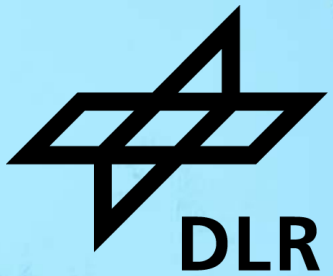
SAFE AND SECURE OVER-THE-AIR SOFTWARE-UPDATES FOR SOFTWARE-DEFINED VEHICLES

From UP2DATE to UP2DATE4SDV



Gregor Nitsche, DLR, Eclipse SDV Community Days, 04.06.2025

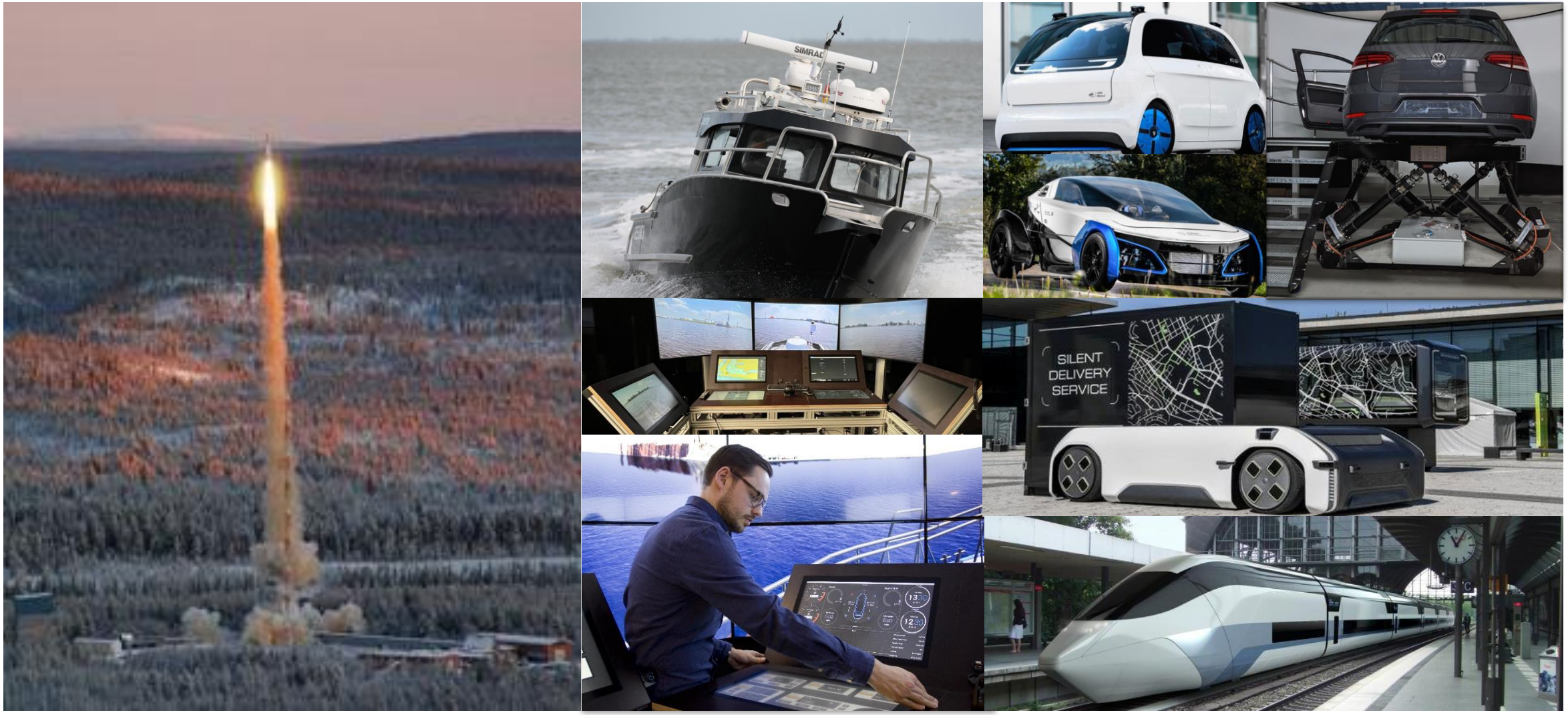
Preview

- DLR is (more than) rocket science
- DLR does SDV and safe & secure OTA SW updates
- We want to integrate and contribute our approaches and technologies to SDV (open source) projects

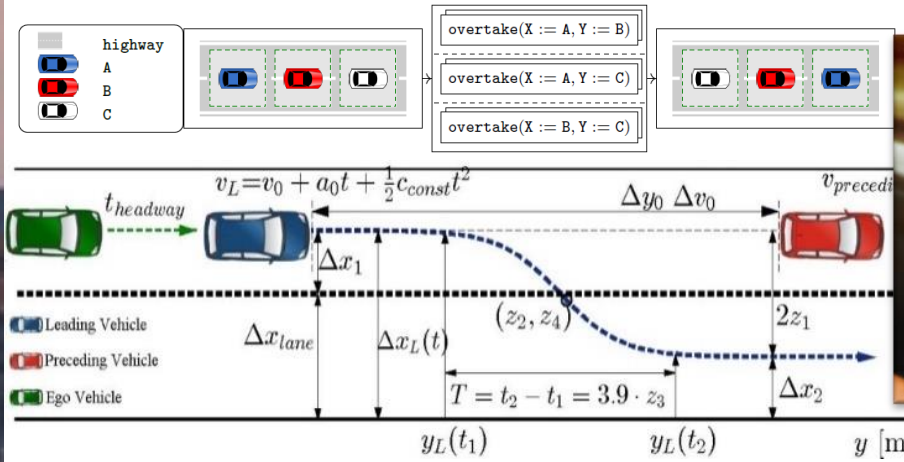
DLR is (more than) Avionics and Rocket Science:

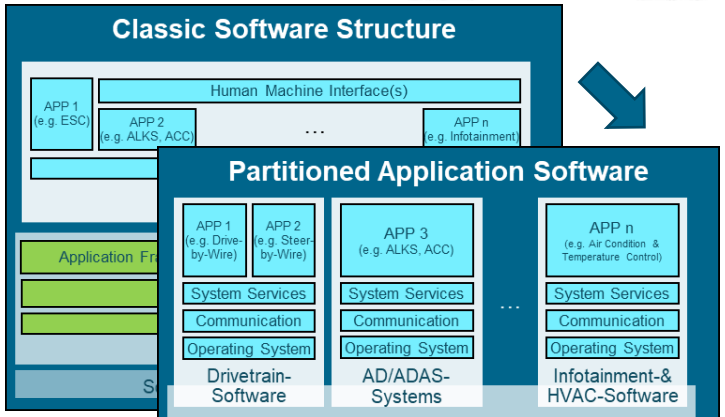
…

DLR is (more than) Avionics and Rocket Science:
… it is Avionics, Space, Energy, and Transportation



DLR is (more than) Avionics and Rocket Science:
… and we are also doing AD & SDV





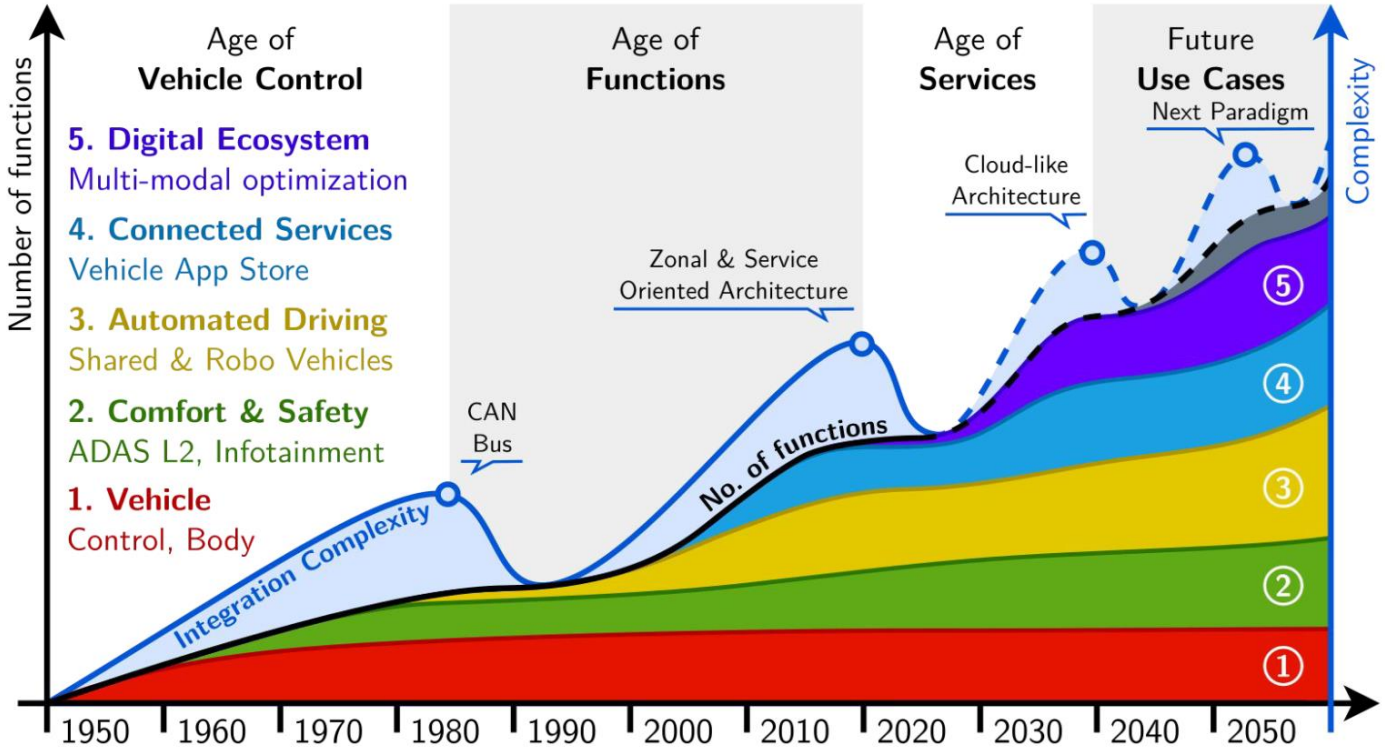
→ Motivation of Updates:

We don’t belief in the ‘Shoot to the Moon’ approach for AD or SDV

- AD (L3+, L4, L5) and SDV are developed incrementally in many, many steps
  - New AI models and perception functions
  - New sensor fusion approaches
  - New driving functions (ADAS → AD)
  - New connectivity (V2X, cloud-services, etc.)
  - …
- Need for safe and secure automated deployment and integration
- Need for modularity and transparency (observability) at model and source-code level

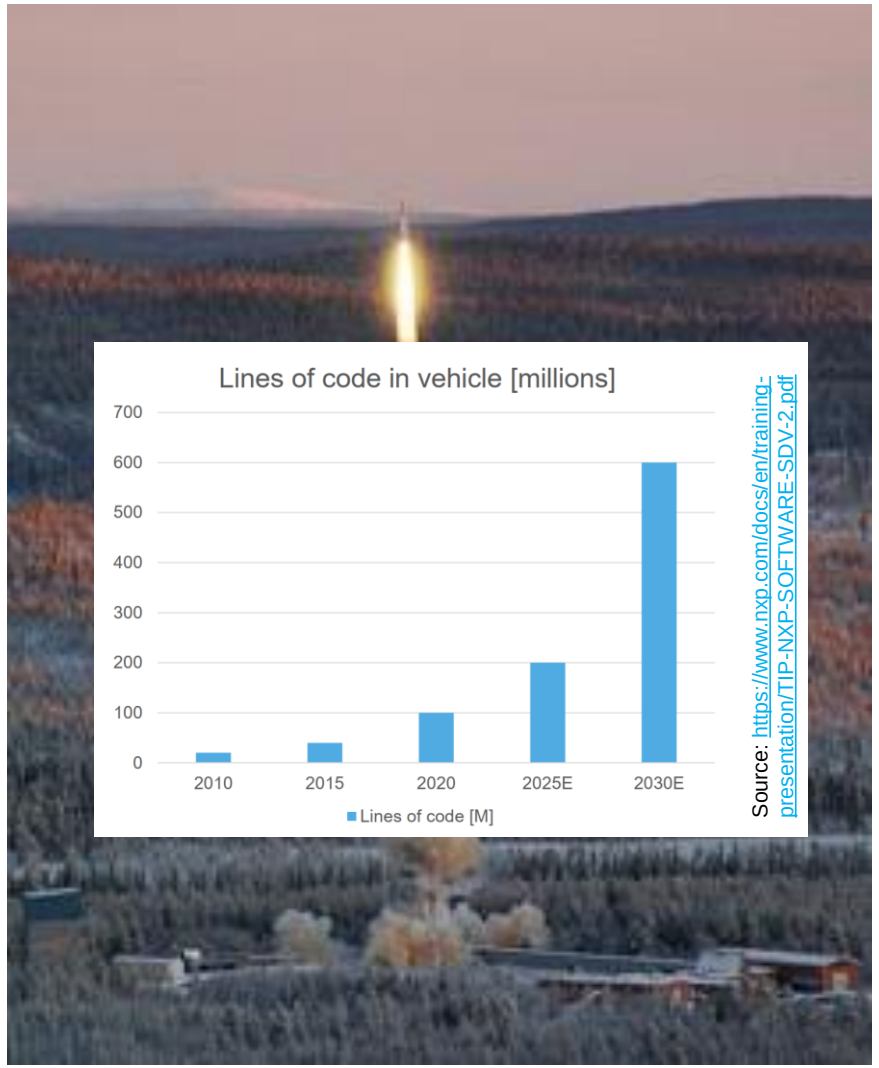
→ Motivation of Updates:

What shoots to the moon is complexity, and integration & test effort



Inspired from C. Buckl et al., "The software car: Building ICT architectures for future electric vehicles" at *IEEE International Electric Vehicle Conference*, 2012

Source: https://youtu.be/nscHI6aO65I?si=IOFrR3_cQNZYwl4x&t=133 &, https://standards.ieee.org/wp-content/uploads/2022/12/D1_02_Pierre-Laclau_Ethernet-as-a-Service-for-Software-Defined-Vehicles.pdf



→ expectation: 50-200 software-updates per year
(corrective, perfective, performative, adaptive)

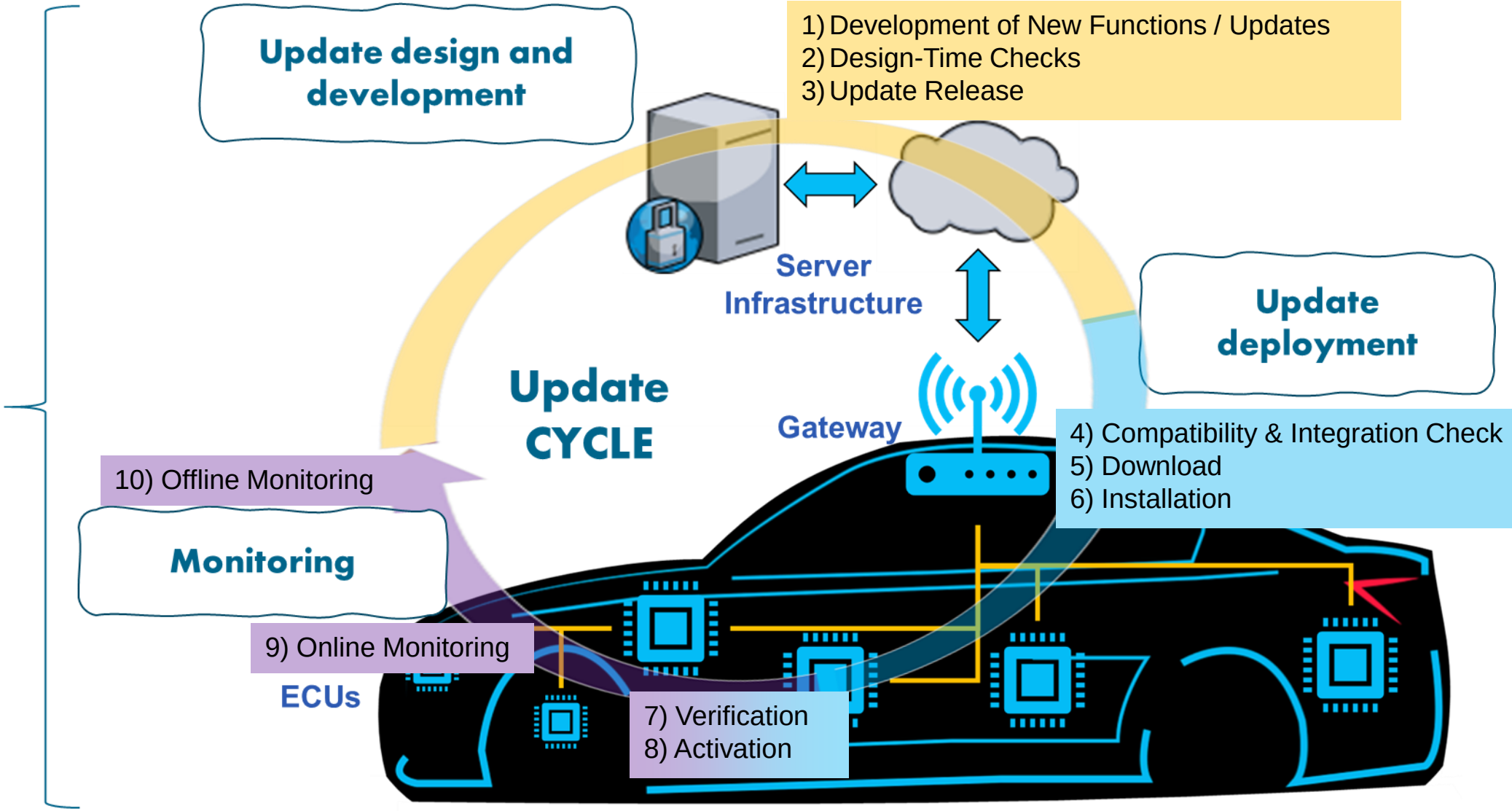
UP2DATE (HORIZON2020, 2019-2022)

https://h2020up2date.eu/

A holistic OTA SW update paradigm (Concept & Prototype)

Formalisms, Processes, and Guidelines for:

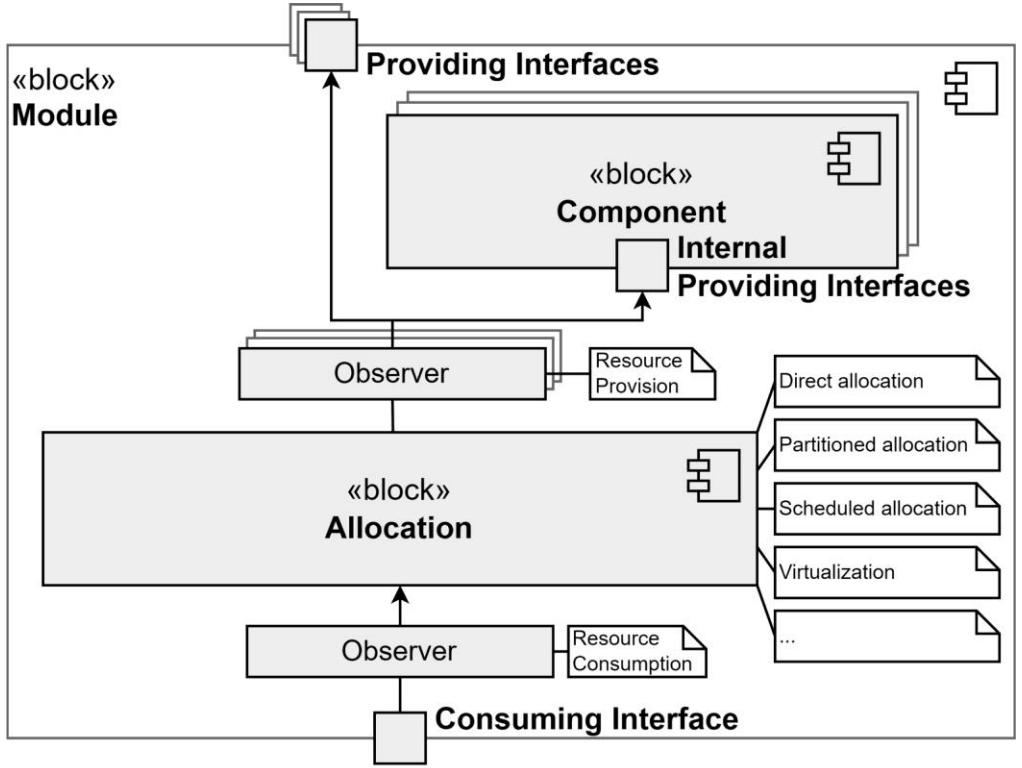
- SW-Updates
- updateable HW-/SW-Platforms
- Dev-Phase, Ops-Phase, & Deploy-ment
- the Server-Fleet-SoS

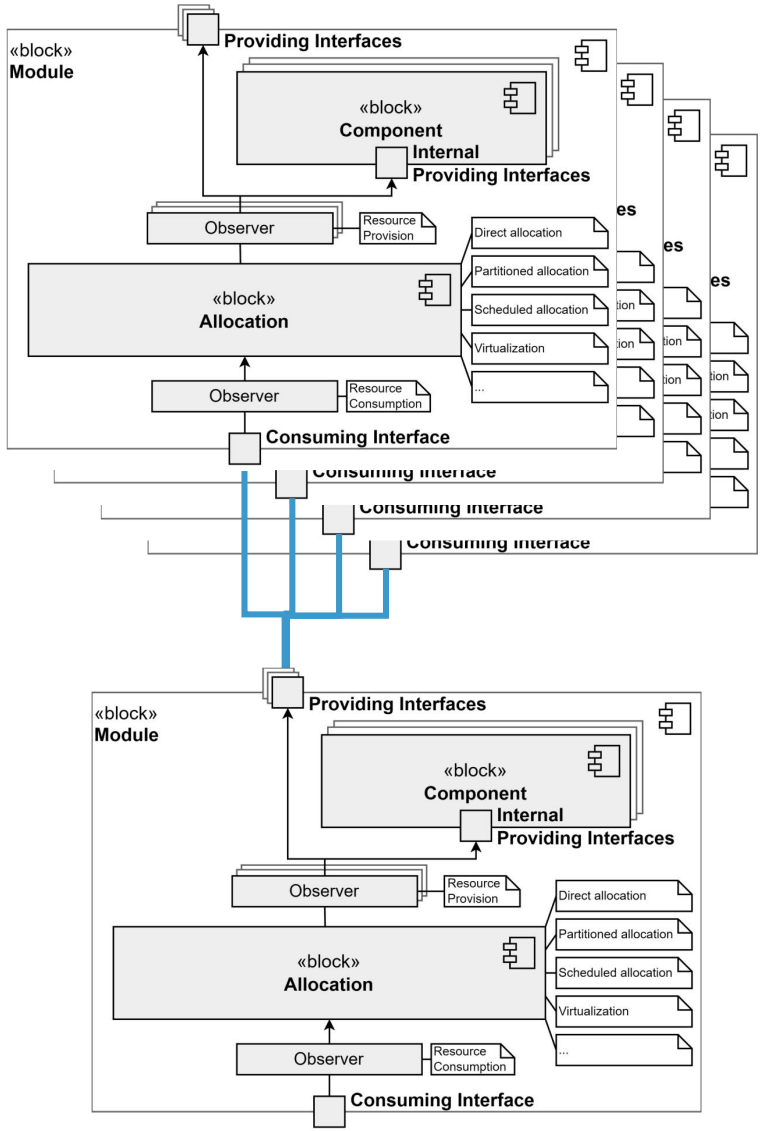


AutoDevSafeOps (BMBF, 2022-2025)

Virtual Module Integration

Patrick Uven, Ralf Stemmer, Gregor Nitsche, **A modular architecture template for resource modeling in Software-Defined Vehicles. EDCC 2025.**





UP2DATE (HORIZON2020, 2019-2022)

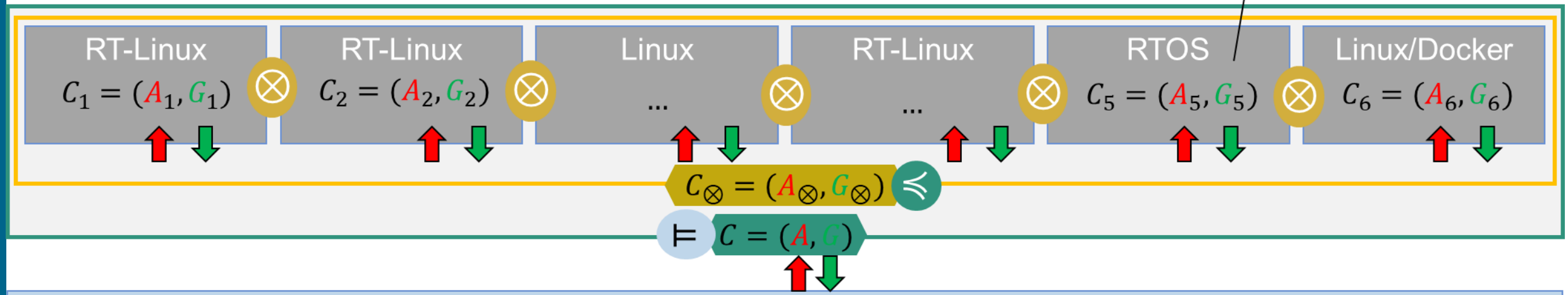
https://h2020up2date.eu/

Contract-Based Compatibility Checking (Concept & Prototype)

A: StartImageProcessing occurs every 5ms.
G: Reaction (StartImageProcessing, StopImageProcessing) within [0, 3]ms.

Frame-Processing

A: OS_CFGID = "OS__Ubuntu_18_04_4_LTS__Linux_4_9_140_rt93_aarch64_aarch64_aarch64_GNU_Linux_"; AND
HV_CFGID = "HV_QEMU_emulator_version_2_11_1_Debian_1_2_11_dfsg_1ubuntu7_39__4_0_0_"; AND
CPU-SET = { 1x "CPU_aarch64_Nvidia_fp_asimd_evtstrm_aes_pmull_sha1_sha2_crc32_atomics_fphp_asimdhp_cpuid_asimdrdm_dcpop_"};
G: CPU-SET = { 1x "CPU_aarch64_Nvidia_fp_asimd_evtstrm_aes_pmull_sha1_sha2_crc32_atomics_fphp_asimdhp_cpuid_asimdrdm_dcpop_"};



Virtual Integration and Verification

Update time HCMC check

Online Monitoring

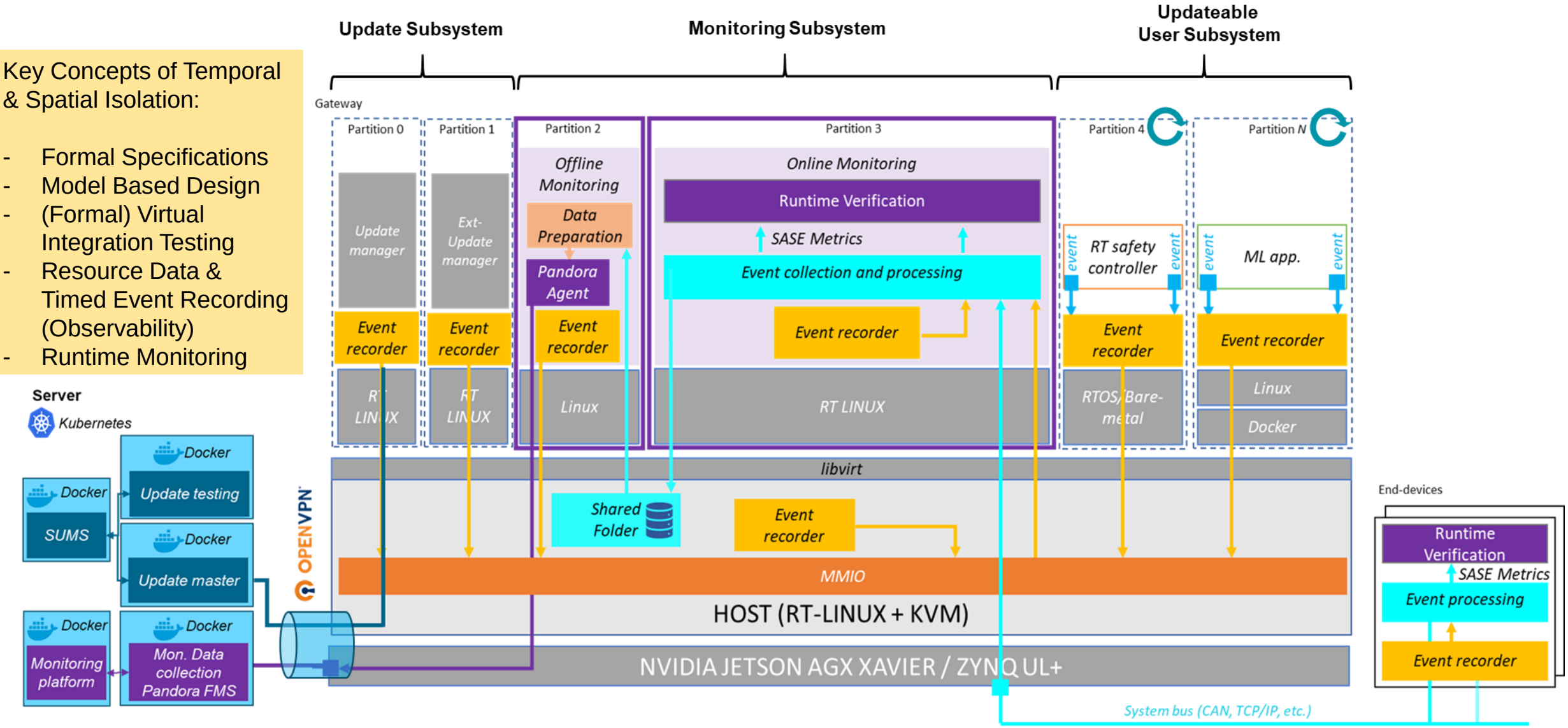
UP2DATE (HORIZON2020, 2019-2022)

https://h2020up2date.eu/

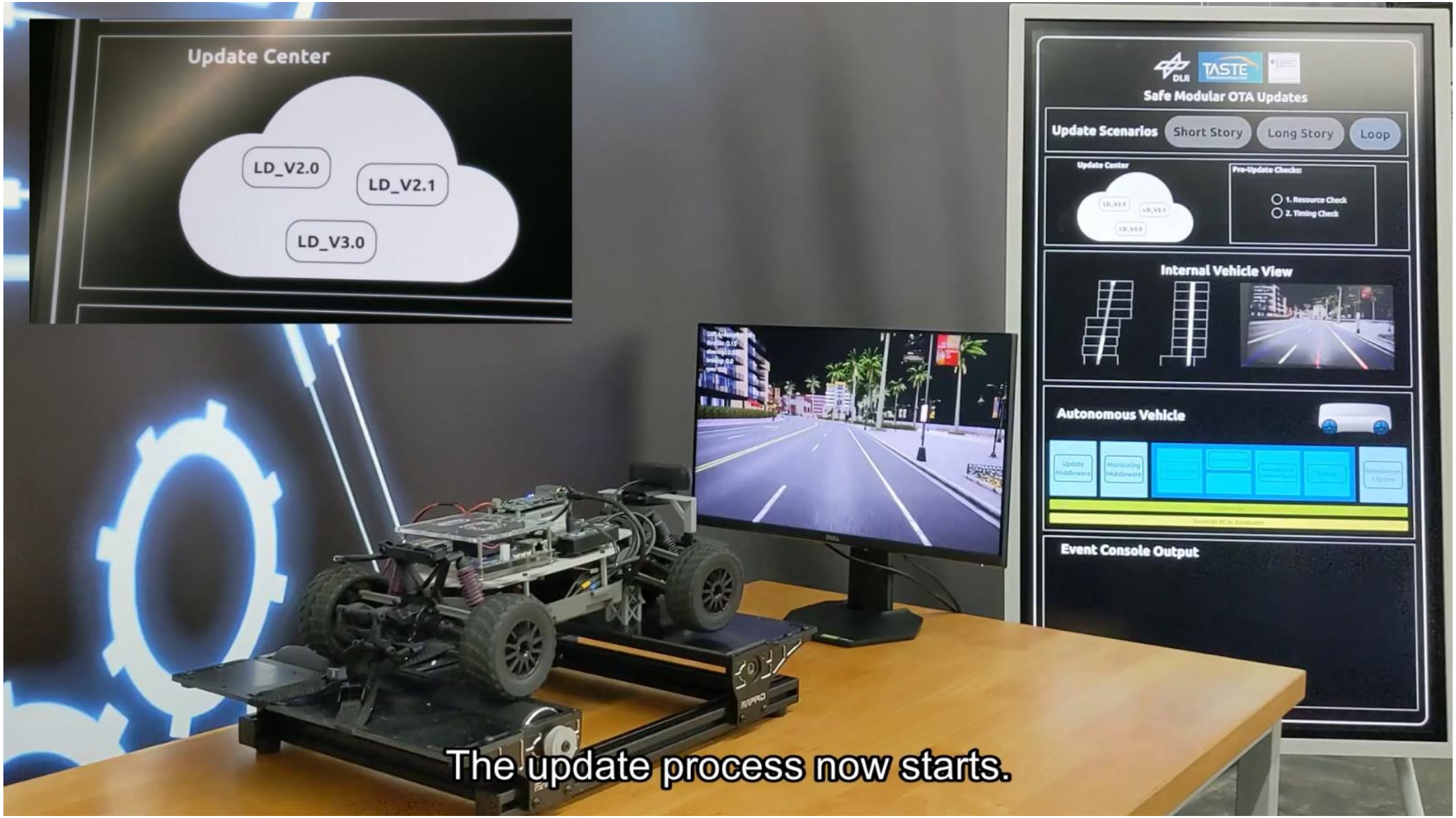
An updateable system architecture (Concept & Prototype)

Key Concepts of Temporal & Spatial Isolation:

- Formal Specifications
- Model Based Design
- (Formal) Virtual Integration Testing
- Resource Data & Timed Event Recording (Observability)
- Runtime Monitoring



AMDEV: Automotive Model Demonstration Evaluation & Verification-Bed



UP2DATE4SDV (HORIZON Europe, 2025-2028)

Incremental deployment of L4+ CAD
in road vehicles
by safe- & secure, modular SW-updates,
HW-upgrades & C2C2 task-reallocation in
SD-CCAM-V architectures.

O4: Cloud-centric CI/CD- and DevOps-framework for design, integration and V&V

O3: Dynamic car2cloud/cloud2car (C2C2) orchestration & reconfiguration plane (ORP)

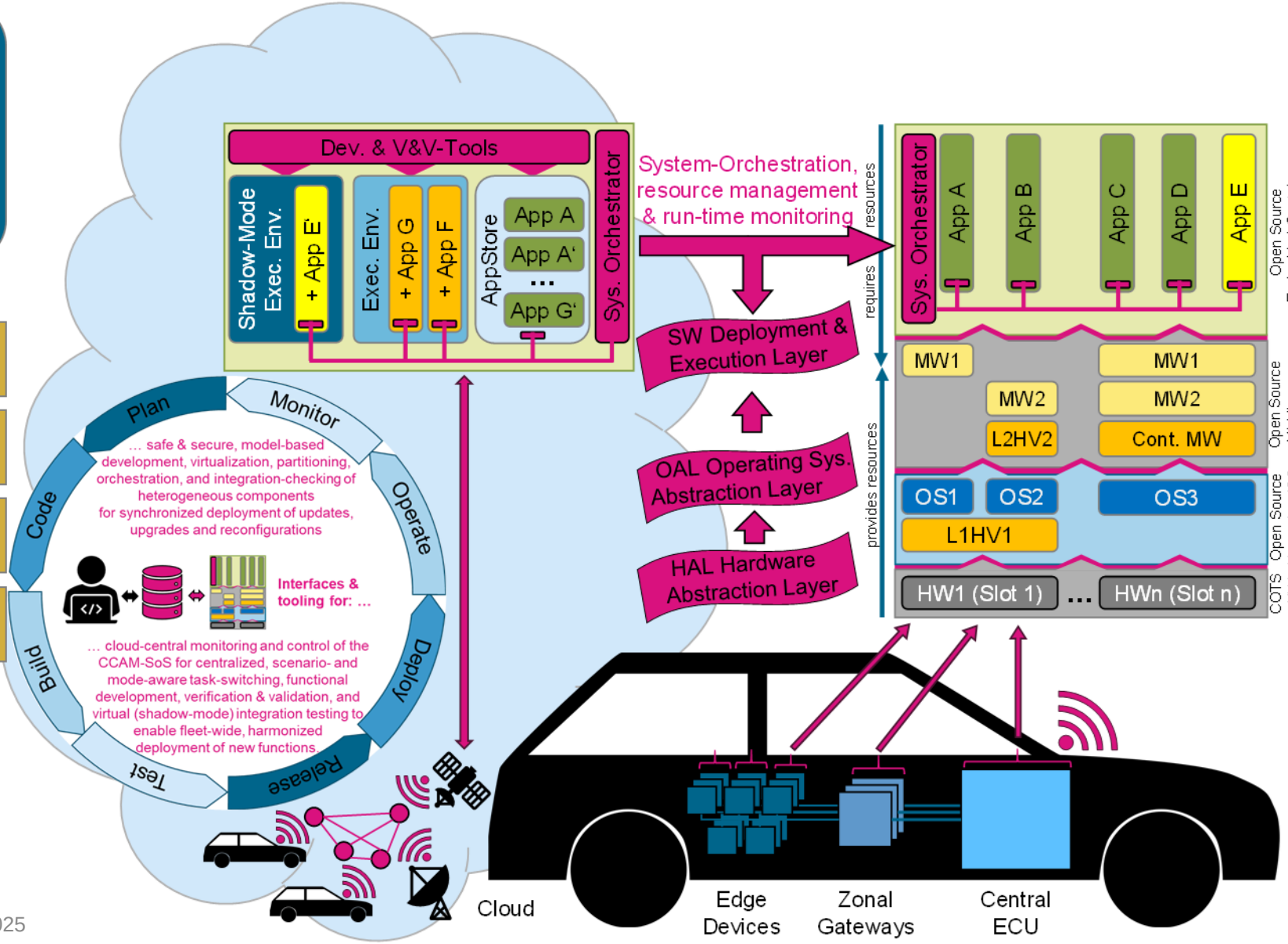
O2: Resource composable SW deployment and execution reference layer (OAL)

O1: Reconfigurable, cloud-connected zonal vehicle HW architecture blueprint (HAL)

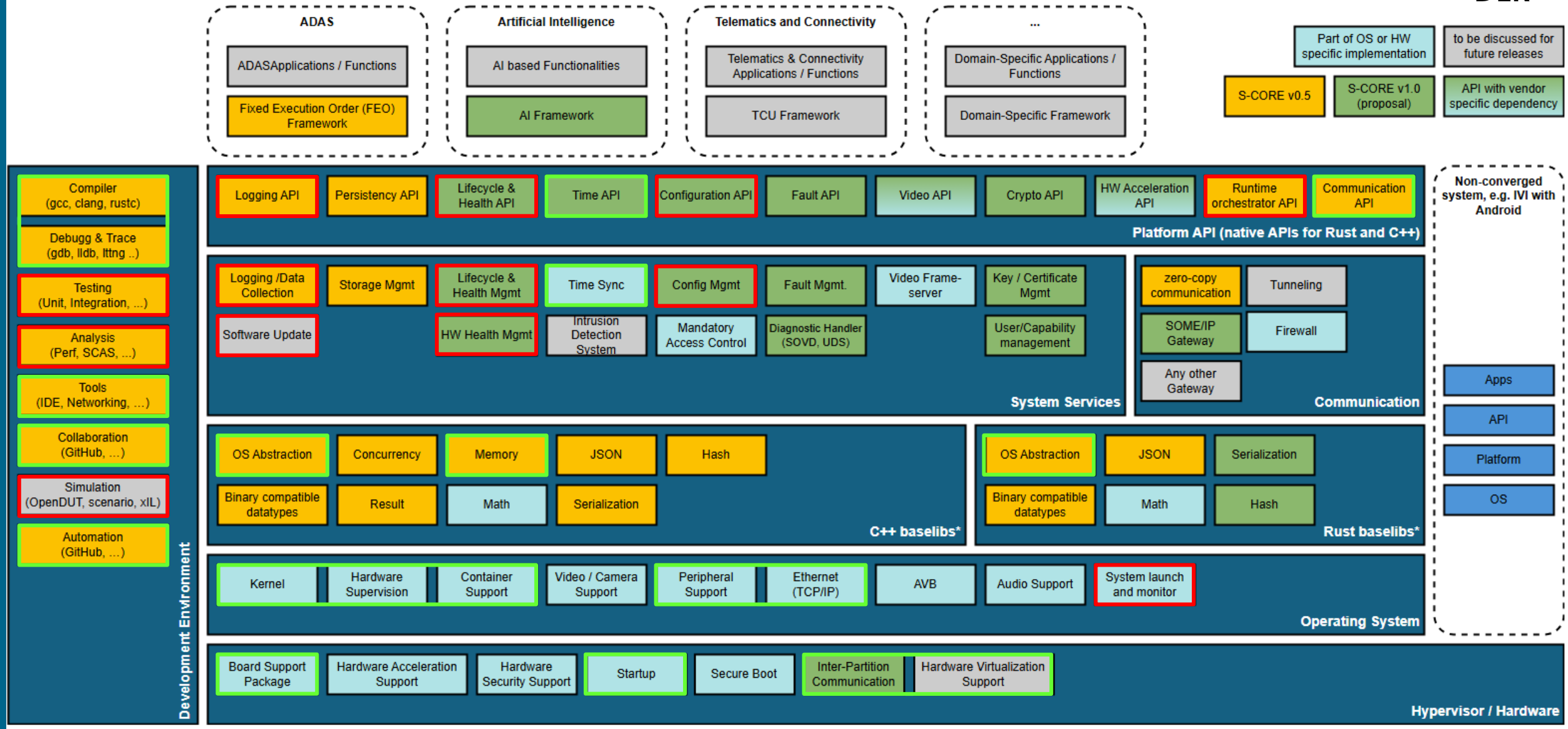
Modularization, Monitoring & Control

Safety- & security-driven MBSE

SDV-Initiative & CCAM-partner. -cooperation

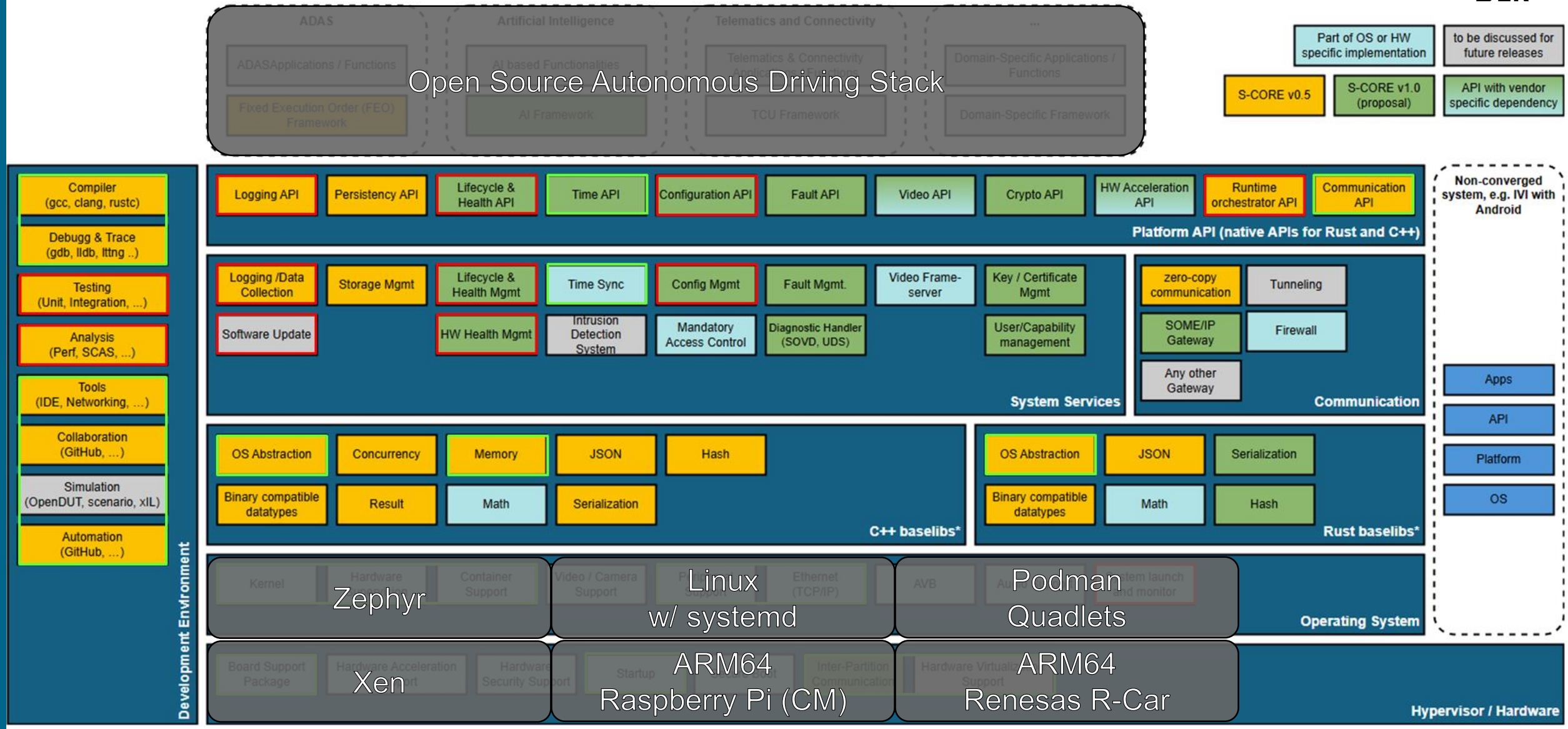


Outlook
(possible contributions & interactions)



Source: https://eclipse-score.github.io/score/main/score_releases/index.html#releases

Outlook
(possible contributions & interactions)



Source: https://eclipse-score.github.io/score/main/score_releases/index.html#releases

Conclusion

- SW integration is a major bottleneck for tomorrow‘s (CCAM/AD) vehicles

  → software modularity and observability at model and code level is key

- in UP2DATE we developed and integrated formal, model-based concepts of a safe- & secure update cycle based on CBD, VIT and runtime-monitoring

- in UP2DATE4SDV we extend this approach to a modular, zonal SD-CCAM-V architecture that is updatable, reconfigurable, and virtually testable from the cloud

Conclusion

- DLR is (more than) Rocket Science → we are also doing SDV
- We have a societal responsibility; thus we
  - value open source as an enabler for scientific and industrial cooperation and success
  - practice applied research along the needs of the German/European industries
  - strive towards fair, green, and efficient transportation technologies, and
  - consider SDV and Safe & Secure OTA SW updates to be a key factor to achieve that
- We want to contribute to / integrate with SDV (open source) projects, like:
  - Eclipse SDV (S-CORE, uProtocol, Velocitas, Symphony, openDUT, …)
  - Safe (automotive), open Operating Systems (ELISA, AGL, …) and Hypervisors (XEN)

QUESTIONS AND DISCUSSION

Quelle: https://pixabay.com/de/photos/frage-fragen-fragezeichen-einzel-6387294/

Imprint

Topic:	Safe and Secure Over-the-Air Software-Updates for Software-Defined Vehicles
Date:	2025-06-04
Author:	Gregor Nitsche (with contributions of many colleagues at DLR SE)
Institute:	Systems Engineering for Future Mobility (SE)
Image sources:	All images “DLR (CC BY-NC-ND 3.0)” unless otherwise stated