DSC 2023

Special Session
ADAS / AD validation process targeting homologation

ArchitectECA2030 has been accepted for funding within the Electronic Components and Systems For European Leadership Joint Undertaking in collaboration with the European Union's H2020 Framework Programme (H2020/2014-2020) and National Authorities, under grant agreement n° 877539

Reference Homologation Process

Jürgen Niehaus

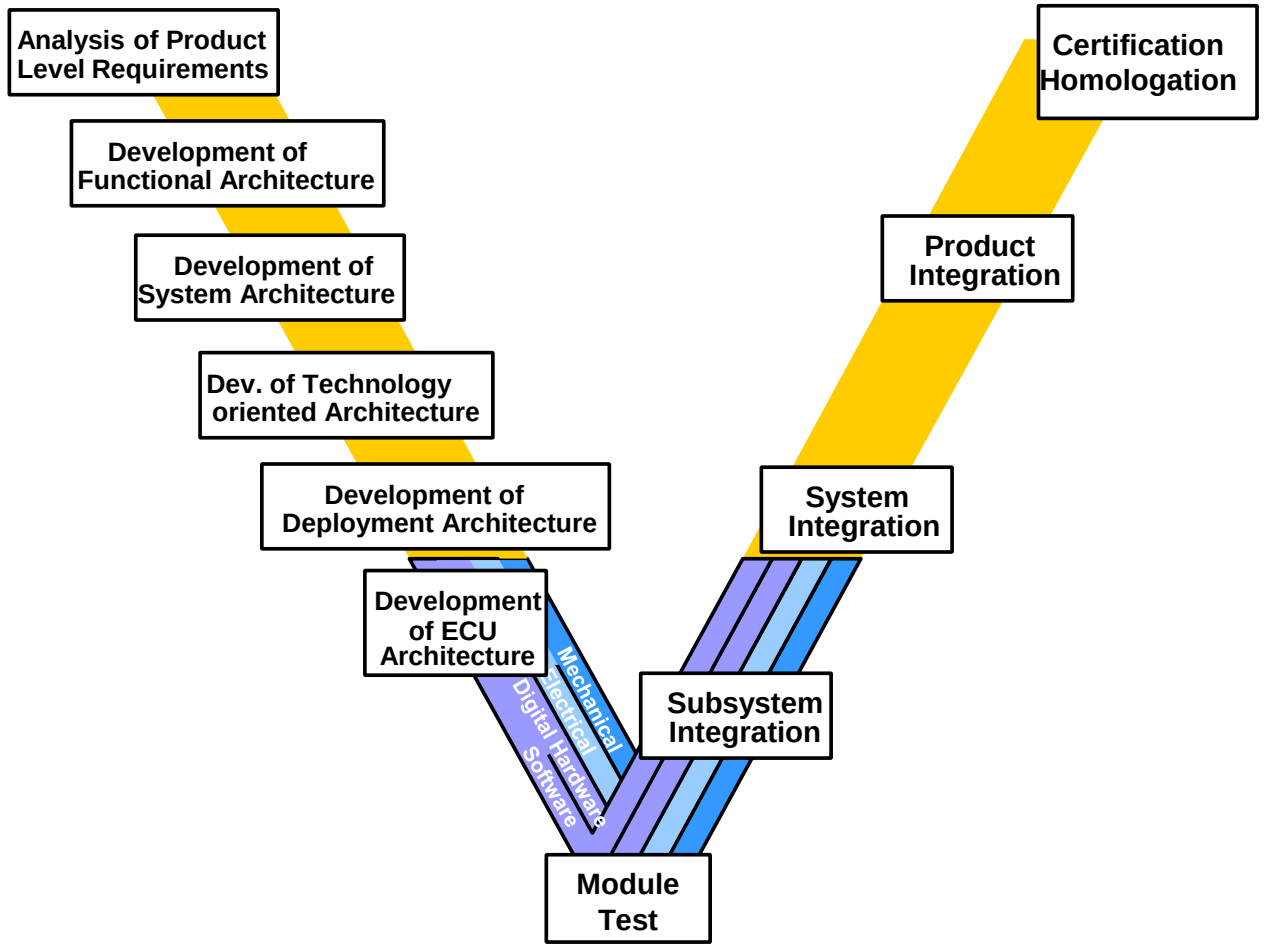
SafeTRANS
SAFETY IN TRANSPORTATION SYSTEMS

ECSEL
Joint Undertaking

Content

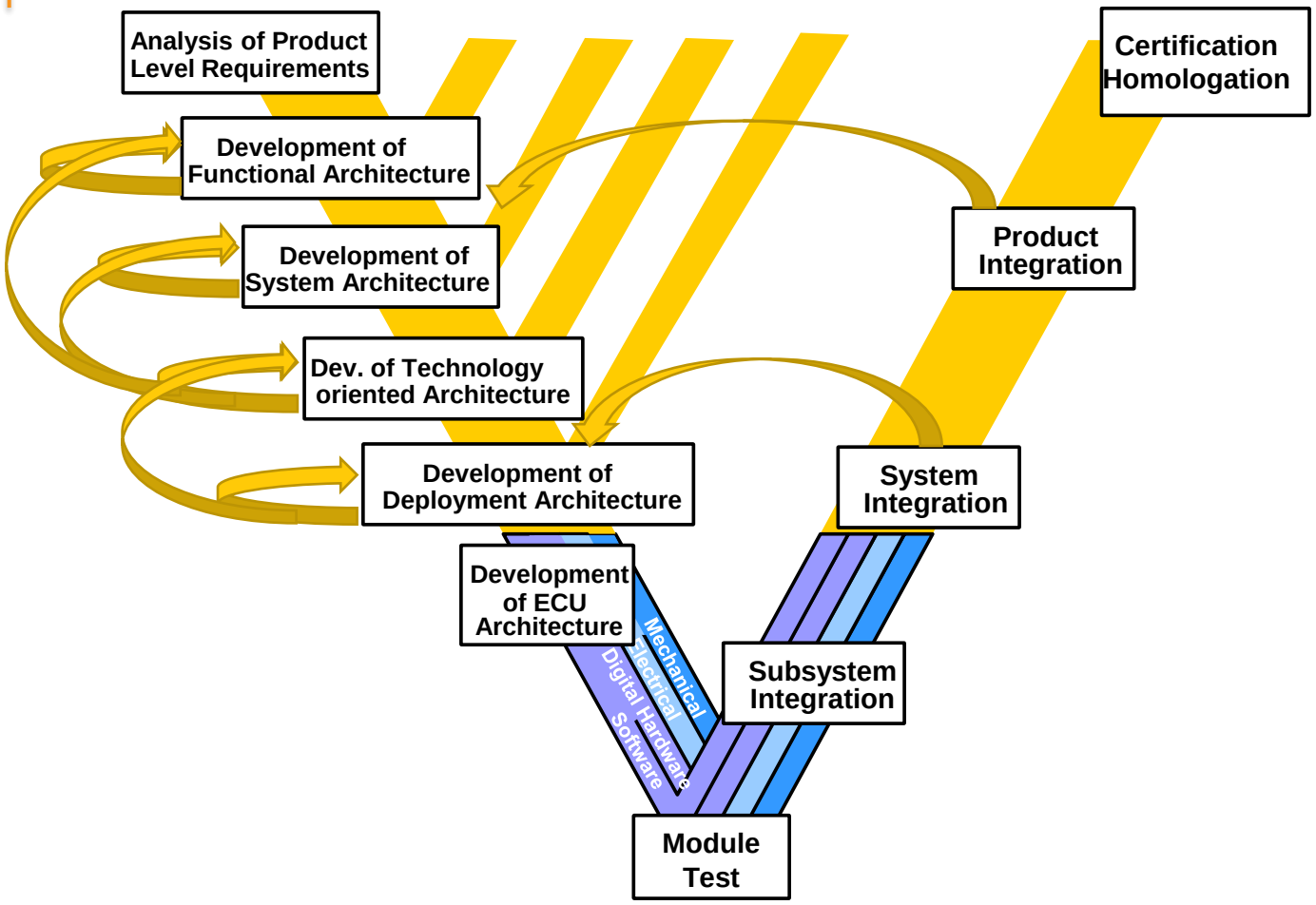
- Reference Homologation Process
  - a.k.a Reference Lifecycle Process
- Mapping Technology Bricks
  - Pegasus Family – Safety Analysis and Argumentation
  - Step-UP!CPS / AutoDevSafeOps – OTA Updates
  - ArchitectECA 2030 – Safety Architecture and Online-Monitoring
- Homologation
  - Regulations, Standards and Challenges

Reference Homologation Process



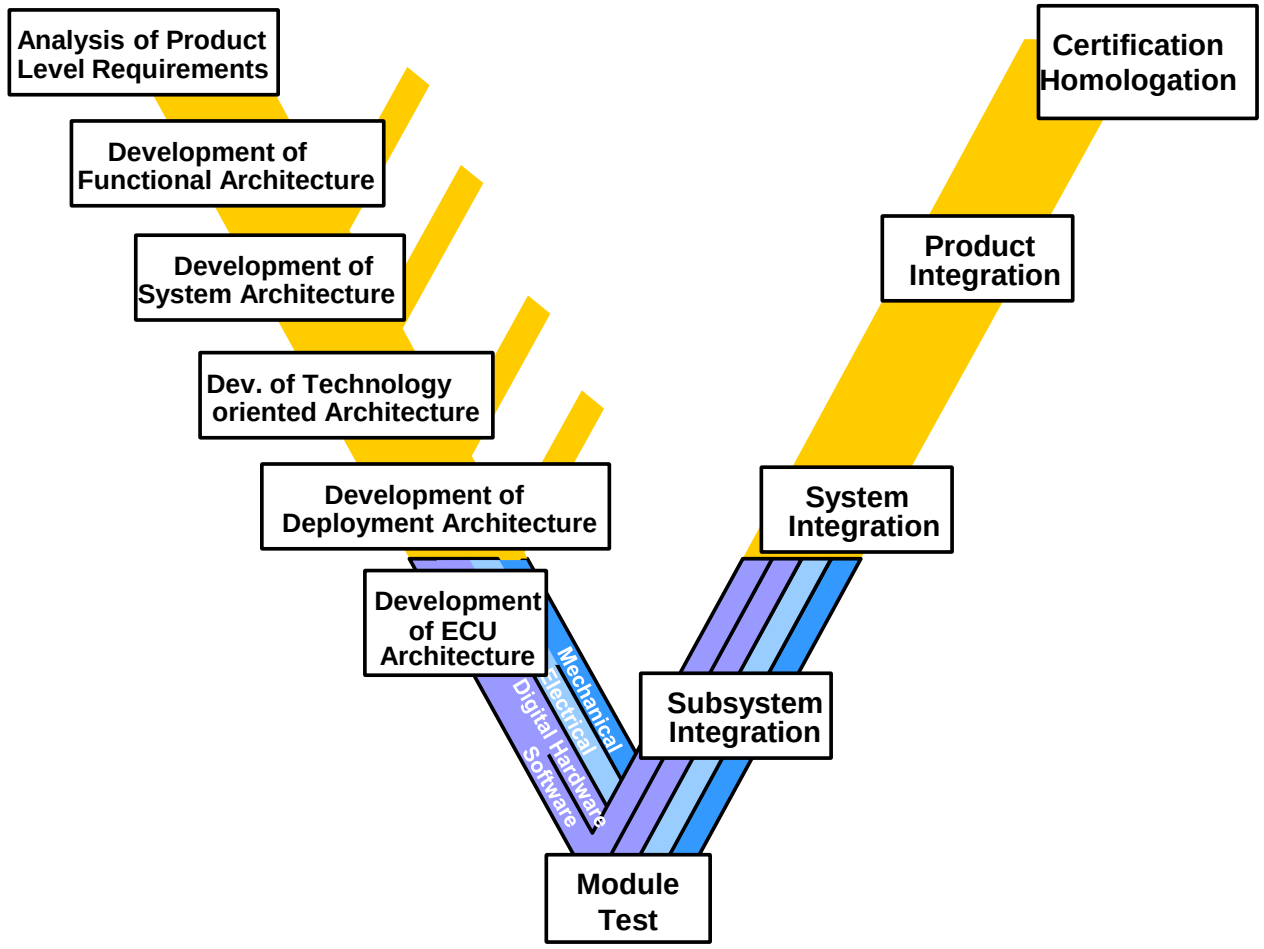
- Process description covering typical steps to
  - develop (design, implement, integrate)
  - validate (analyze, simulate, test, verify,…)
- Based on V-Model
- Model based, hierarchical design
  - System – Subsystems – Components – Modules
- Each step/substep defines ‚Design Artefacts‘ and the way in which they are created resp. tranformed.
- As a reference, not as a mandatory obligation

Reference Homologation Process

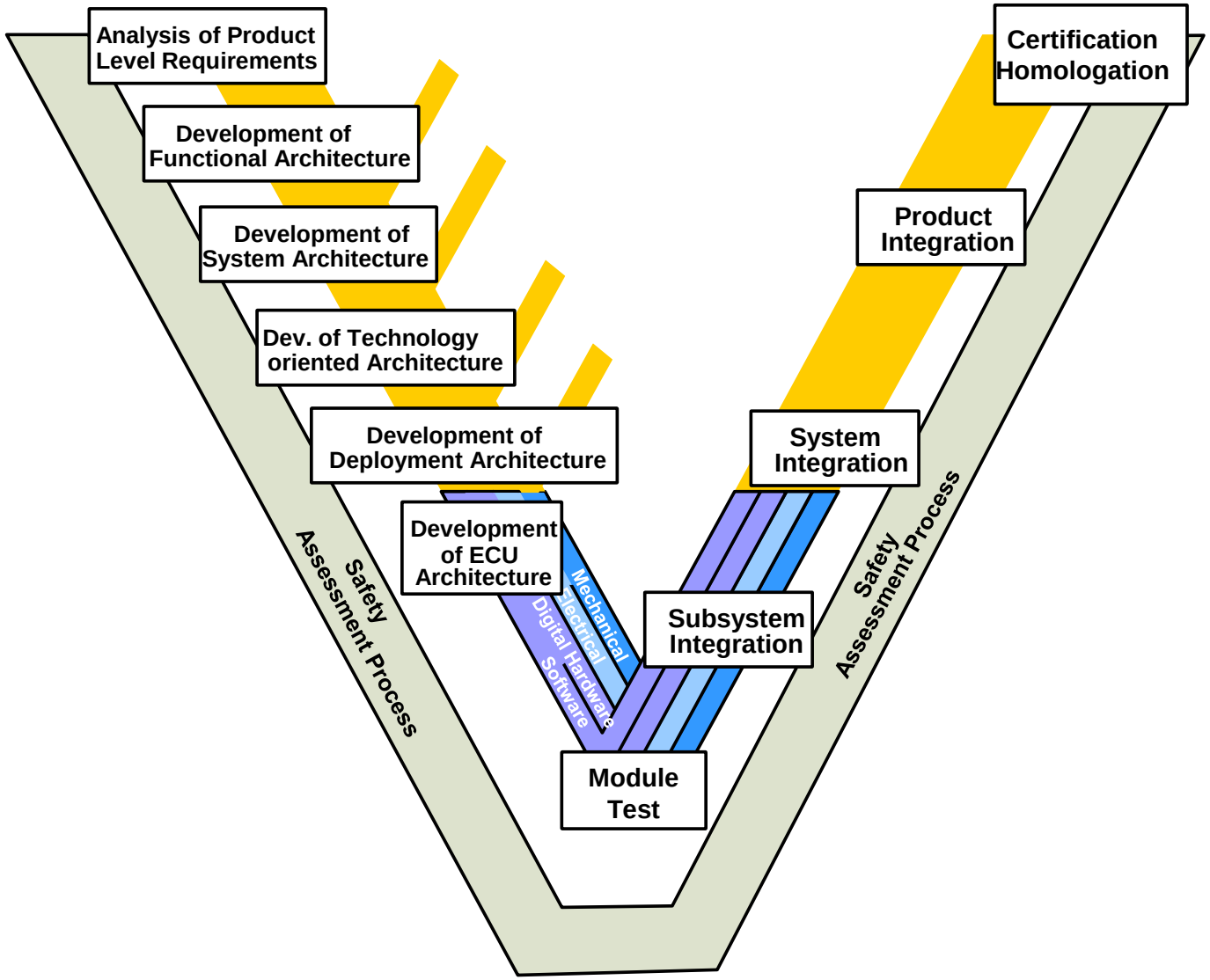


- For sake of clarity *in the pictures* wie ommit
  - Iterations, loops, backtracking,…
  - Early (prototype) integration and test (‚executable models‘)
  - Development for specific target architectures,…
  - Data bases, Libraries,…
  - …

Reference Homologation Process



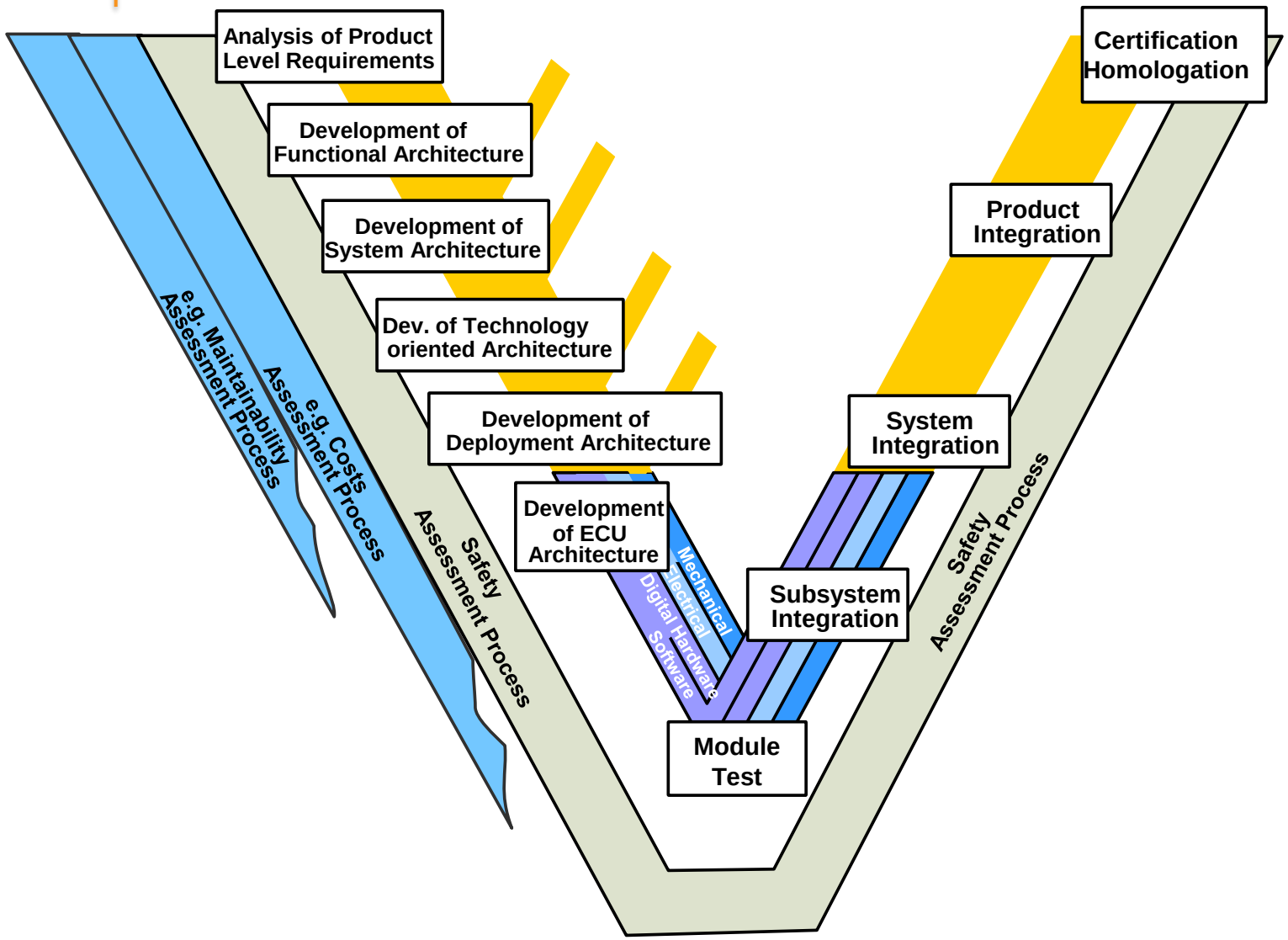
Reference Homologation Process



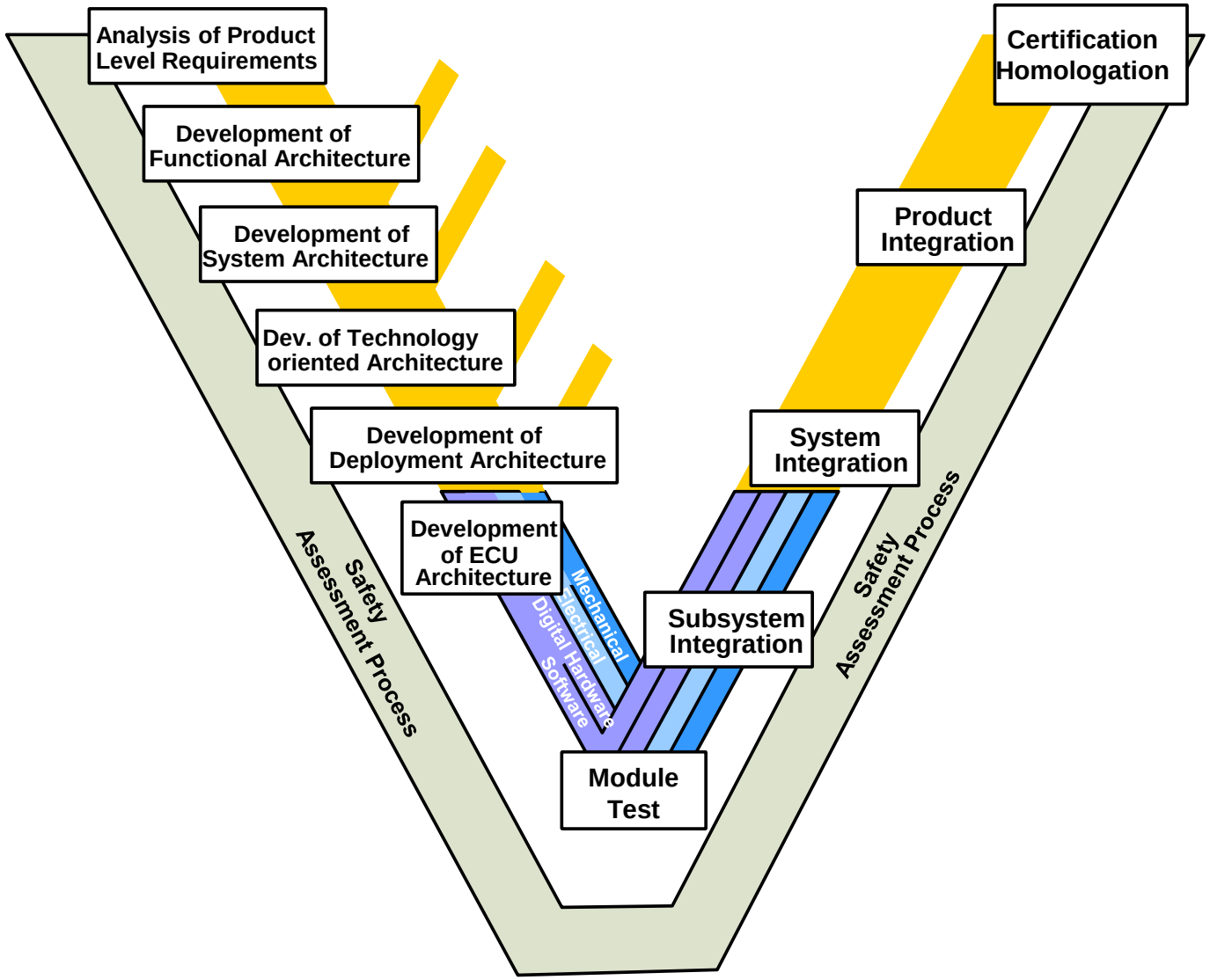
Safety Assessment Process

- Set-up Safety Assurance Case(s)
  - Structured Argument
  - CAE: Claims – Arguments -- Evidence
- Claims: Based on Product Level Requirements and Product Capabilities
- Evidence: Typically derived
  - deductively from Safety Architecture and from formal Verification
  - empirically from Testing, Simulation,..

Reference Homologation Process

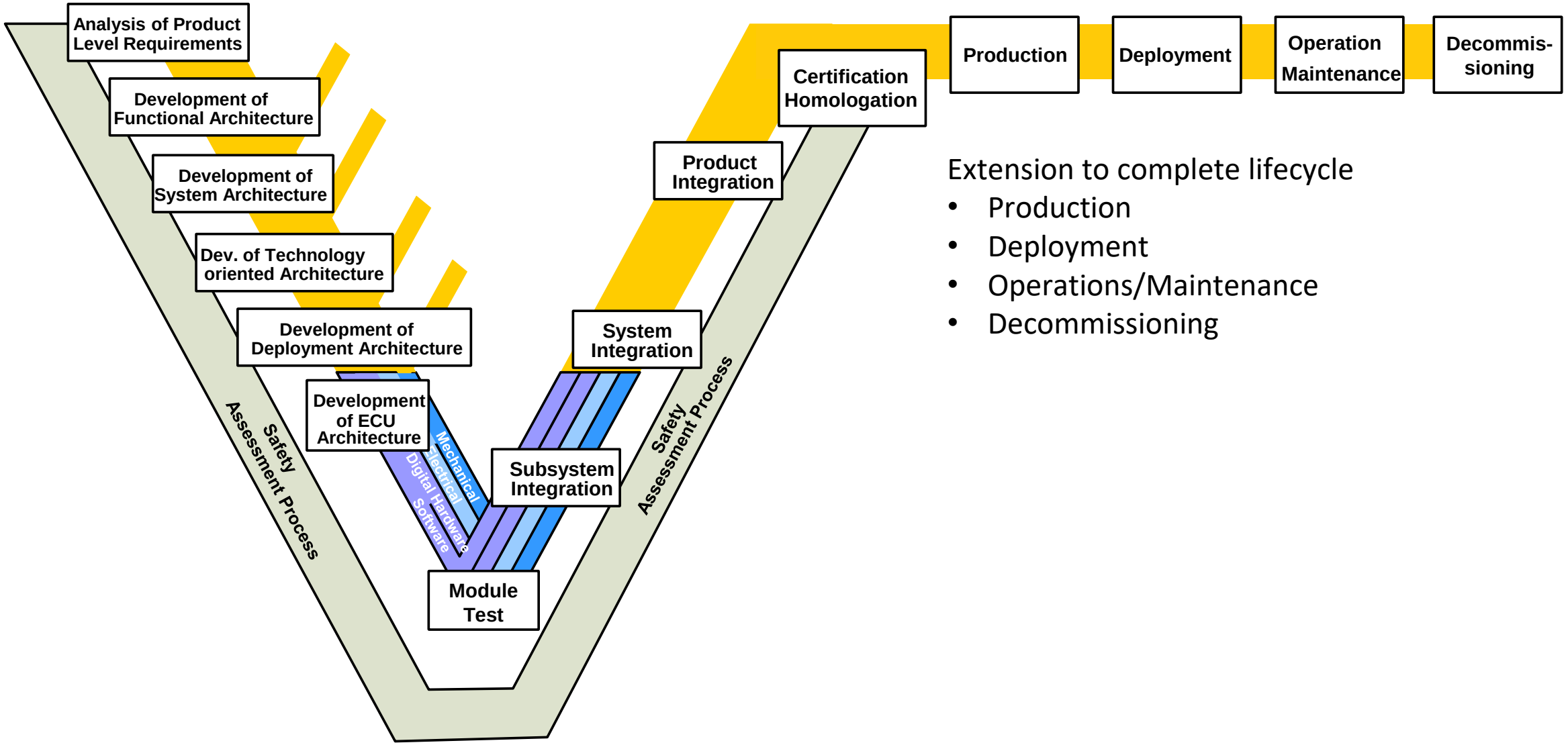


Reference Homologation Process



Reference Homologation Process

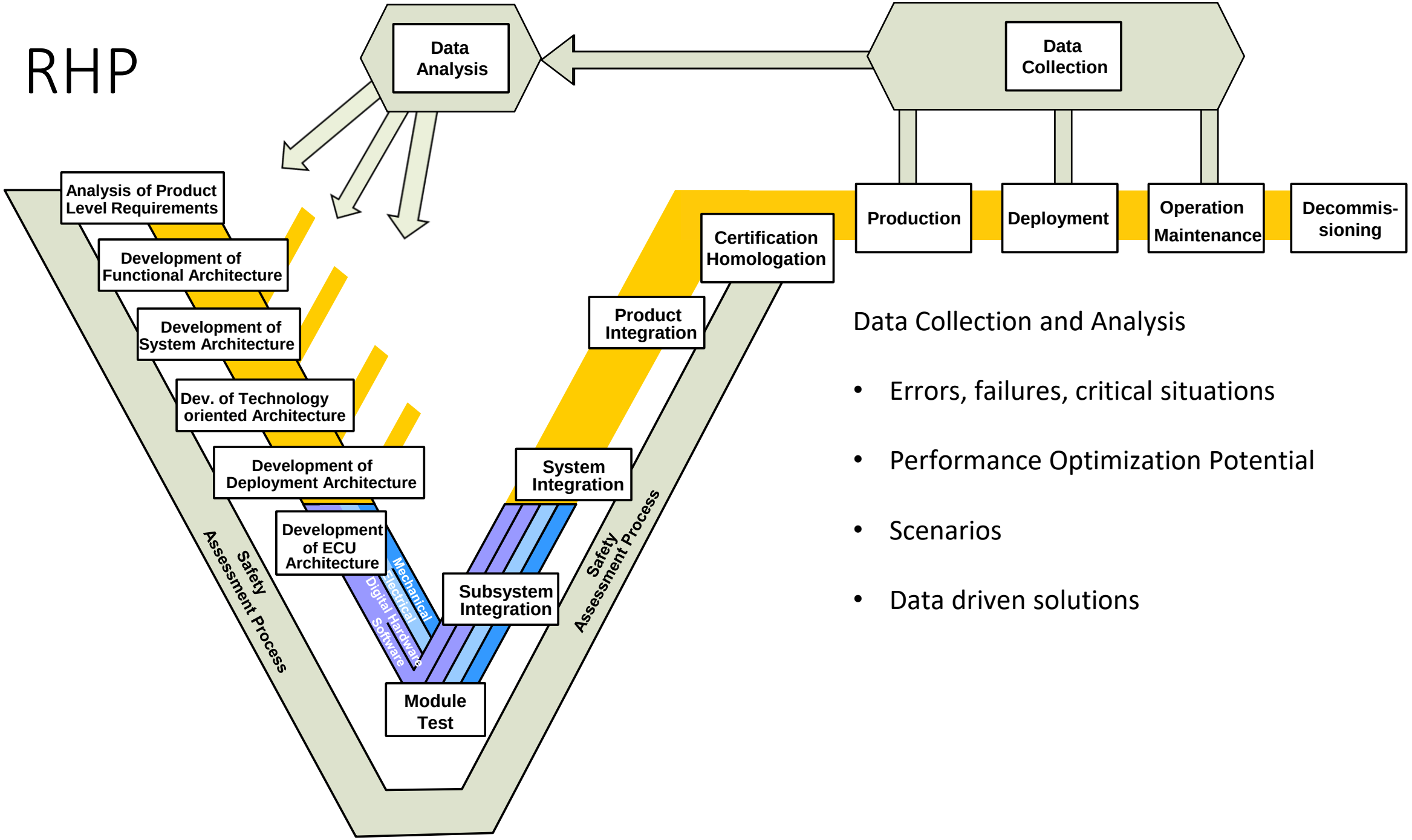
a.k.a. Reference Lifecycle Process



Extension to complete lifecycle

- Production
- Deployment
- Operations/Maintenance
- Decommissioning

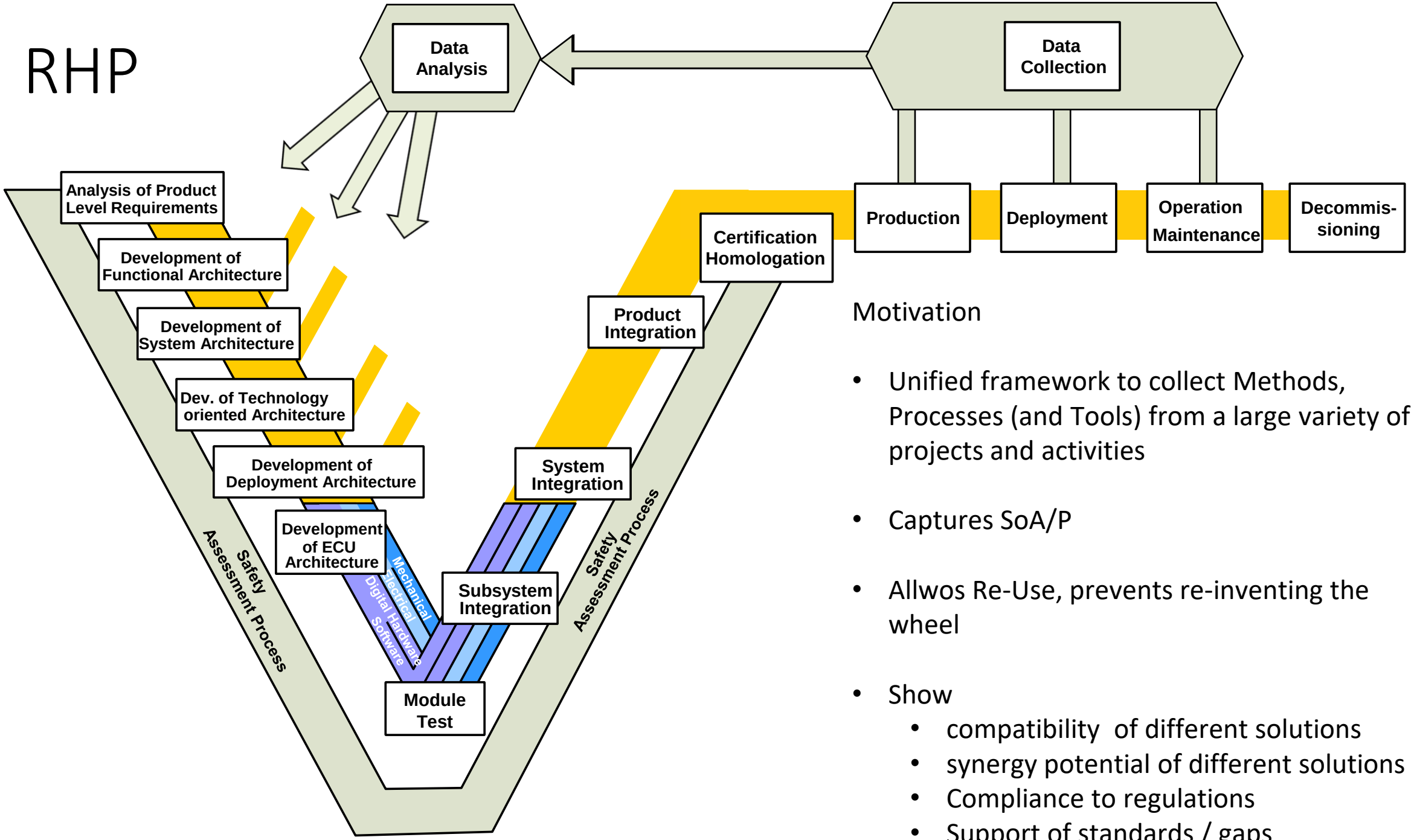
RHP



Data Collection and Analysis

- Errors, failures, critical situations
- Performance Optimization Potential
- Scenarios
- Data driven solutions

RHP

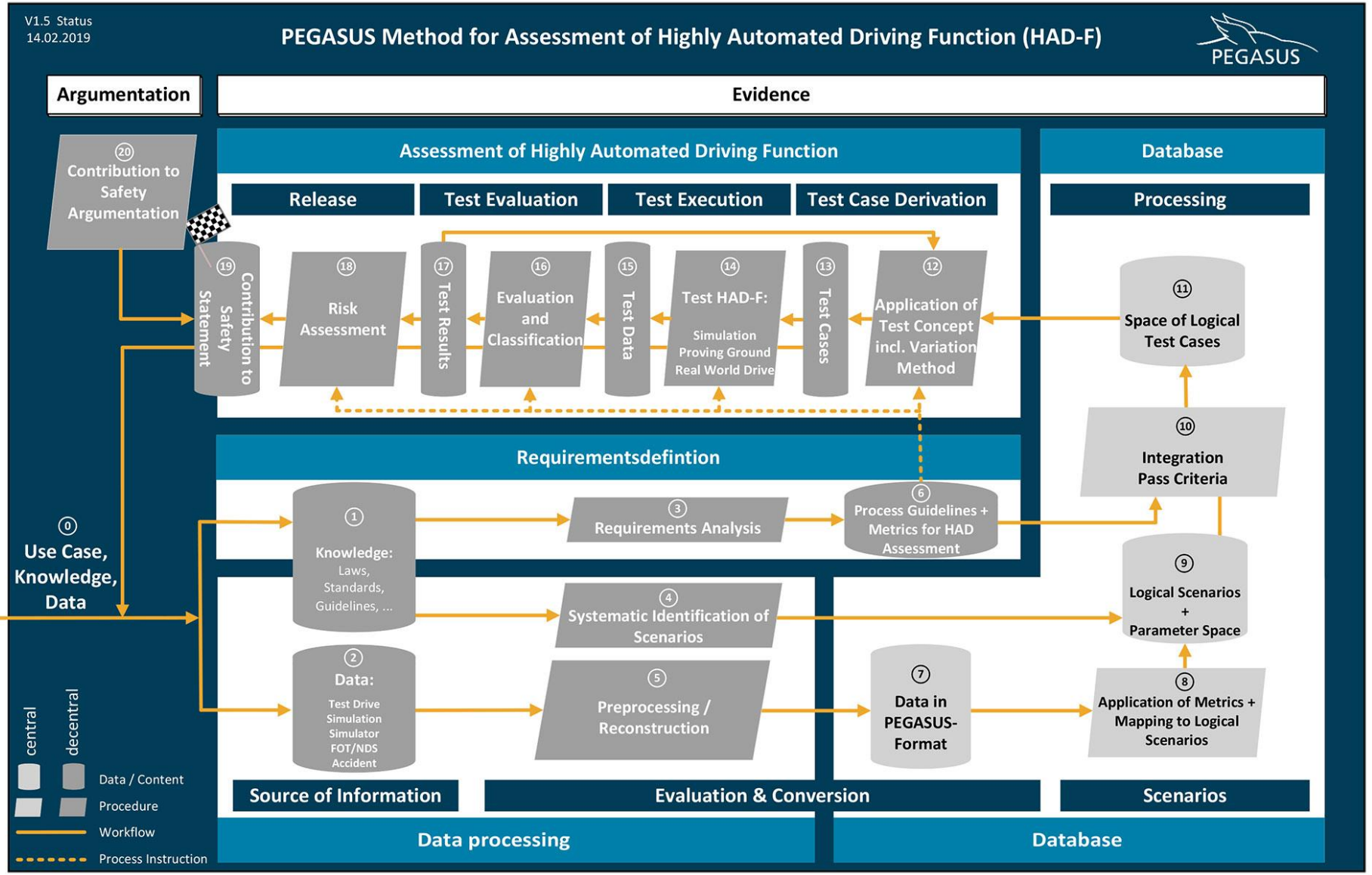


Motivation

- Unified framework to collect Methods, Processes (and Tools) from a large variety of projects and activities
- Captures SoA/P
- Allwos Re-Use, prevents re-inventing the wheel
- Show
  - compatibility of different solutions
  - synergy potential of different solutions
  - Compliance to regulations
  - Support of standards / gaps

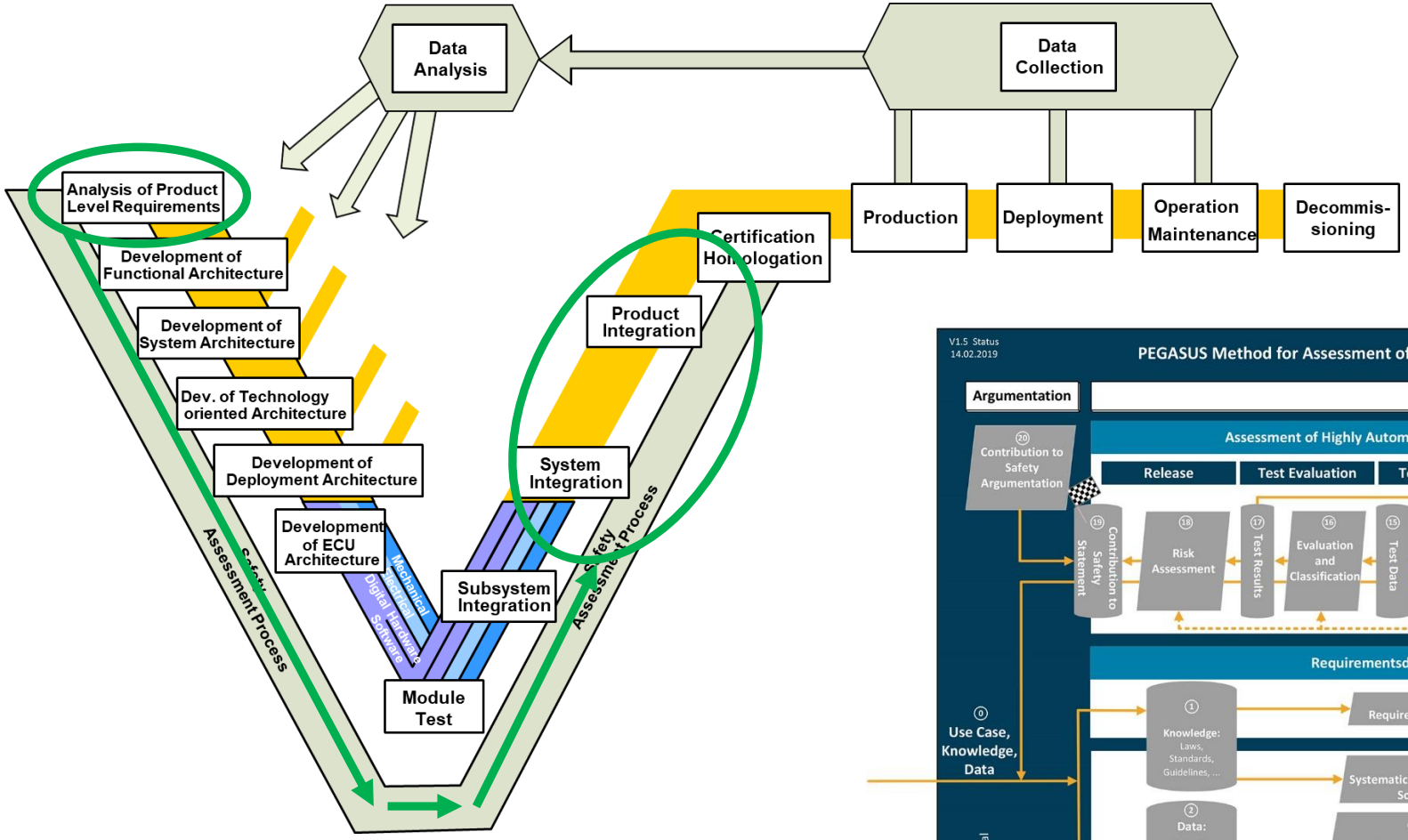
Mapping Technology Bricks

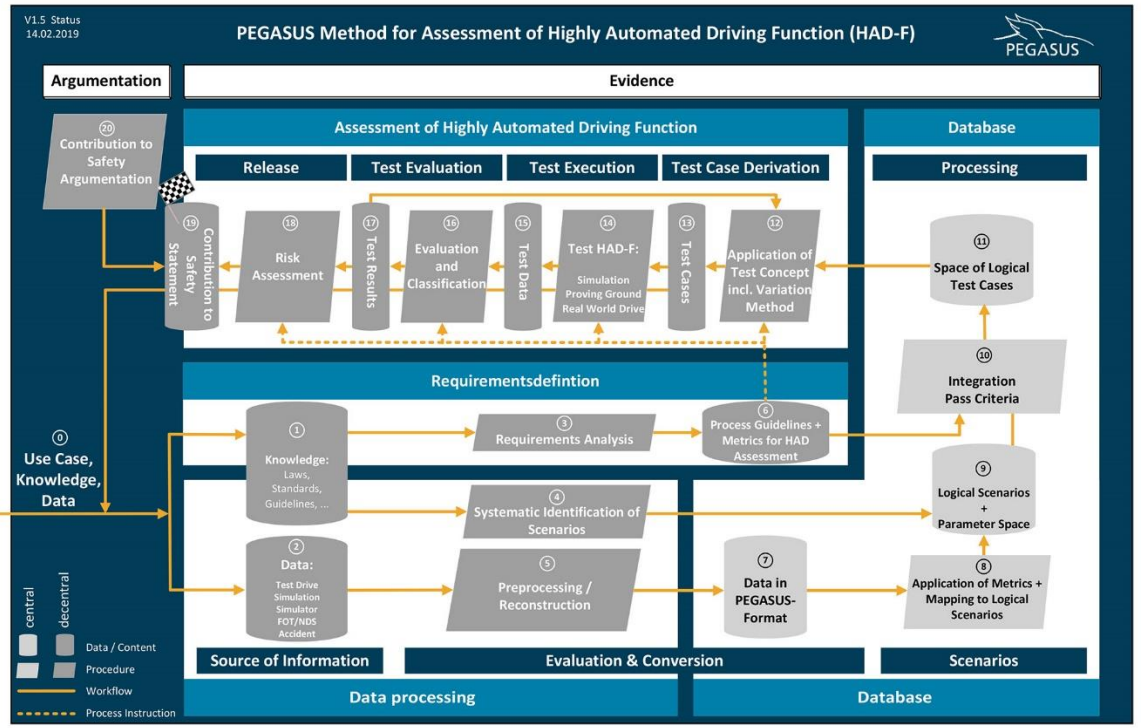
Pegasus – Scenario based Assessent of HAD-F



Mapping Technology Bricks

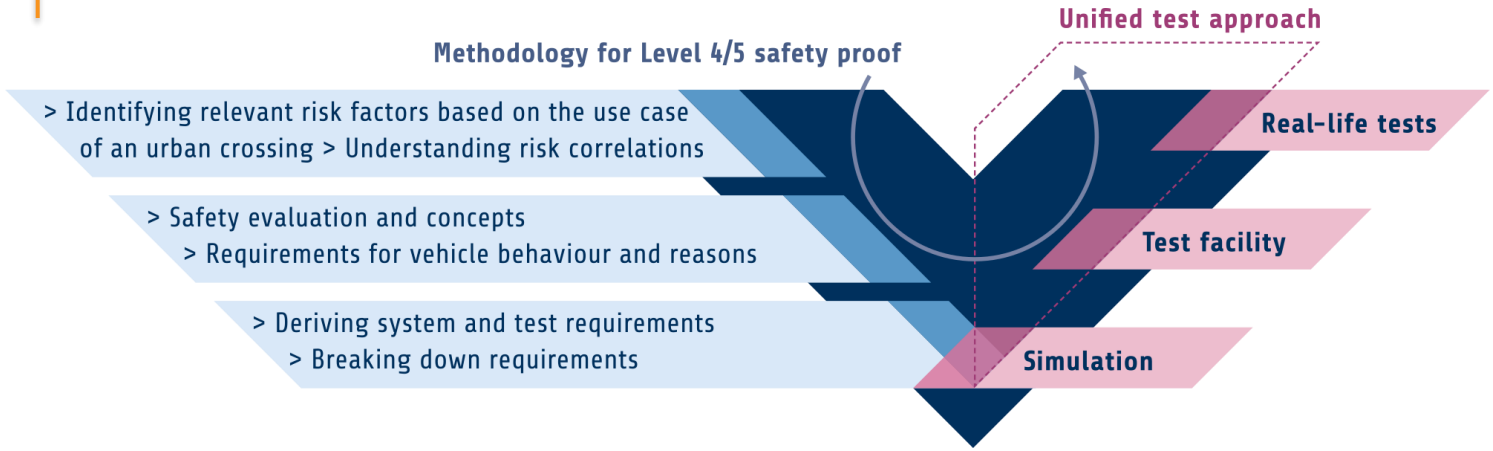
Pegasus – Scenario based Assessent of HAD-F

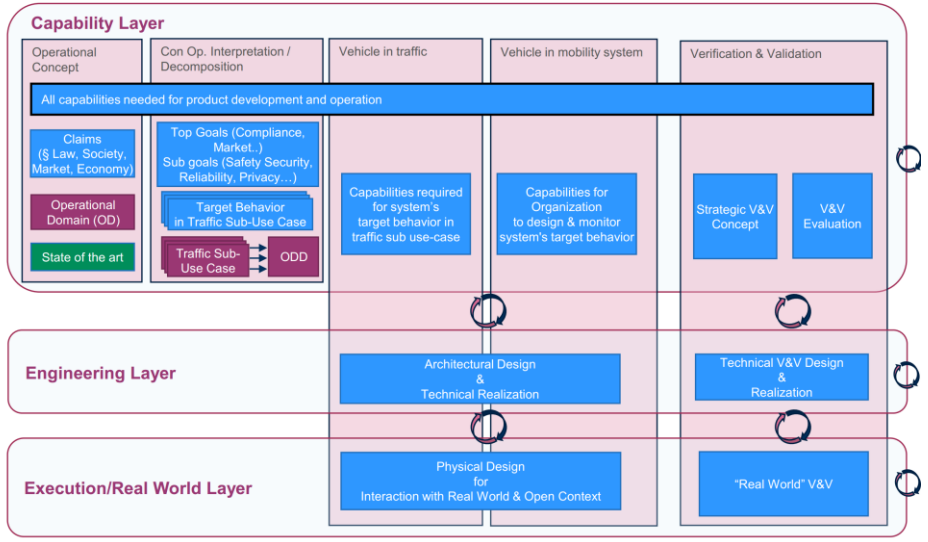




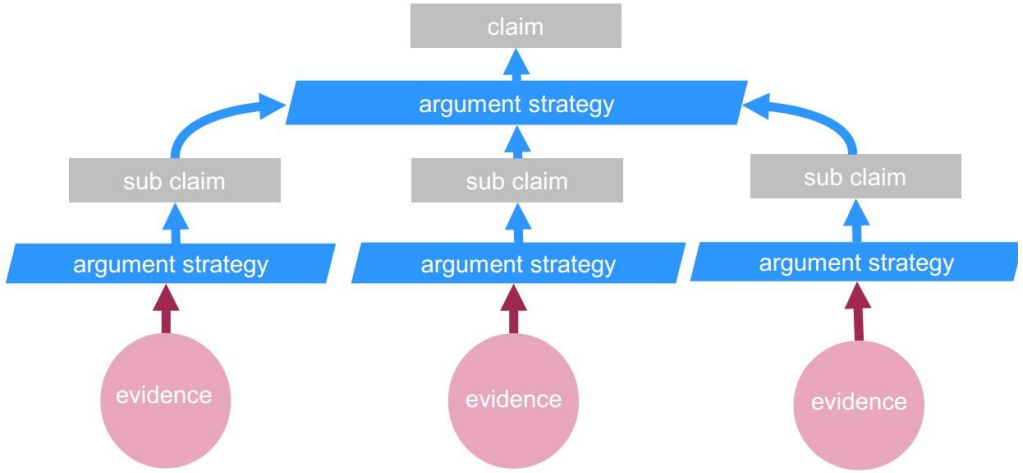
Mapping Technology Bricks

VVM – Methodology for Level 4/5 Safety Proof



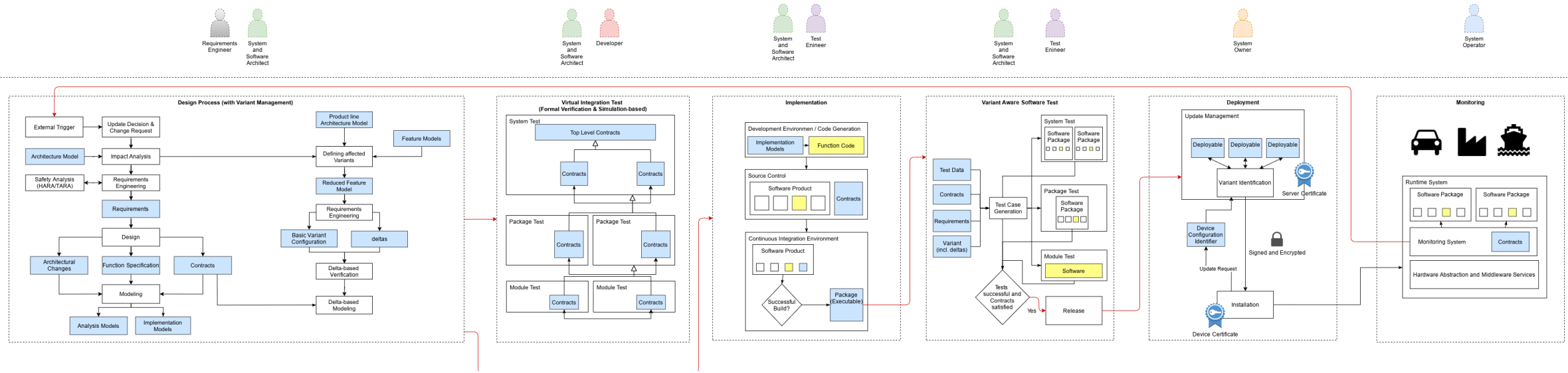


- Identify risk factors
- Test requirements based on
  - Use-Case / ODD
  - System/product requirements
  - Vehicle behavior and reasons
- Validation methodology across all system levels
- Unified test approach (deriving evidences) from simulation to real wolrd driving



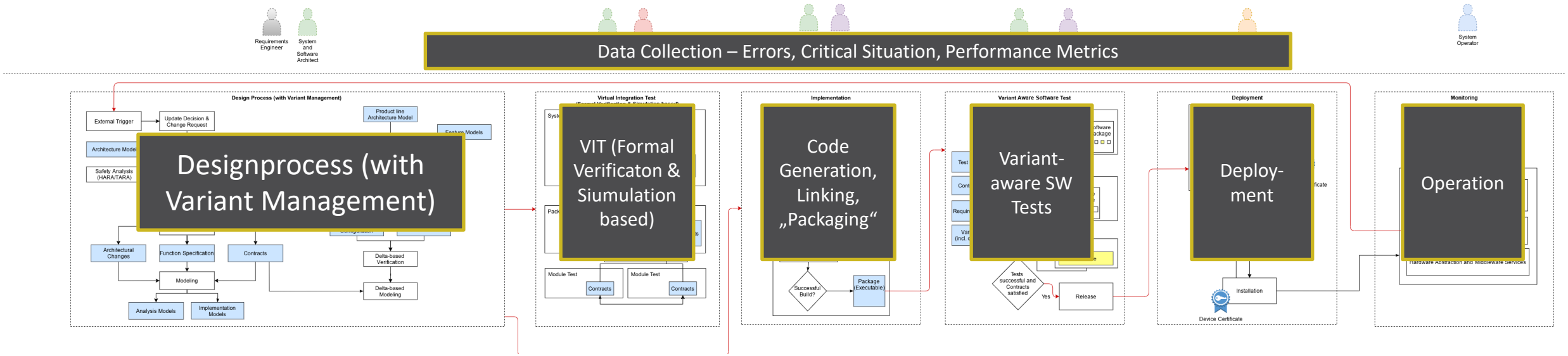
Mapping Technology Bricks

StepUp!CPS – OTA Updates (and Variants)



Mapping Technology Bricks

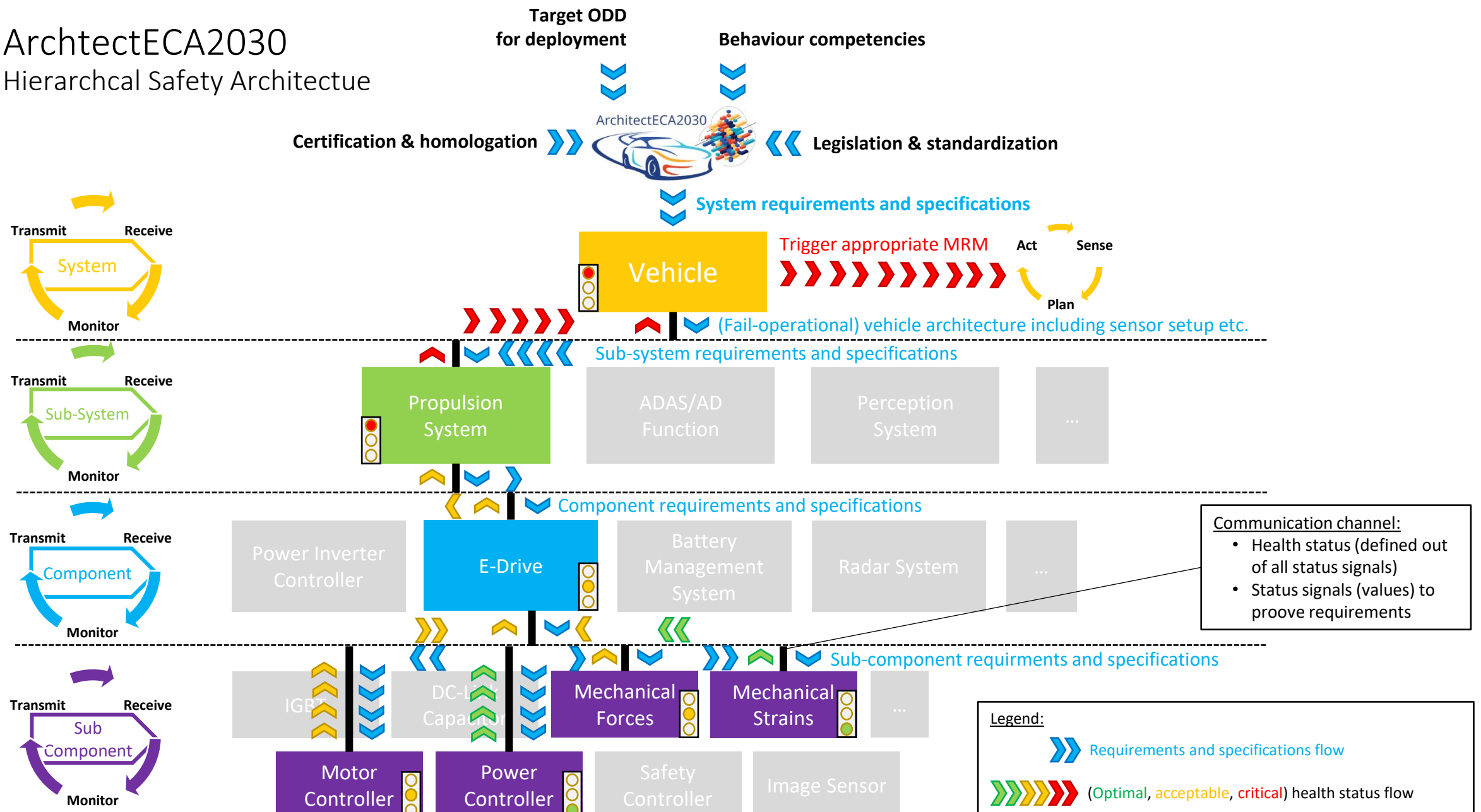
StepUp!CPS – OTA Updates (and Variants)



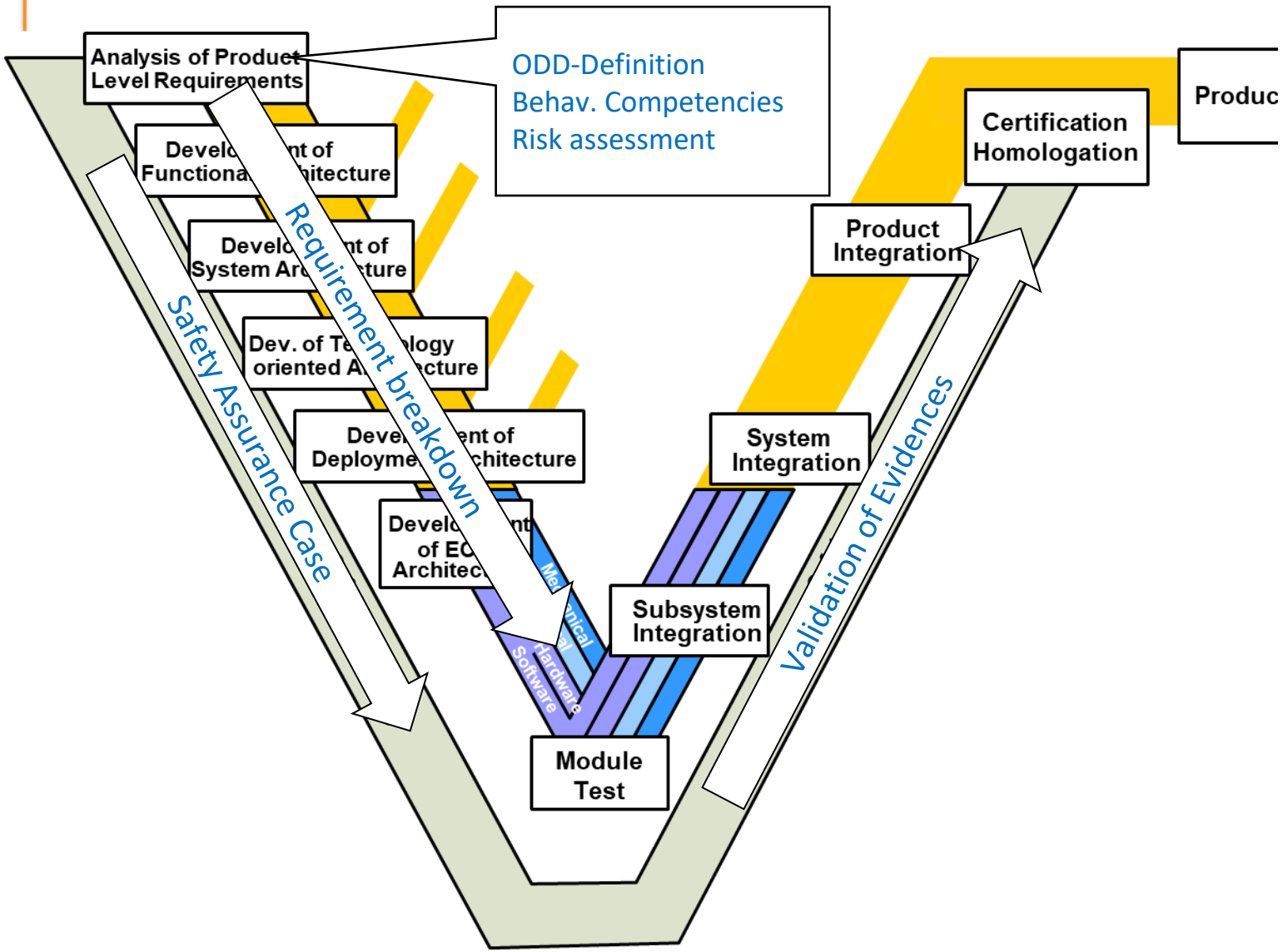
- Over-the-Air (Software) Updates require
  - Data collection (Errors and critical situaitons; performance data)
  - Virtual Integration Testing / Validation (based on contracts)
  - Safe (and secure) Deployment
  - …
- Variants require
  - Variant aware (‚delta-based‘) Validation and Test

ArchtectECA2030

Hierarchcal Safety Architectue

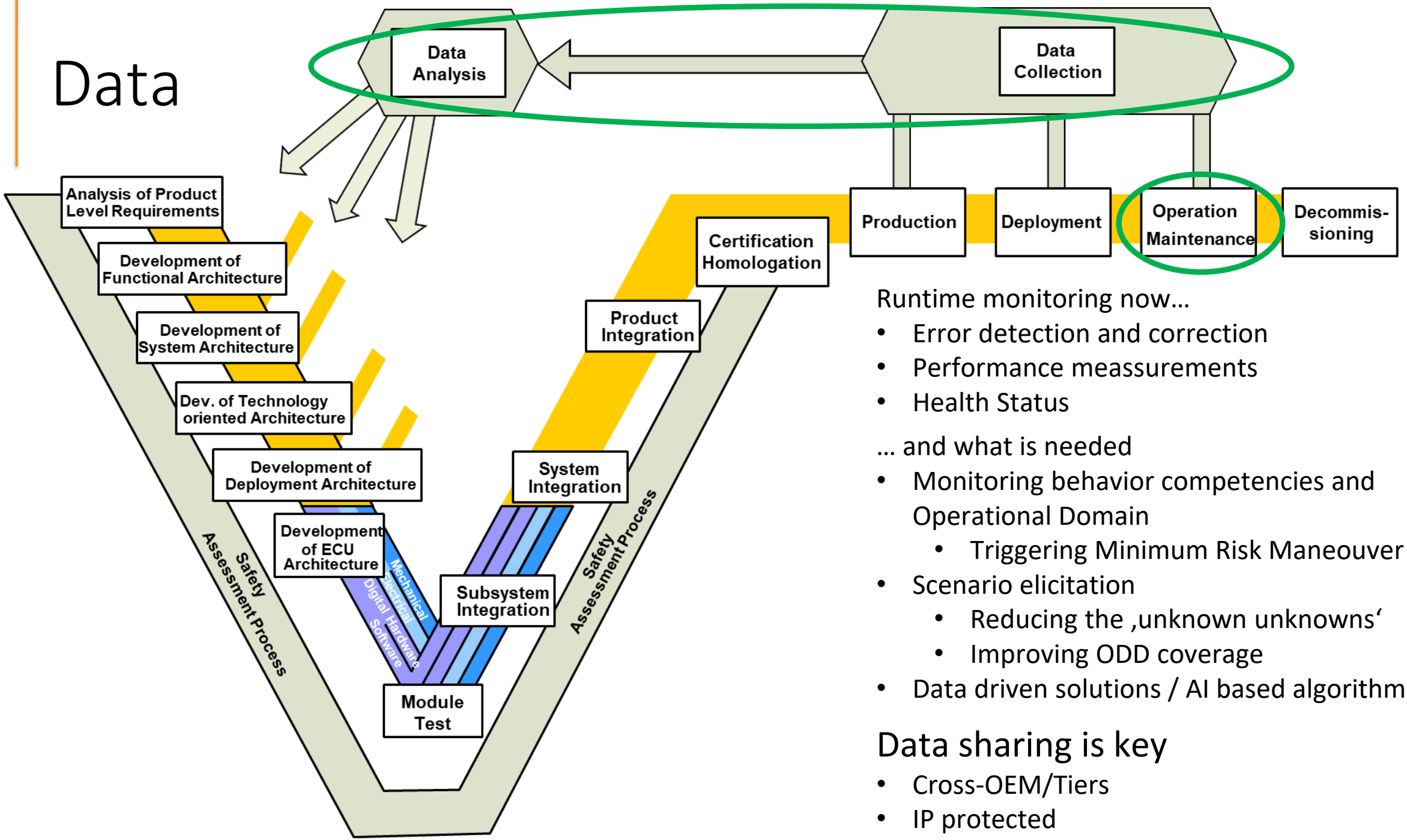


Deriving challenges



- New Challenges…
  - Incomplete requirements (open world), unknown scenarios, incomplete perception,…
- … are ‚handled' by
  - Scenario based tasting targeting behviour competences needed for ODD focusing on risk assessment
  - Combined with ‚in-field monitoring'
- Remaining Problems
  - (Relevant) Scenario Generation
  - How safe is safe enough?
    - ODD coverage
    - Behavior Competences Coverage
    - ‚Awareness of Unknown unknowns'/ disfunctional cases
  - Realism/ Accuracy of Models and Simulation
  - Uncertainties in perception

Data



Runtime monitoring now…

- Error detection and correction
- Performance meassurements
- Health Status

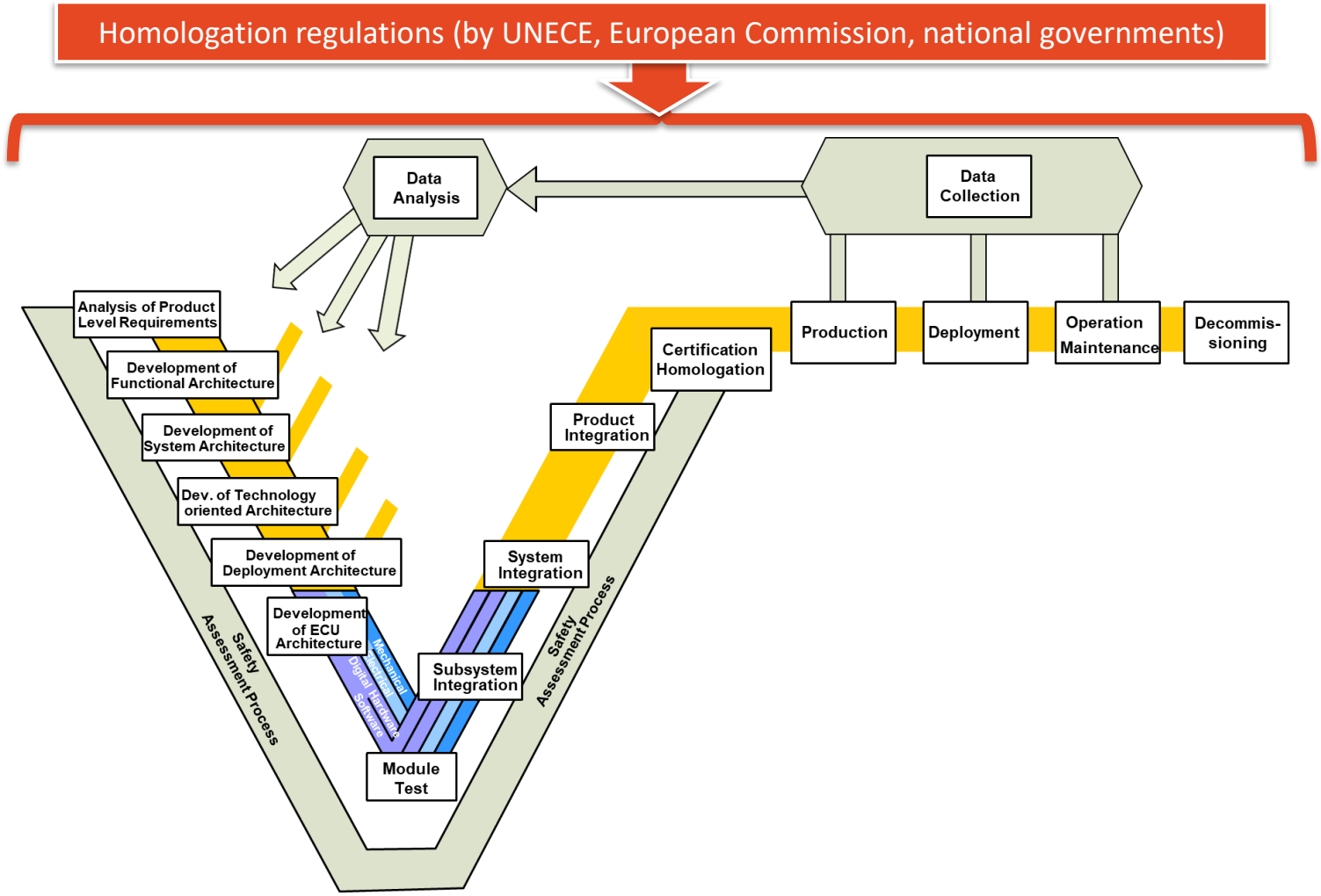
… and what is needed

- Monitoring behavior competencies and Operational Domain
  - Triggering Minimum Risk Maneouver
- Scenario elicitation
  - Reducing the ‚unknown unknowns‘
  - Improving ODD coverage
- Data driven solutions / AI based algorithms

Data sharing is key

- Cross-OEM/Tiers
- IP protected

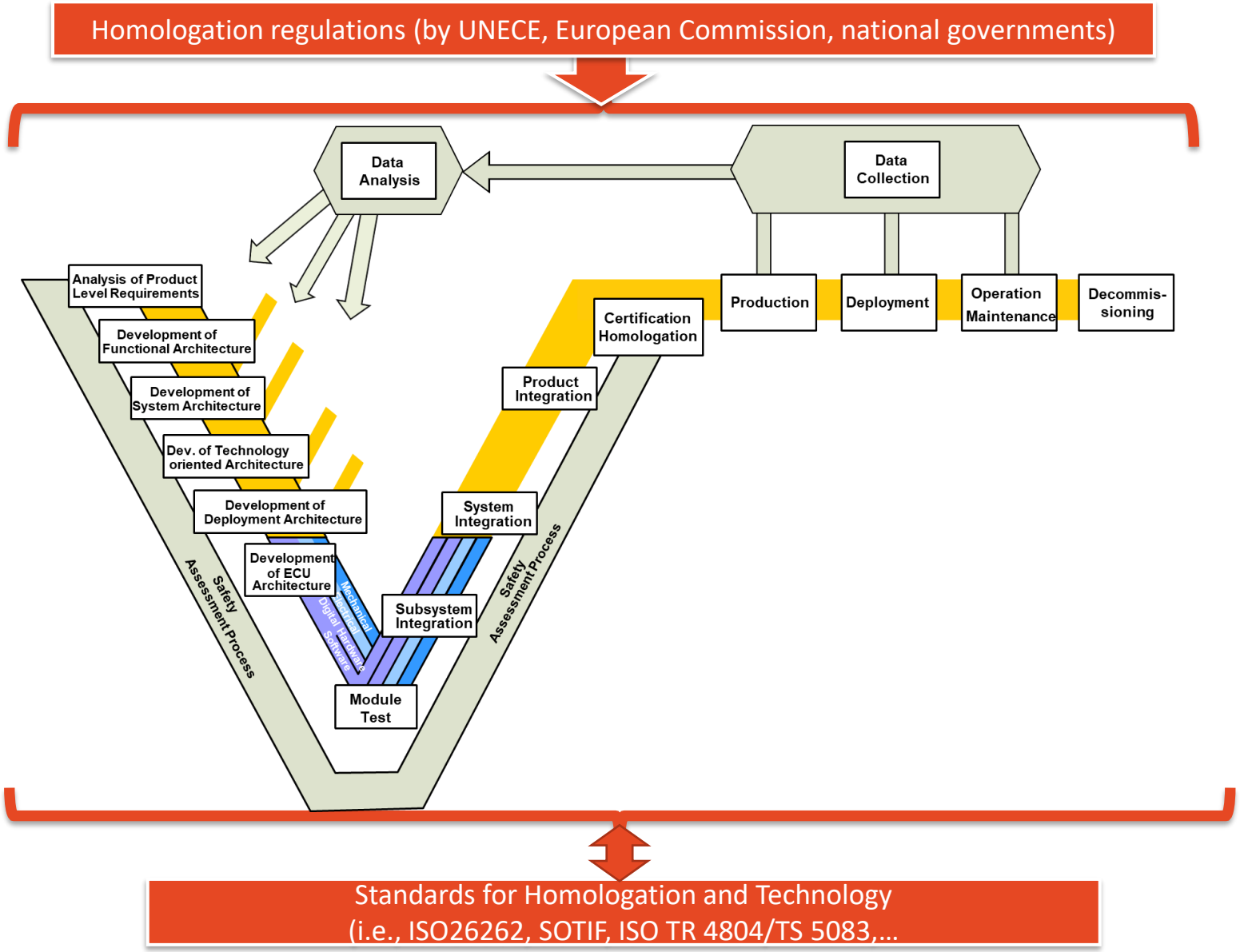
Compliance to Regulations



- New Regulations, e.g.
  - EU General Safety Regulation (EU) 2019/2144
  - New Assessment/Test Method for Automated Driving (NATM)
  - UN R157 (Automated Vehicles, ALKS), 2020 and 2022
  - EU ADS Regulations (fully driverless vehicles)
  - More to come…
- Checks
  - Compliance of technology bricks
  - Can the evidence required by regulations be provided?

- RHP has potential for uniform way of providing process information ot Audit of the 5-pillar approach

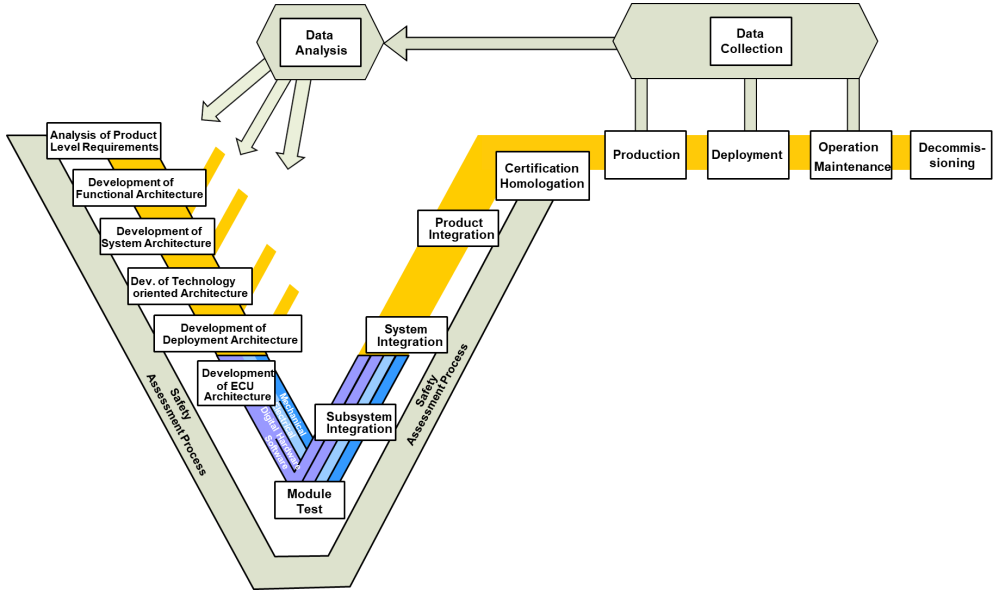
Support by Standards



- Homologation relevant Standards
  - ISO 26262 (Functional Safety) and ISO 21448 (SOTIF)
  - ISO TR 4804 resp. ISO AWI TS 5083 (Safety for automated driving systems — Design, verification and validation)
  - ISO 24089 (Automotive Software Updates)
  - ISO 21434 (Automotive Cybersecurity)
  - ISO 34503 (ODD)
  - ASAM OpenScenario, OpenODD,…
  - (UL 4600)
  - (RSS – responsibility sensitive safety)
- Missing
  - Behavior competences (analog ISO 34503)
  - (Critical) Scenario elicitation
  - …
- Fill gaps in existing standards, push new ones.

Take-away message

- Reference Homologation Process provides a uniform way to describe technology bricks – methods, processes, tools – needed for safety assurance/homologation of SAE L3+ ECAs.
  - Captures SoA
  - Allows re-use, prevents ‚re-invinting the wheel‘
  - Check lifecycle coverage: Identify missing pieces and links
  - Check compliance to regulations
  - Check support by standards
- Open Challenges
  - Scenario Generation, Scenario Database
  - Inclusion of Multi-Pillar Approach
  - ODD coverage, behavioral competencies coverage
  - Realism/accuracy of models and simulation
  - Uncertainty in perception
  - …



Thank You !

Contact
Jürgen Niehaus
SafeTRANS Competence Cluster
juergen.niehaus@safetrans-de.org
https://www.safetrans-de.org