

Advancing concepts and implementations of

Safe-and-Secure OTA Software Updates

from UP2DATE to UP2DATE4SDV

Gregor Nitsche (DLR), 05.11.2025



Funded by
the European Union



DLR is (more than) Avionics and Rocket Science:



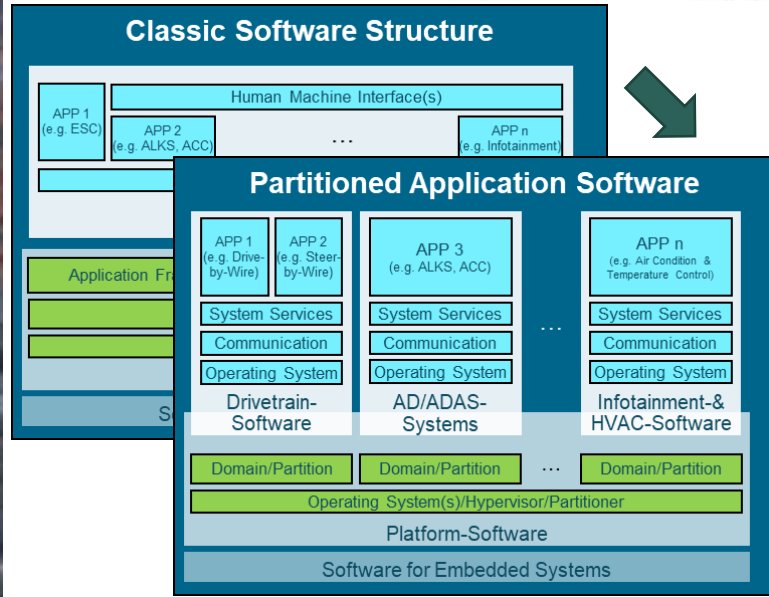
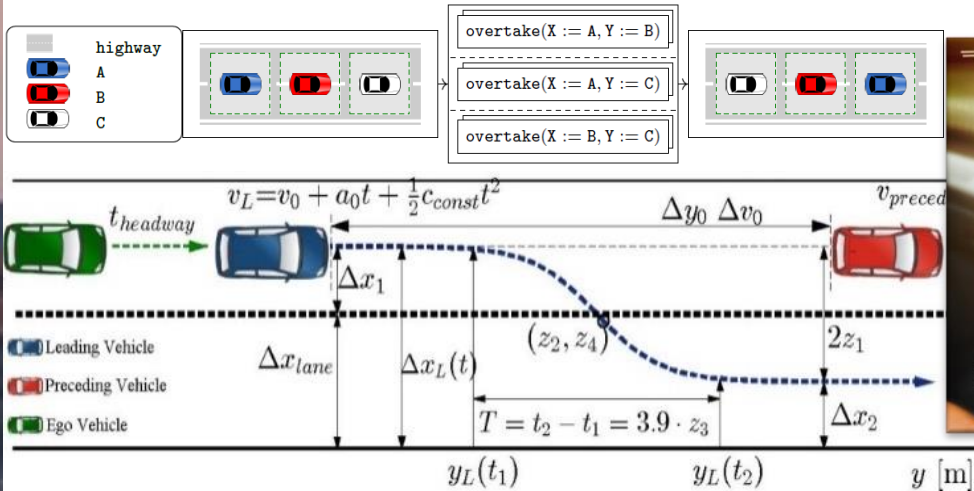
DLR is (more than) Avionics and Rocket Science: ... it is Avionics, Space, Energy, and Transportation



DLR is (more than) Avionics and Rocket Science: ... in transportation it is maritime, rail & automotive



DLR is (more than) Avionics and Rocket Science: ... and it is also researching on AD & SDV

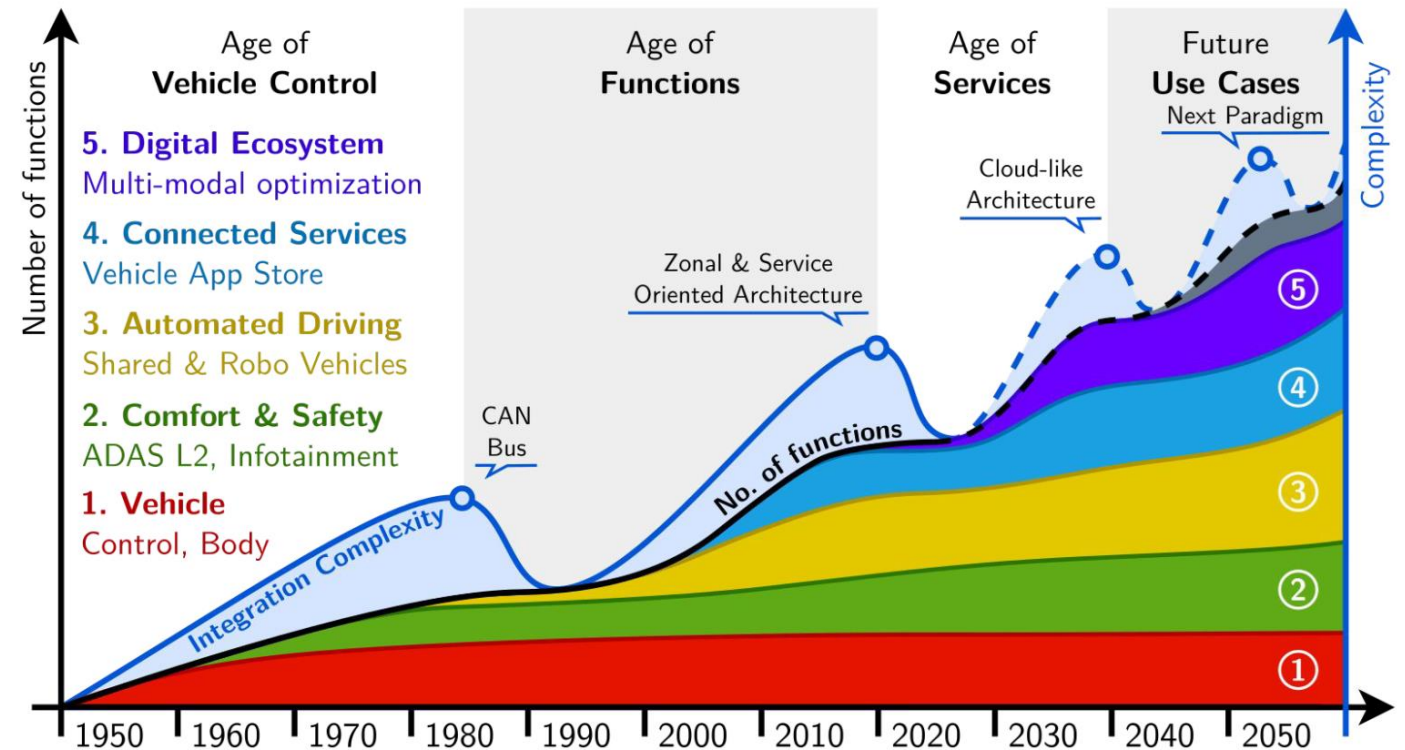
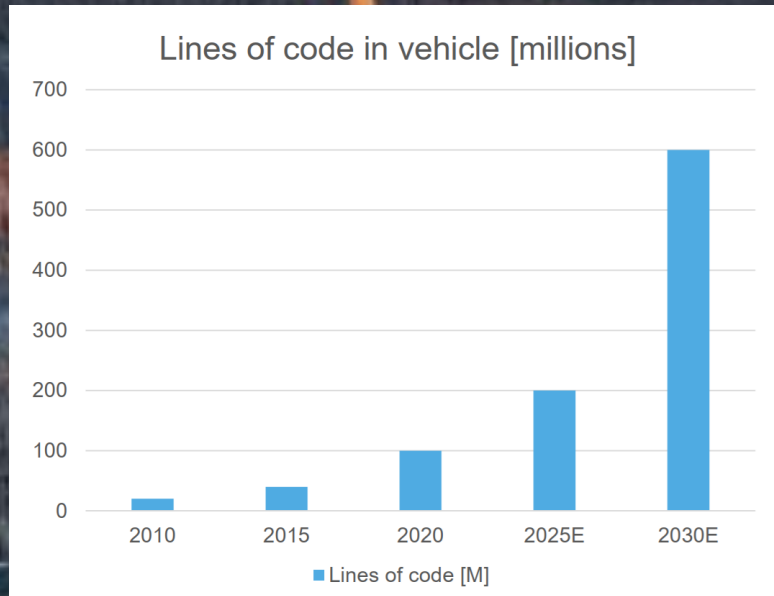


→ Motivation of Updates: We don't believe in the 'Shoot to the Moon' approach for AD or SDV



- 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

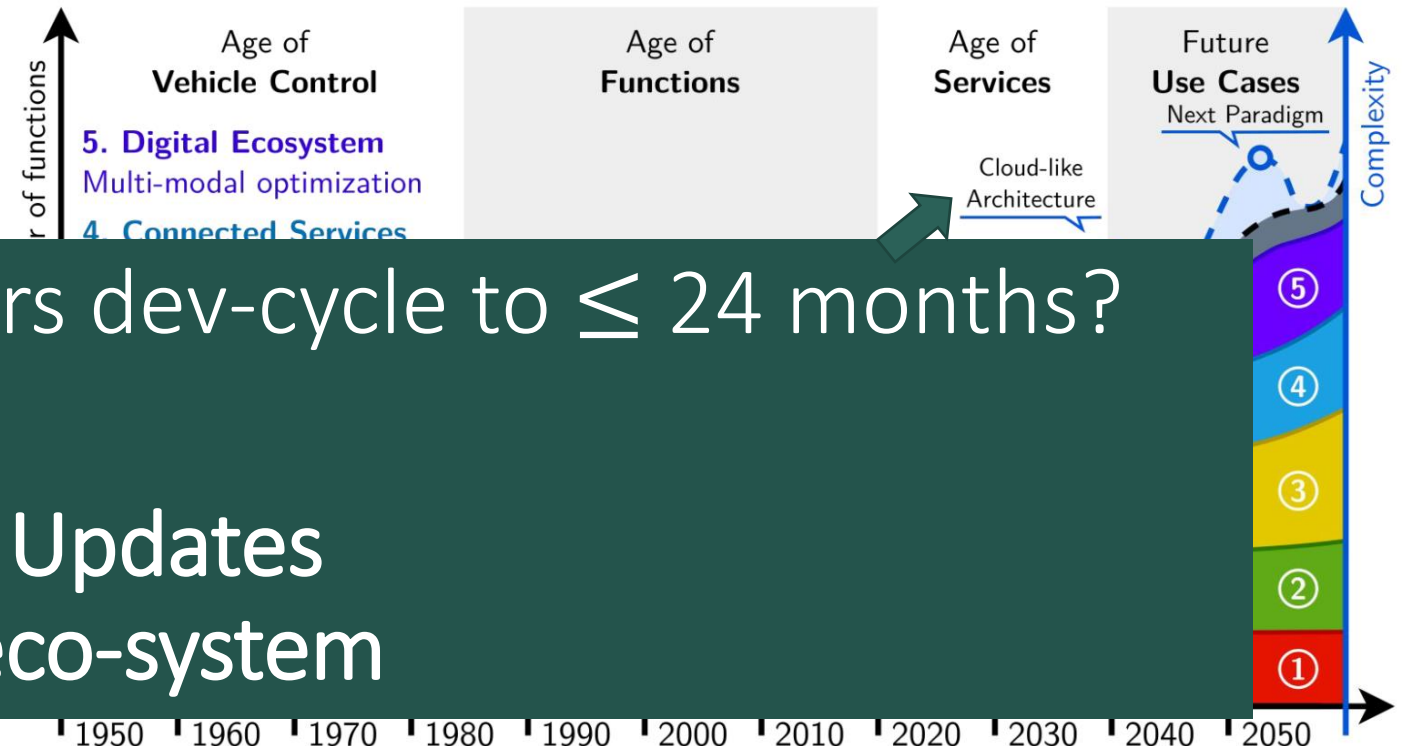
→ Motivation of Updates: What shoots to the moon is complexity and integration & test effort



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_cQNZYwI4x&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)

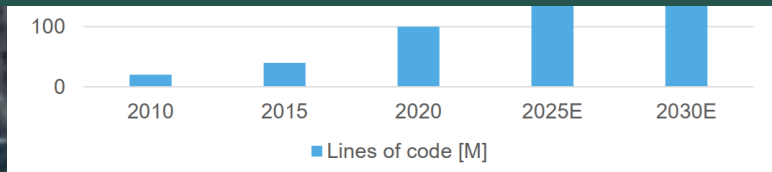
→ Motivation of Updates: What shoots to the moon is complexity and integration & test effort



How to compress 4-5 years dev-cycle to ≤ 24 months?

our contribution:

Safe-and-Secure Modular Updates
+ an update-centric SDV eco-system



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_cQNZYwI4x&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)

Research & Support Activities



- **CSA Federate**

- SDV of the Future (SDVoF) Initiative

- SDV Manifesto

- EU Automotive Action Plan

- & European Connected and Autonomous Vehicle Alliance (ECAVA)

- **Eclipse Safe Open Vehicle Core (S-CORE)**

- non-differentiating OSS core of a software stack running (ASIL-B) on HPC ECUs



- **RIA HAL4SDV**

- unifying software interfaces and development methodologies to abstract from HW



- **RIA SHIFT2SDV**

- common SDV MW framework, API, and flexible micro-services-based architecture



- **RIA UP2DATE4SDV**

- ecosystem for SW updates, HW upgrades and reconfigurations



Research & Support Activities



- **CSA Federate**

- SDV of the Future (SDVoF) Initiative

- SDV Manifesto

- EU Automotive Action Plan

- & European Connected and Autonomous Vehicle Alliance (ECAVA)

- COVESA, SOAFEE, AUTOSAR
- CATENA-X
- EEA4CCAM
- TWINLOOP
- CODE4EV
- RIGOLETTO

...



ment methodologies

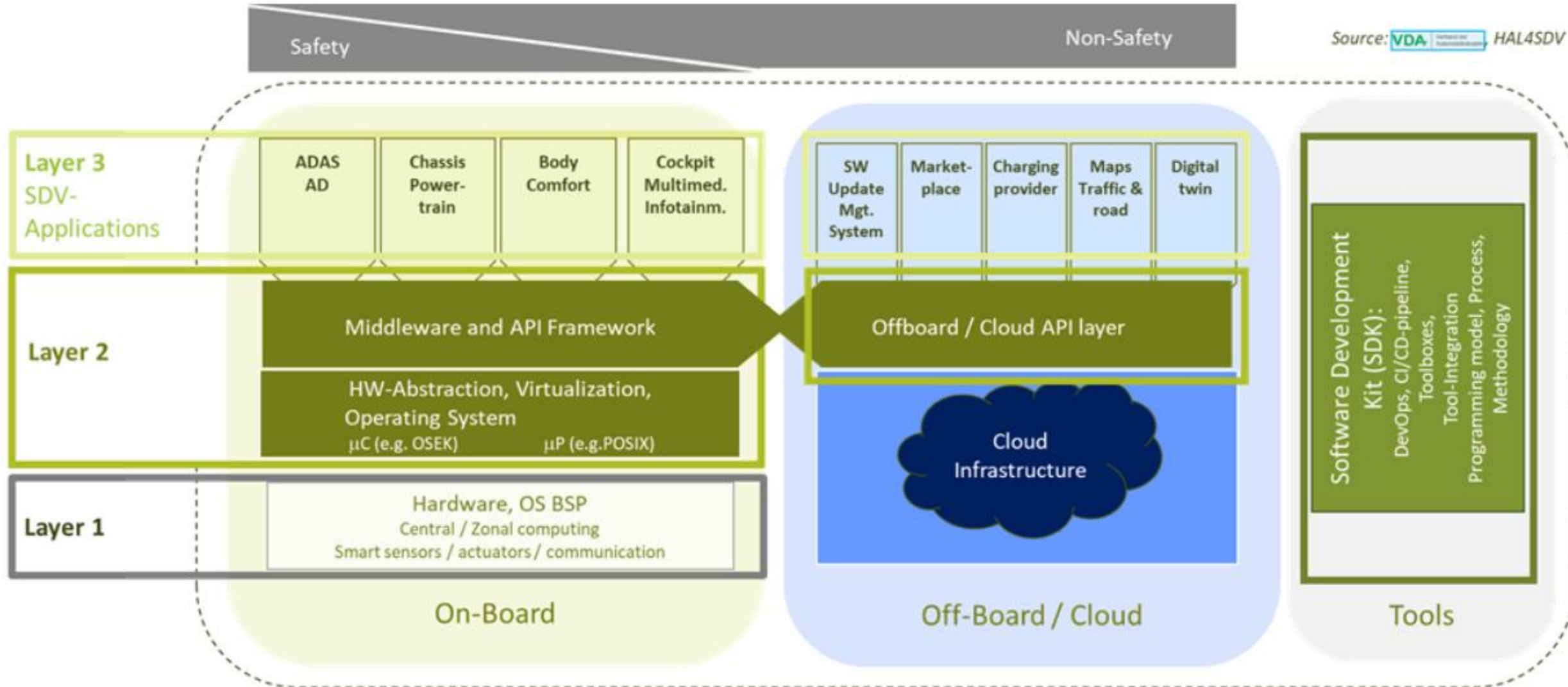


- **RIA UP2DATE4SDV**

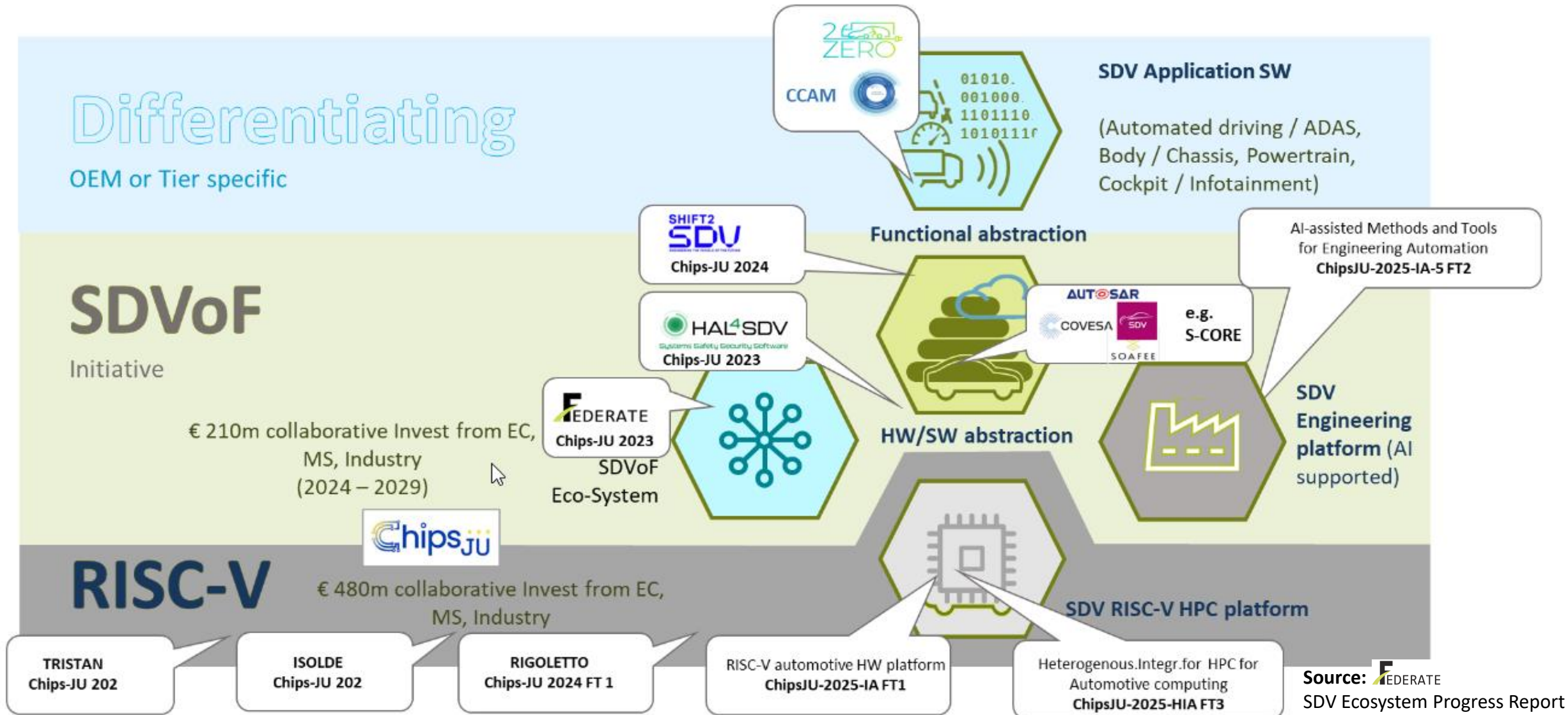
- ecosystem for SW updates, HW upgrades and reconfigurations



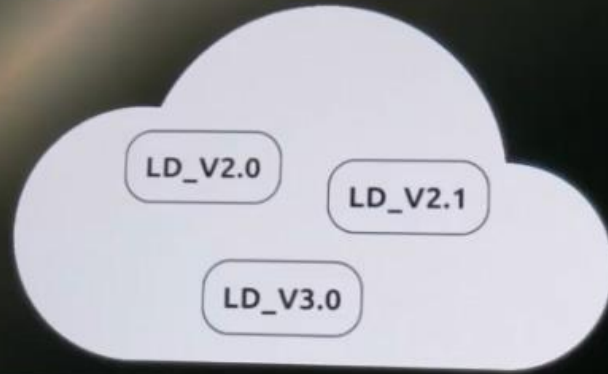
Research & Support Activities



Research & Support Activities



Update Center



Safe Modular OTA Updates

Update Scenarios **Short Story** Long Story Loop



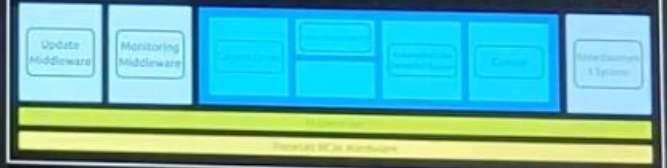
Pre-Update Checks:

- ☐ 1. Resource Check
- ☐ 2. Timing Check

Internal Vehicle View



Autonomous Vehicle



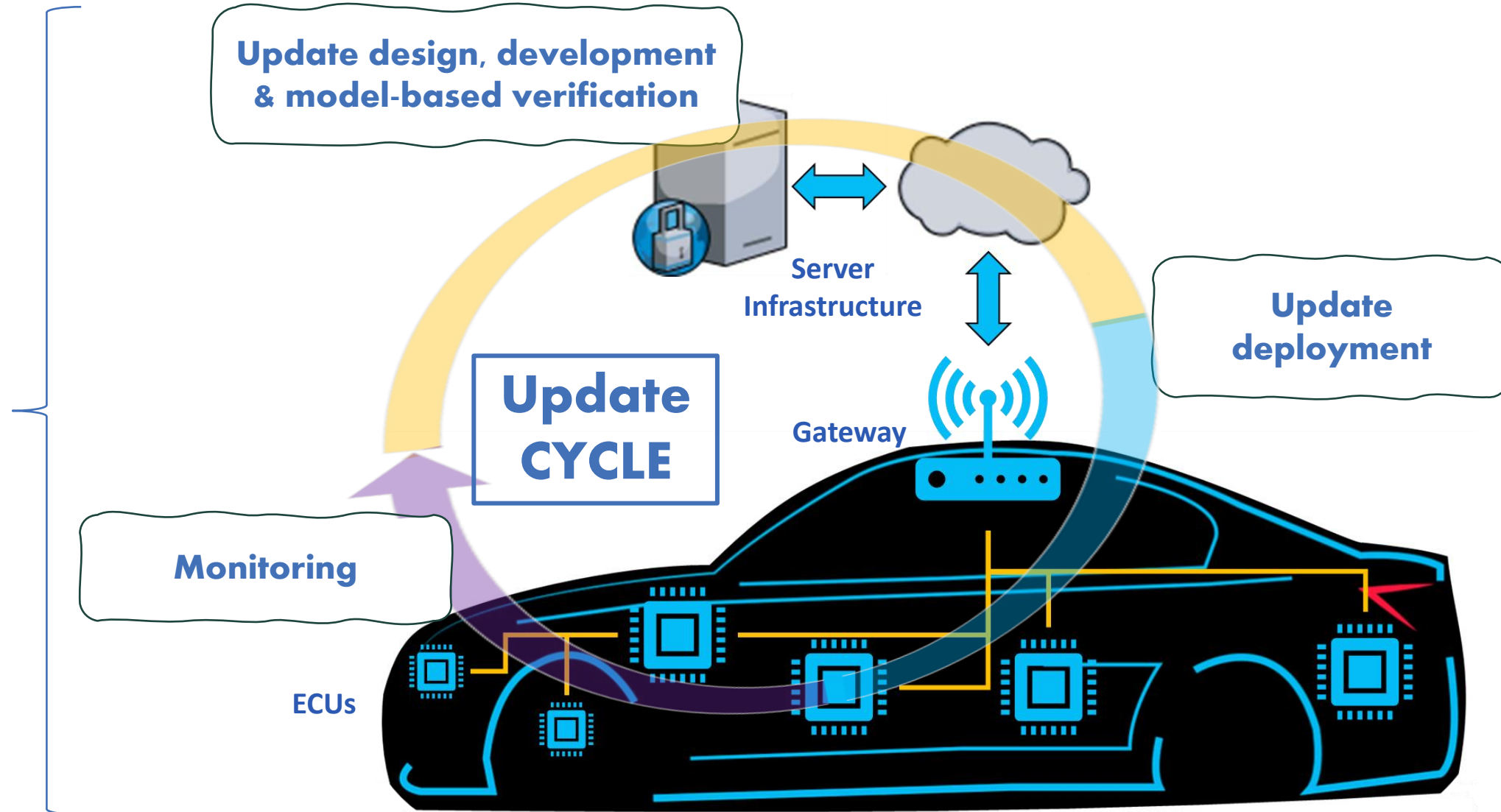
Event Console Output

The update process now starts.

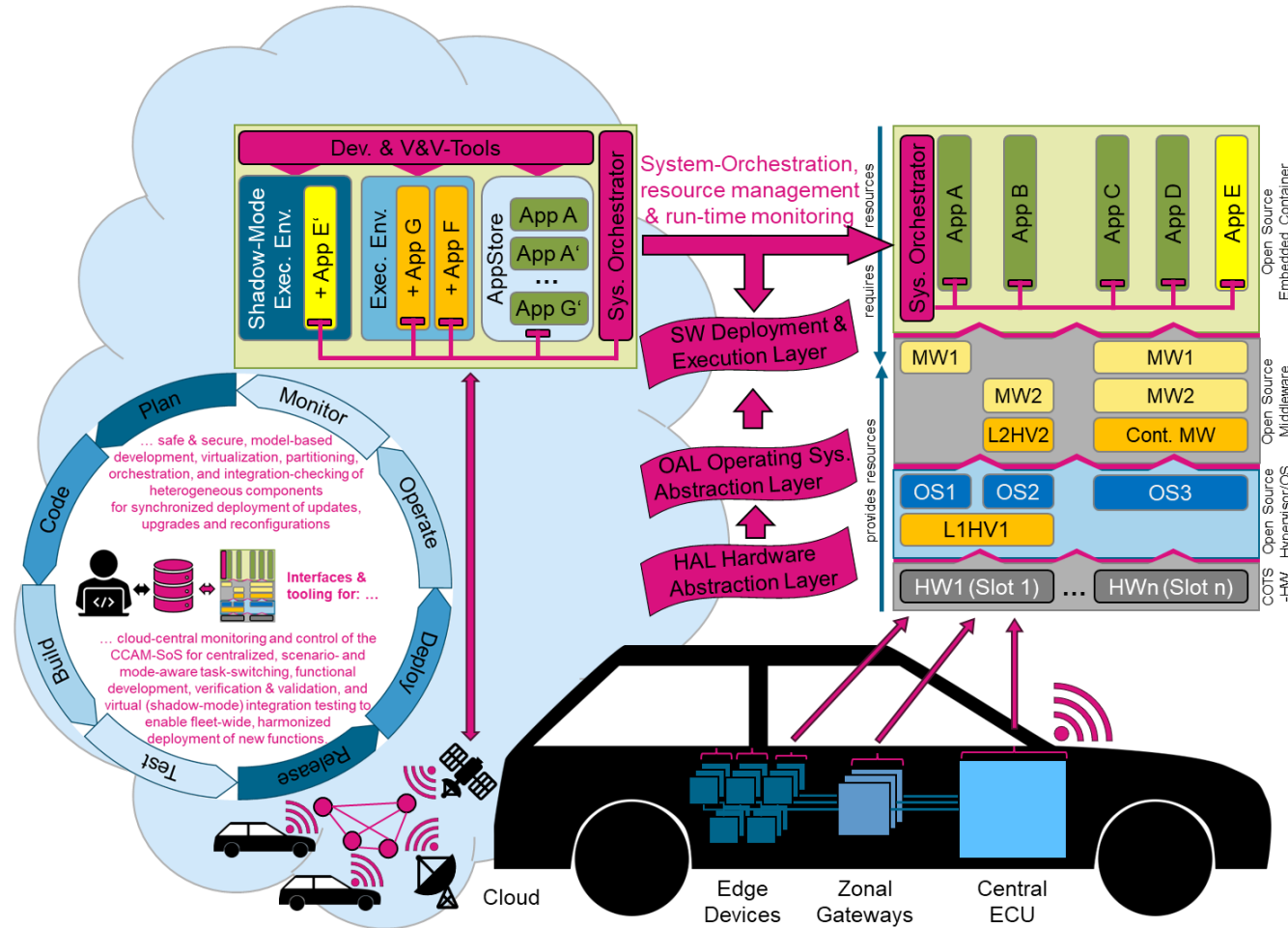
The Base: A holistic OTASU paradigm

Formalisms,
Processes, and
Guidelines for:

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

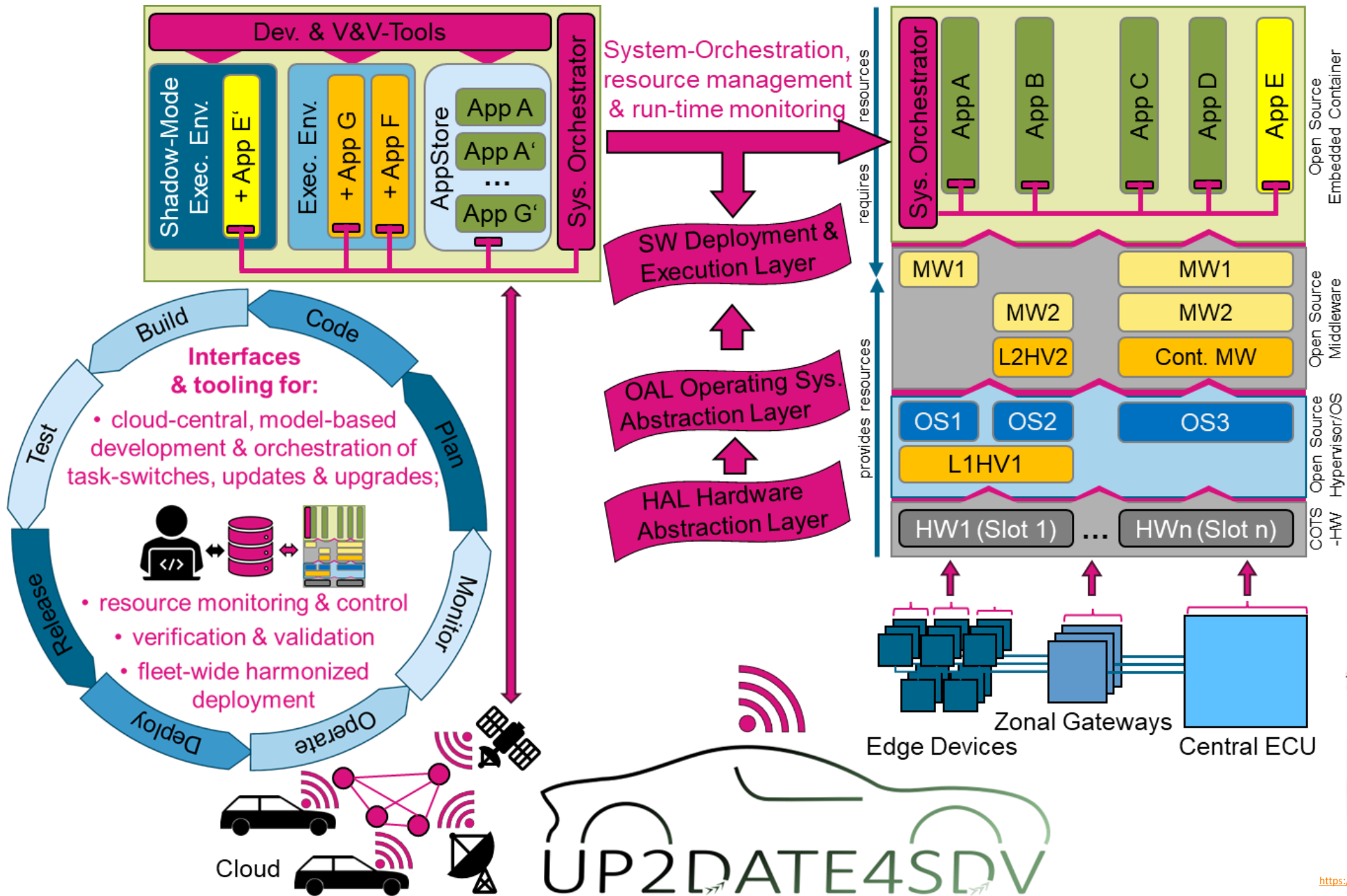


The Goal



“UP2DATE4SDV aims

... to develop a **comprehensive ecosystem** for seamless and efficient **software-updates, hardware-upgrades, and situation-dependent reconfigurations** of software-defined CCAM vehicles”



Conclusion



- DLR is (more than) Avionics and Rocket Science
- Complexity, integration & test effort* shoots to the moon
(*of automotive SW & E/E architecture)
- Europe is facing this challenge*
(*with coordinated research & support activities richly advised by industries)
- DLR provides solutions for **Safe-and-Secure Modular OTA Software Updates**
 - Full stack oriented: centralized HPC(-cluster), HV/OS/MW, DevOps-EcoSystem
 - Full DevOps-oriented: model-based (shift-left) + monitoring-based (stretch-right)
 - Resource-Focused: observation, monitoring, and control of CPU, MEM, ETH, ...



Gregor Nitsche

+49 441 770507-354

gregor.nitsche@dlr.de

<https://DLR.de>

German Aerospace Center (DLR)

Deutsches Zentrum für Luft- und Raumfahrt e. V.

Institute of Systems Engineering for Future Mobility (SE)

Escherweg 2 | 26121 Oldenburg

THANK YOU