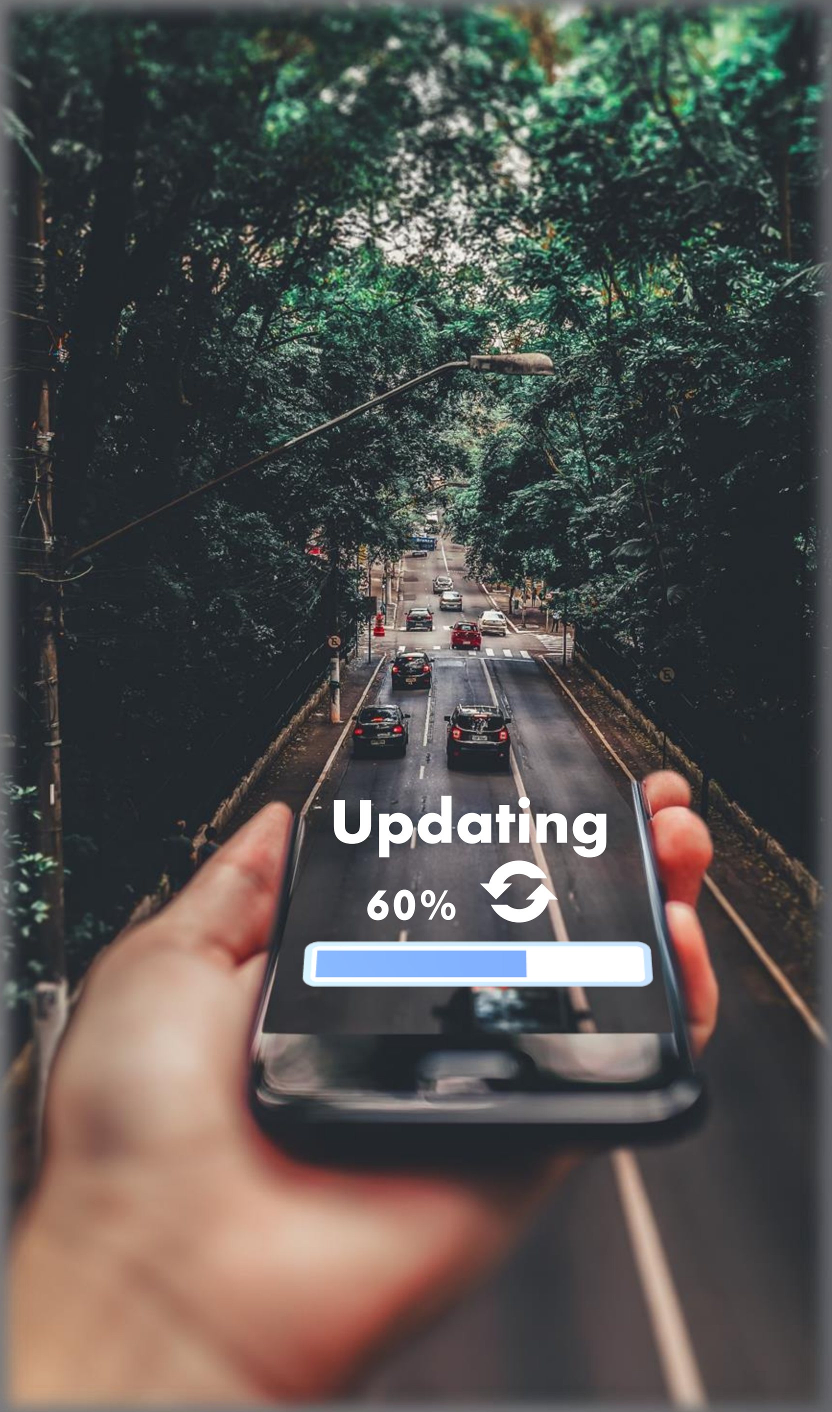
Last checked for update at 11:49 AM

New functionalities

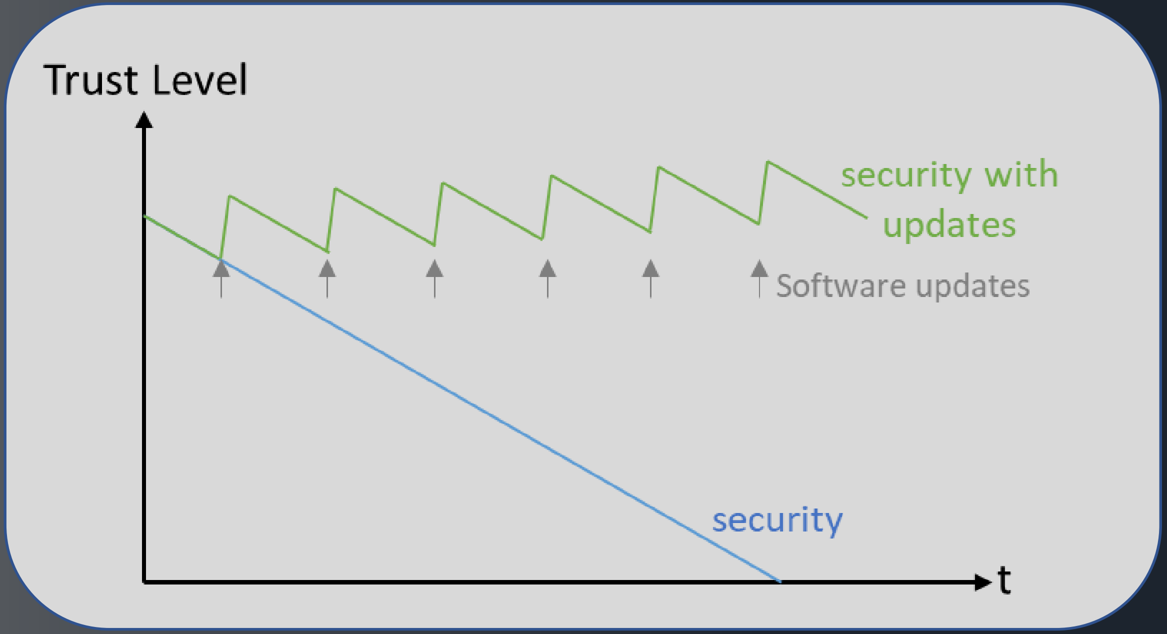
Latest version

Security patches

Bug fixing

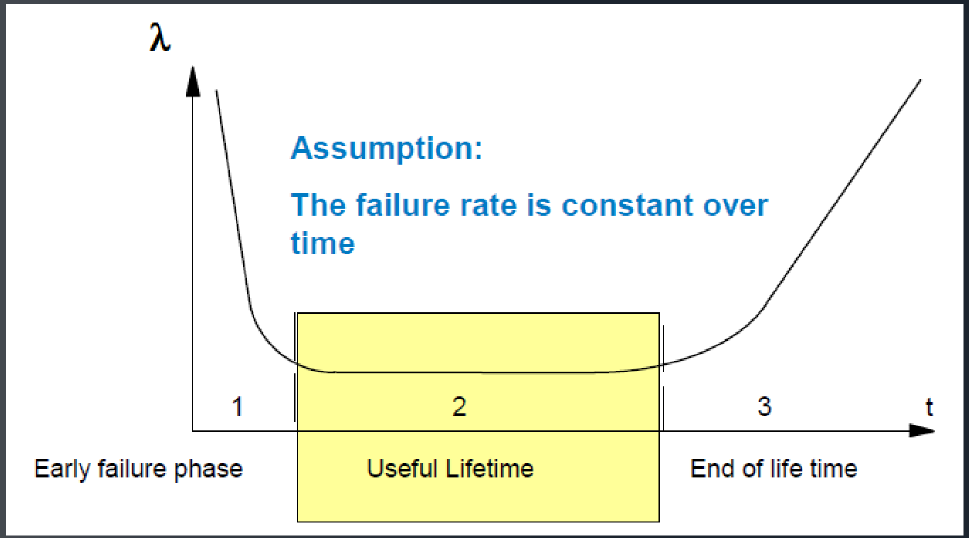


- Connected car is vulnerable to cyber-attacks
- Security mechanisms become obsolete over time
    - New vulnerabilities disclosed every day
- Updates are crucial to guarantee security



- Security demands frequent / critical updates
  - Over-the-air (OTA) updates

- Functional Safety and OTA updates
  - Safety lifecycle (V-model) for critical SW development
  - Modification are discouraged during service life
    - Standards require an impact analysis, new safety validation, re-certification



Source: Hardware-Software Design acc. IEC 61508. Training, TÜV Rheinland, 2012

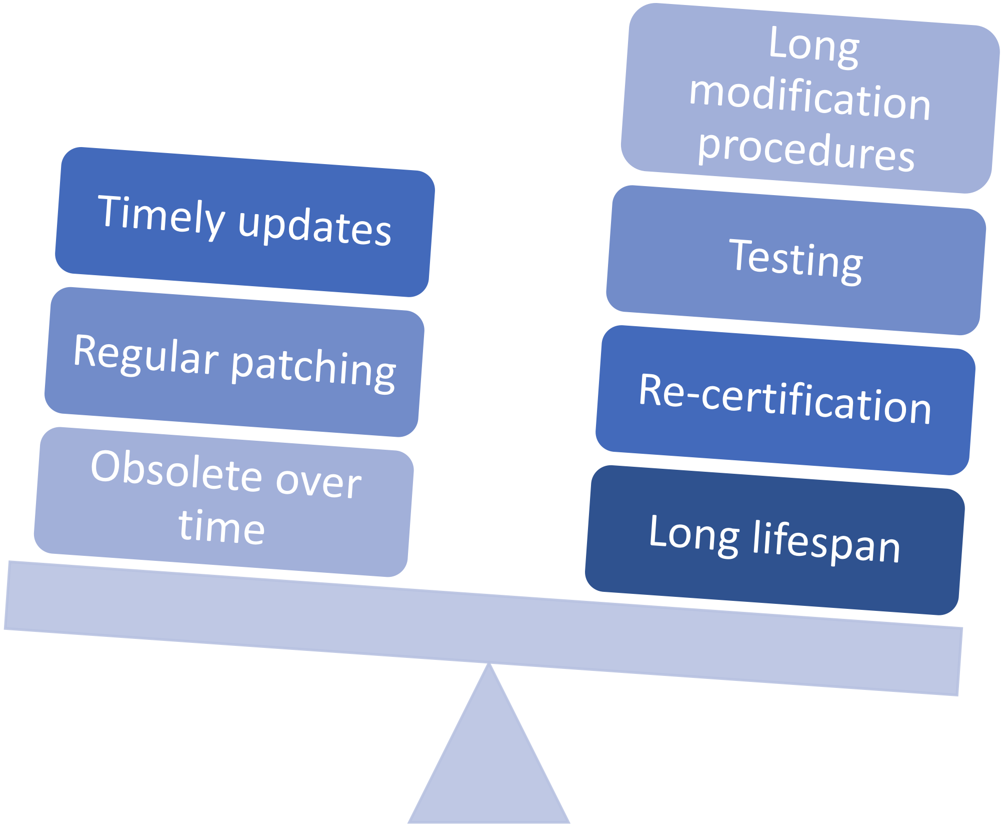
SAFE & SECURE UPDATE MANAGEMENT PROCESS

MODULAR AND MIXED-CRITICALITY ARCHITECTURE DESIGN

APPLICABLE TO EMERGING HIGH-PERFORMANCE EMBEDDED COMPUTING PLATFORMS

SUPPORTED BY MONITORING AND CONTROLABILITY SERVICES

Security vs Safety



Timely updates

Regular patching

Obsolete over time

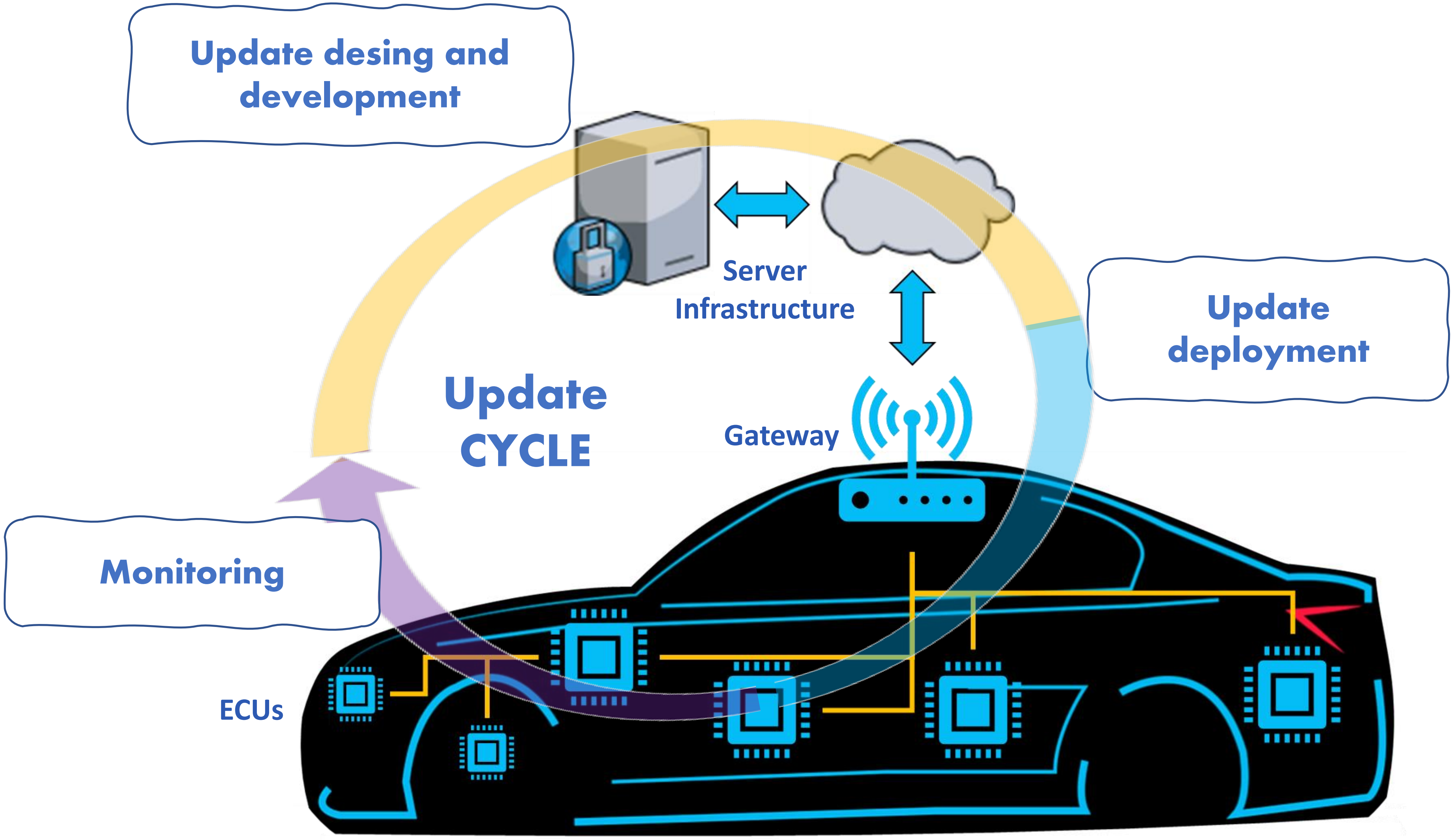
Long modification procedures

Testing

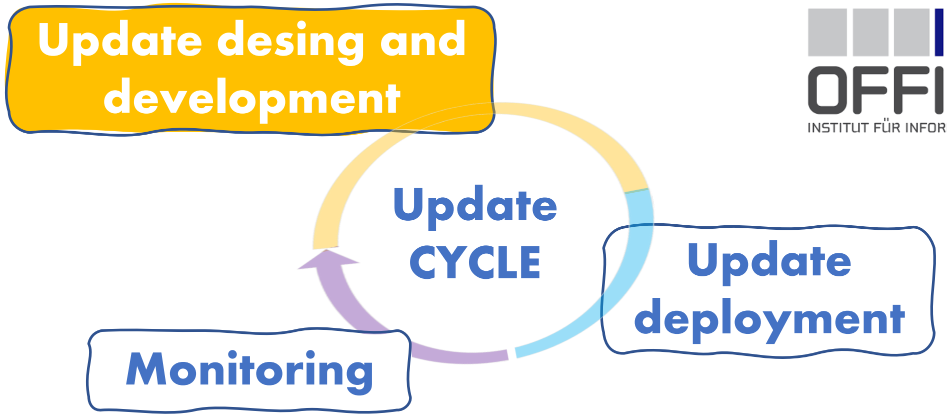
Re-certification

Long lifespan

UP2DATE OTA Architecture



Update desing and development



> **7.4.2.4** The design method chosen shall possess features that facilitate software modification. Such features include modularity, information hiding and encapsulation.
> *IEC-61508-3*

Contract – formalized description of the conditions of integration (real-time, resources, functionality, safety aspects)

UP2DATE update compatibility is defined by:
→ Mutual satisfaction of resource- and metadata-requirements
→ Refinement of (implicit) resource-limits and metadata-criteria
→ Mutual satisfaction of timing-requirements
→ Refinement of timing-specifications

Resource- & Metadata (RMD):

- System-Configurations
- Resource Usage
- Interference
- Power Supply
- Temperature

- (Process- & Data-Integrity)

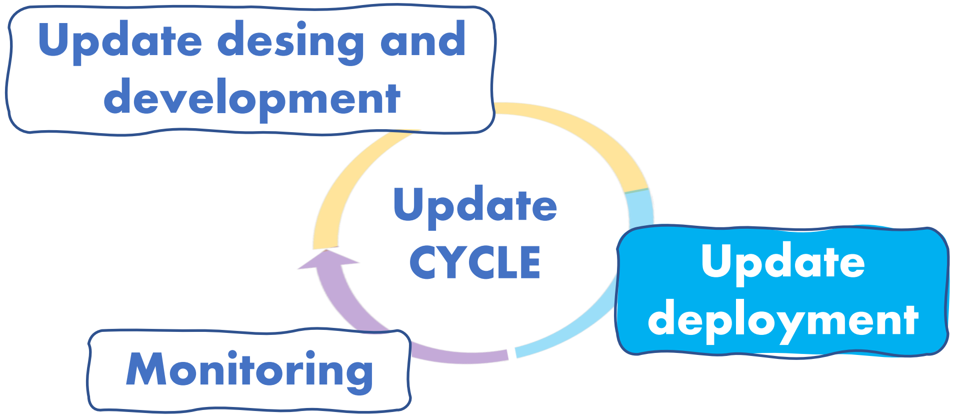
Timing (FET):

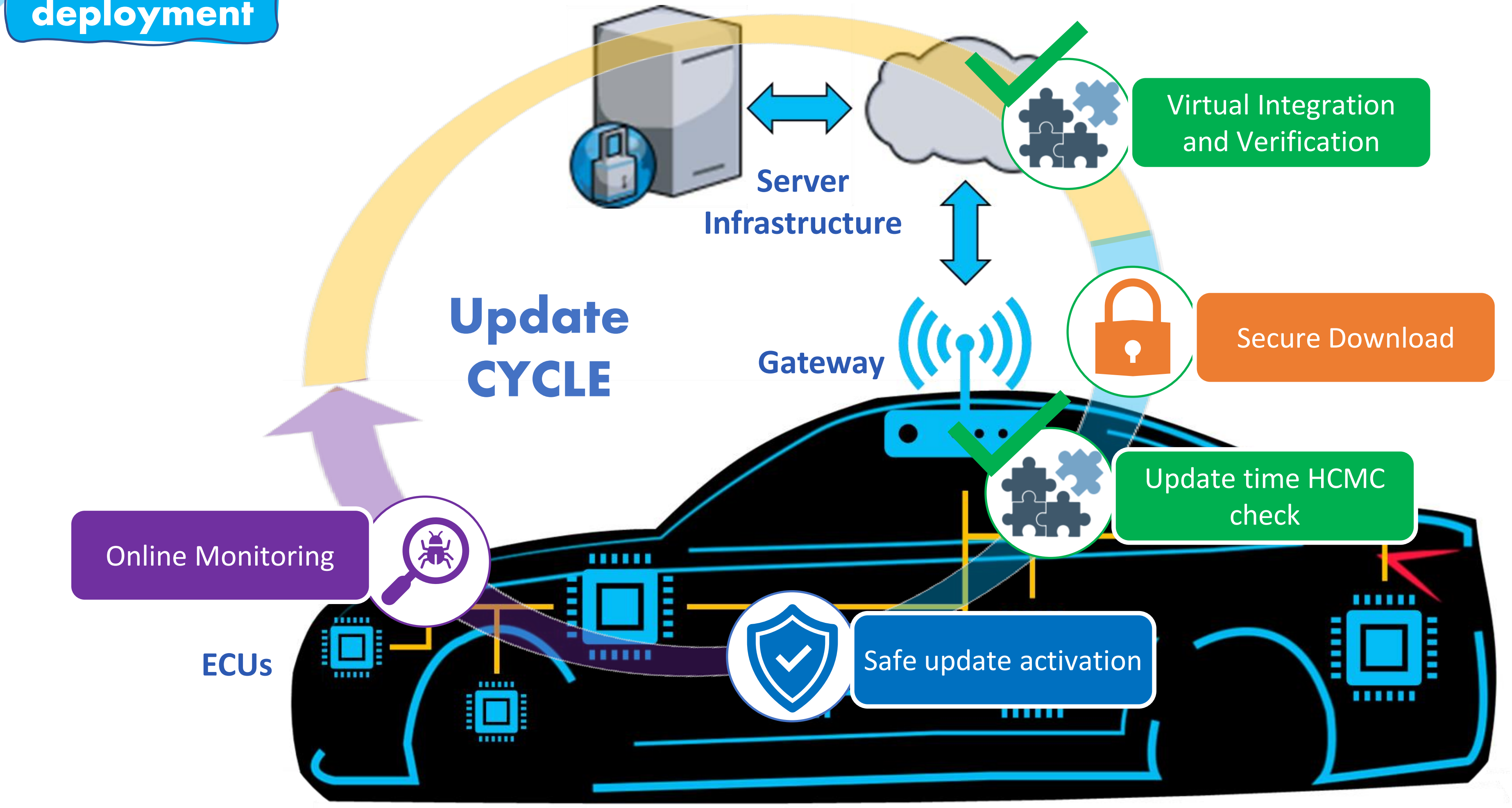
- Absolute & relative timing of functional events (i.e., control-/data-flow-events)

- Regularity & variance of functional-event timing (i.e., period, delay, jitter,)

Slide contents by Gregor Nitsche / Patrick Uven (OFFIS)

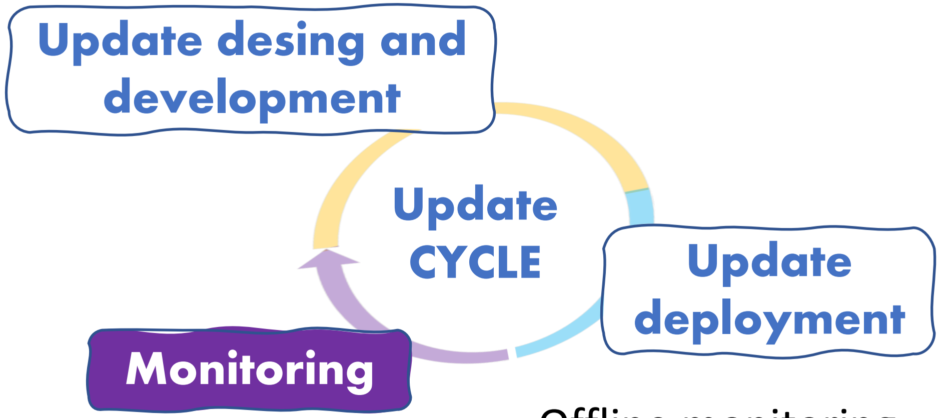
Update design and development





HCMC – Hierarchical Constraint and Metadata Check

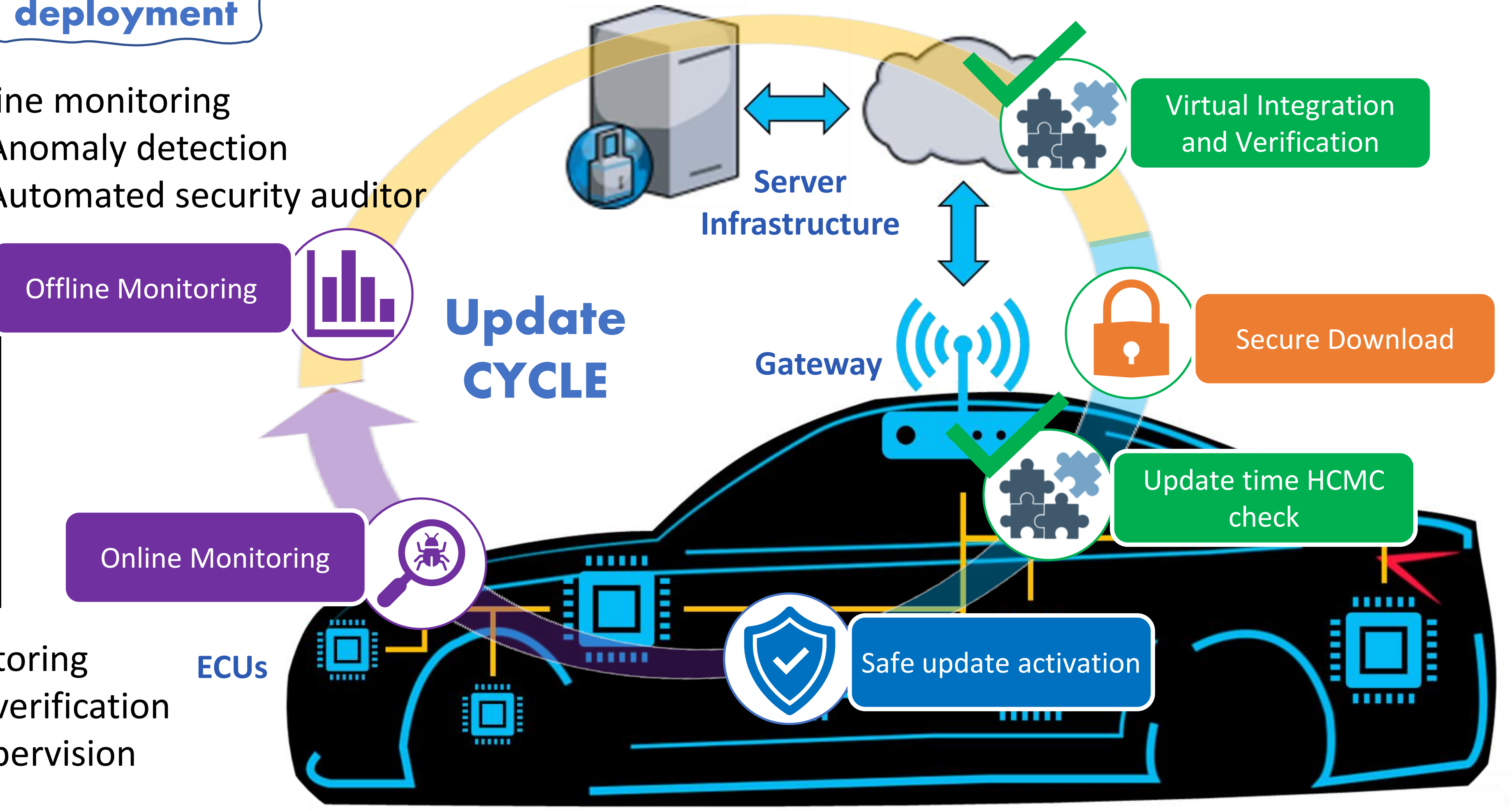
Monitoring



Barcelona Supercomputing Center
Centro Nacional de Supercomputación

ikerlan
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Offline monitoring
- Anomaly detection
- Automated security auditor

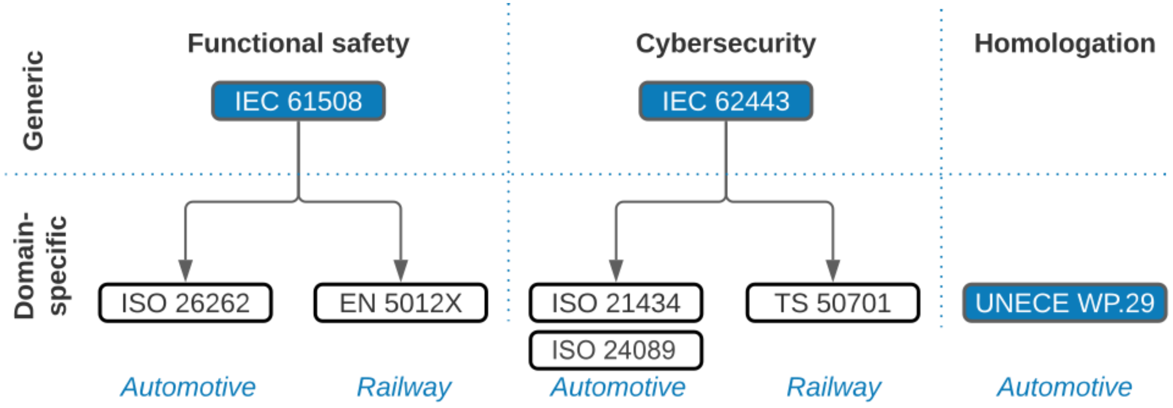


Online monitoring
- Runtime verification
- Safety supervision

HCMC – Hierarchical Constraint and Metadata Check

Safety and security

Regulations and Standards



Generic

Domain-specific

Functional safety

IEC 61508

ISO 26262

EN 5012X

Automotive

Railway

Cybersecurity

IEC 62443

ISO 21434

ISO 24089

TS 50701

Automotive

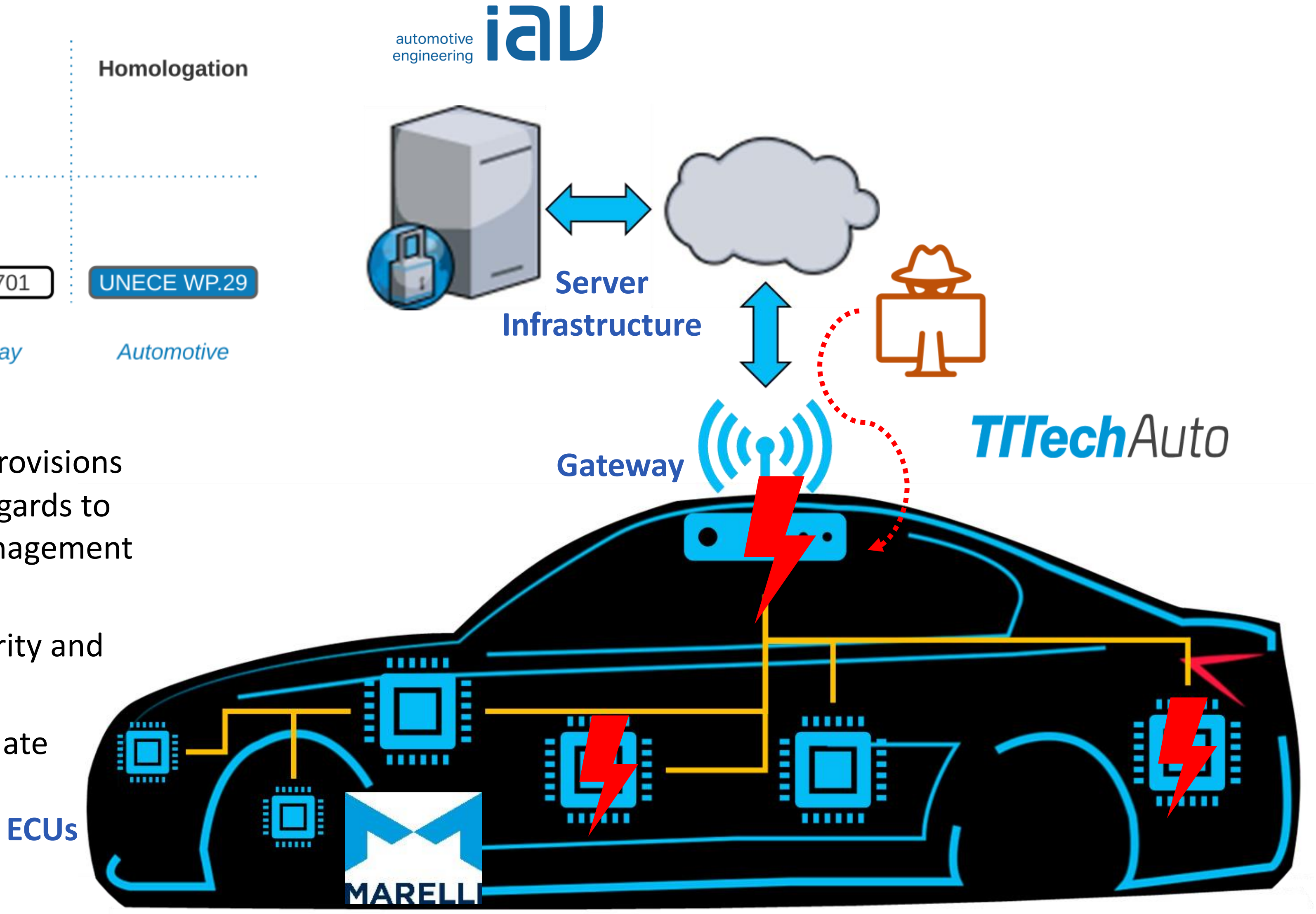
Railway

Homologation

UNECE WP.29

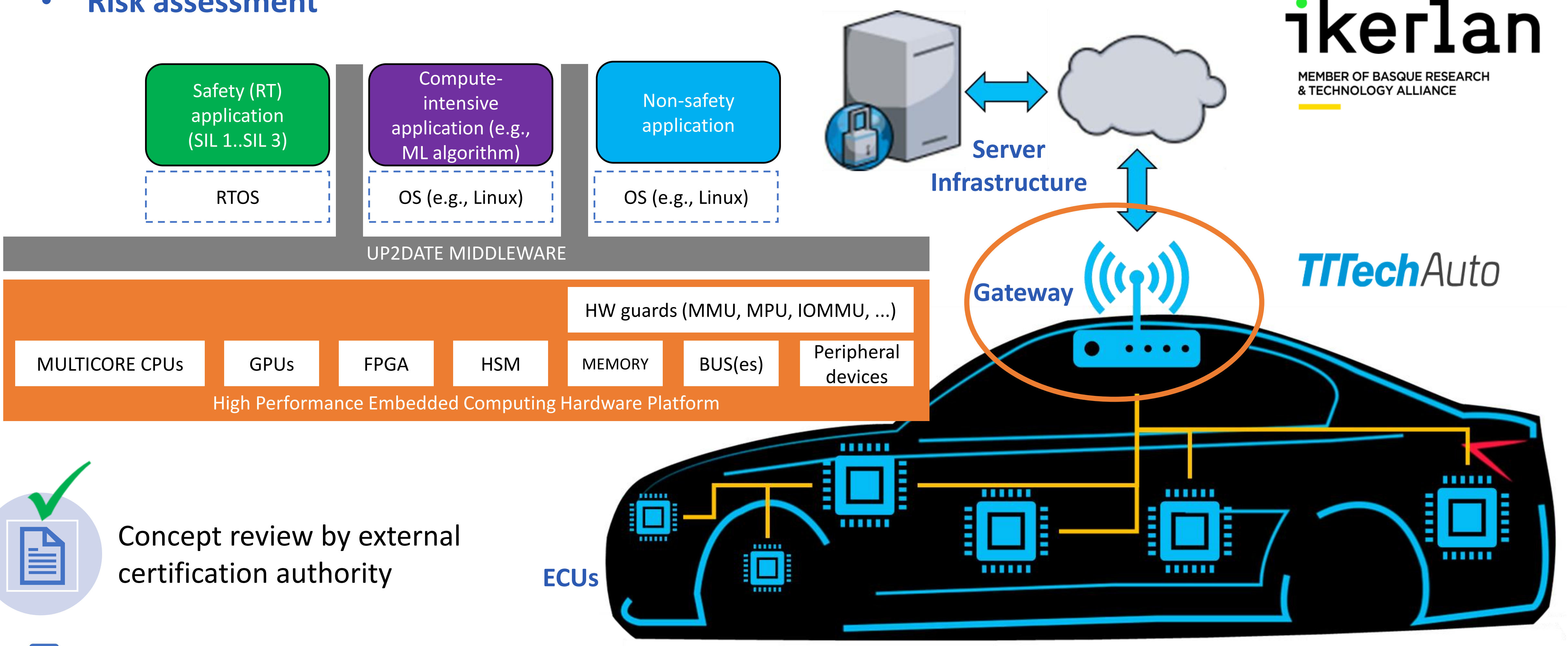
Automotive

- **UNECE UN Regulation No. 156:** Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system
- **UNECE UN Regulation No. 155:** Cyber security and cyber security management system
- **ISO/CD 24089 Road vehicles:** Software update engineering



Safety and security

- **Safe and secure update management procedure**
- **Safe and secure requirements and mixed-criticality architecture design**
- **Risk assessment**


Safety (RT) application (SIL 1..SIL 3)
Compute-intensive application (e.g., ML algorithm)
Non-safety application
RTOS
OS (e.g., Linux)
OS (e.g., Linux)
UP2DATE MIDDLEWARE
HW guards (MMU, MPU, IOMMU, ...)
MULTICORE CPUs
GPUs
FPGA
HSM
MEMORY
BUS(es)
Peripheral devices
High Performance Embedded Computing Hardware Platform
Server Infrastructure
Gateway
ECUs

ikerlan

MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

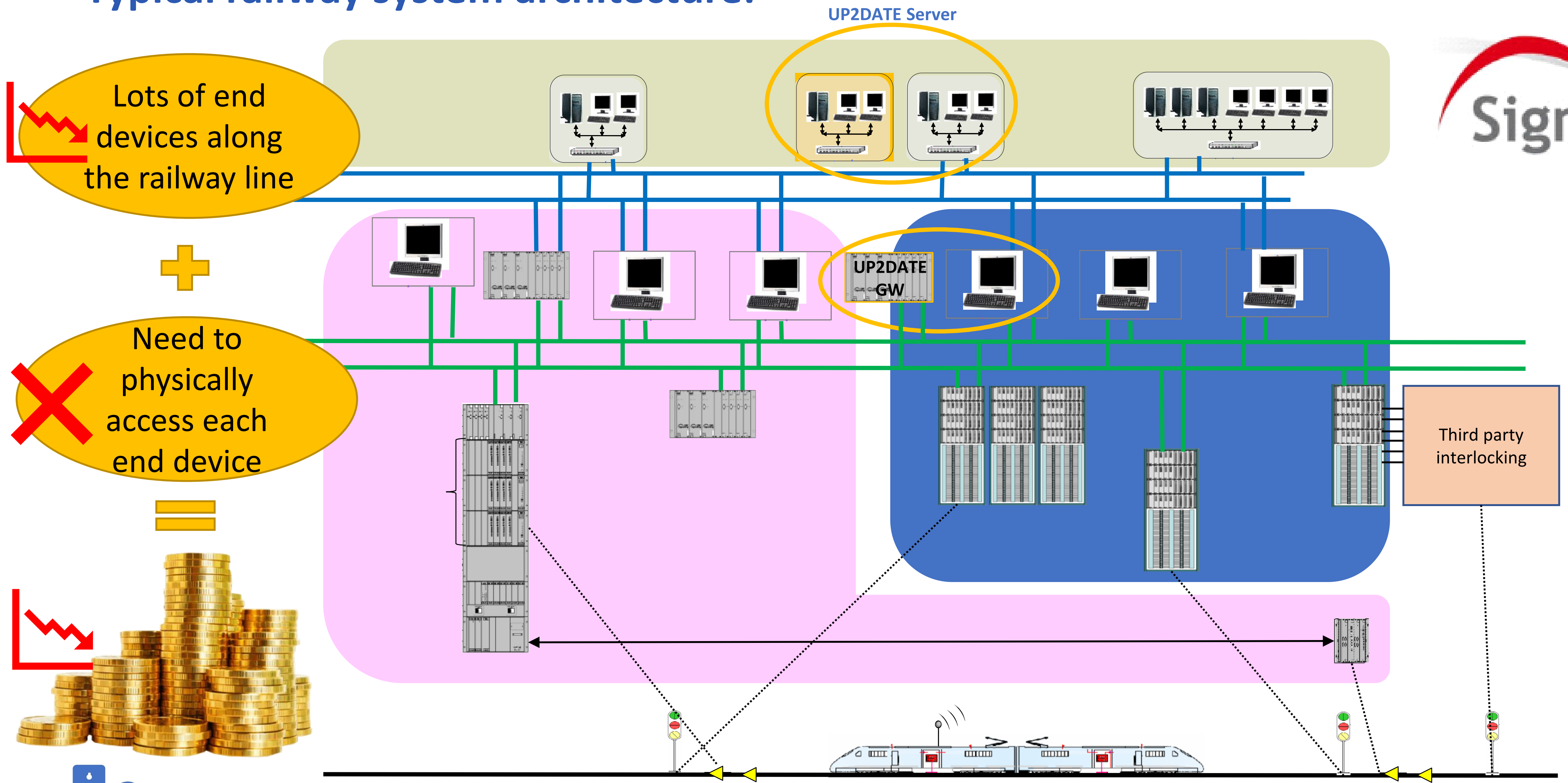
TTTechAuto

Concept review by external certification authority

UP2DATE

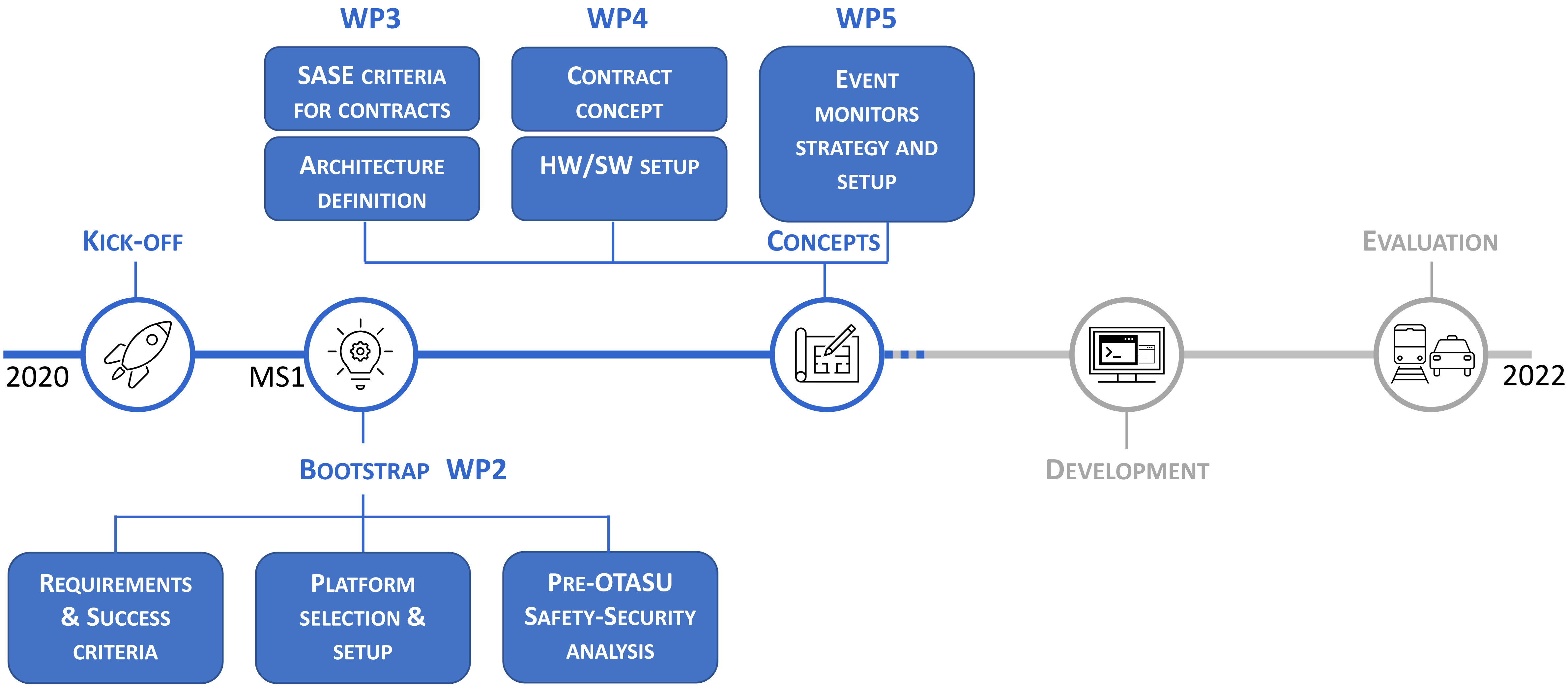
Railway use-case

Typical railway system architecture:


UP2DATE Server
Lots of end devices along the railway line
+
Need to physically access each end device
=
UP2DATE GW
Third party interlocking

Slide contents by Juan Maria Orbegozo (CAF Signalling)

Project planning and status



WP3

SASE criteria for contracts

Architecture definition

WP4

Contract concept

HW/SW setup

WP5

Event monitors strategy and setup

Kick-off

Concepts

Evaluation

2020

MS1

2022

Development

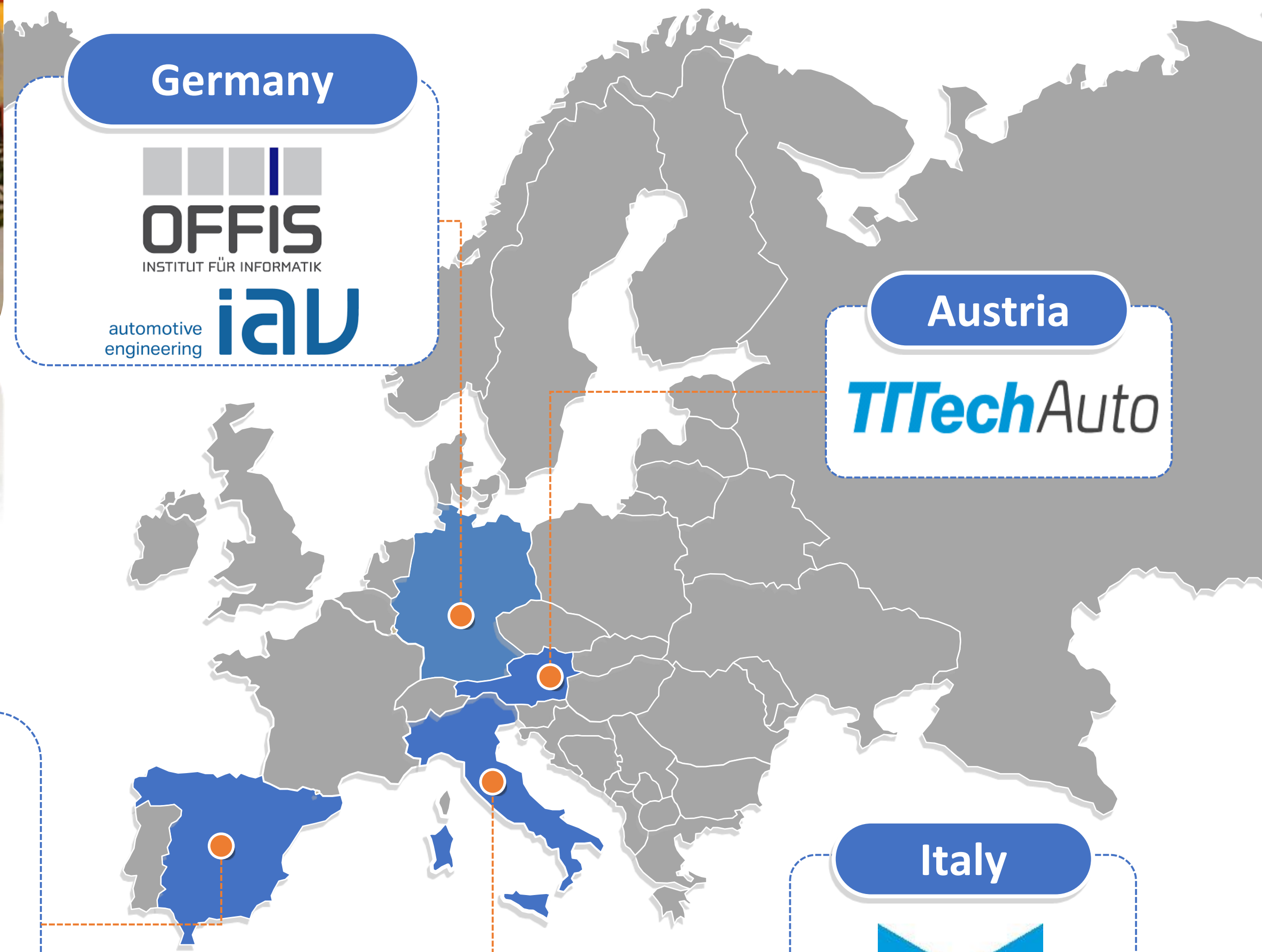
Bootstrap WP2

Requirements & Success criteria

Platform selection & setup

Pre-OTASU Safety-Security analysis

Consortium



Germany

OFFIS
INSTITUT FÜR INFORMATIK

automotive engineering iav

Austria

TTTechAuto

Spain

ikerlan
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

CAF Signalling

BSC Barcelona Supercomputing Center
Centro Nacional de Supercomputación

Italy

MARELLI

UP2DATE

www.h2020up2date.eu/

Follow us!

@UP2DATE_H2020

H2020_UP2DATE

This project and the research leading to these results has received funding from the European Community's Horizon 2020 Programme [H2020-ICT-2019-2] under grant agreement 871465