A methodology for *transforming* a *local* safety-critical cyber-physical system into a *distributed* safety-critical solution

Krzysztof Oborzyński (Philips) & Astrid Rakow (German Aerospace Center)

TRANSACT Impact Webinar, EUCloudEdgeIoT.eu

June 4, 2024

TRANSACT Reference Architecture

TRANSACT
transact-ecsel.eu/

ESI
Powered by industry, academia and TNO

ITI INVESTIGATE TO INNOVATE

Solutions:

- Safet
- Performa
- Secur
- Priva

Use-cases:

TRANSACT reference architecture:
a universally applicable distributed solution architecture concept

Presenters: Javier Coronel (ITI)
Teun Hendriks (TNO)
jcoronel@iti.es, teun.hendriks@tno.nl

TRANSACT Impact Webinar
*EU**Cloud**Edge**IoT**.eu*
June 4th, 2024

KDT JU
KEY DIGITAL TECHNOLOGIES JOINT UNDERTAKING

EUCloudEdgeIoT.eu

Transition methodology overview

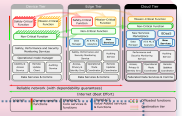
Transformation focus areas

Why?
to engage into the transition?

Business
- Business drivers
- Solution requirements

What?
system functionality needs transition to the distributed CPS solution?

Architecture



Product
- Architecture
- Development
- Operation
- DevOps

Infrastructure

Who?
can build and operate the distributed CPS solution

Organization
- People/skills
- Processes+ technology
- Structure

Cross-cutting aspects

- Safety
- Performance
- Security & privacy
- Regulatory & certification

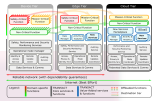
Transition methodology overview

Transformation focus areas

Why?
to engage into the transition?

Business

What?
system functionality needs transition to the distributed CPS solution?



Architecture

Who?
can build and operate the distributed CPS solution

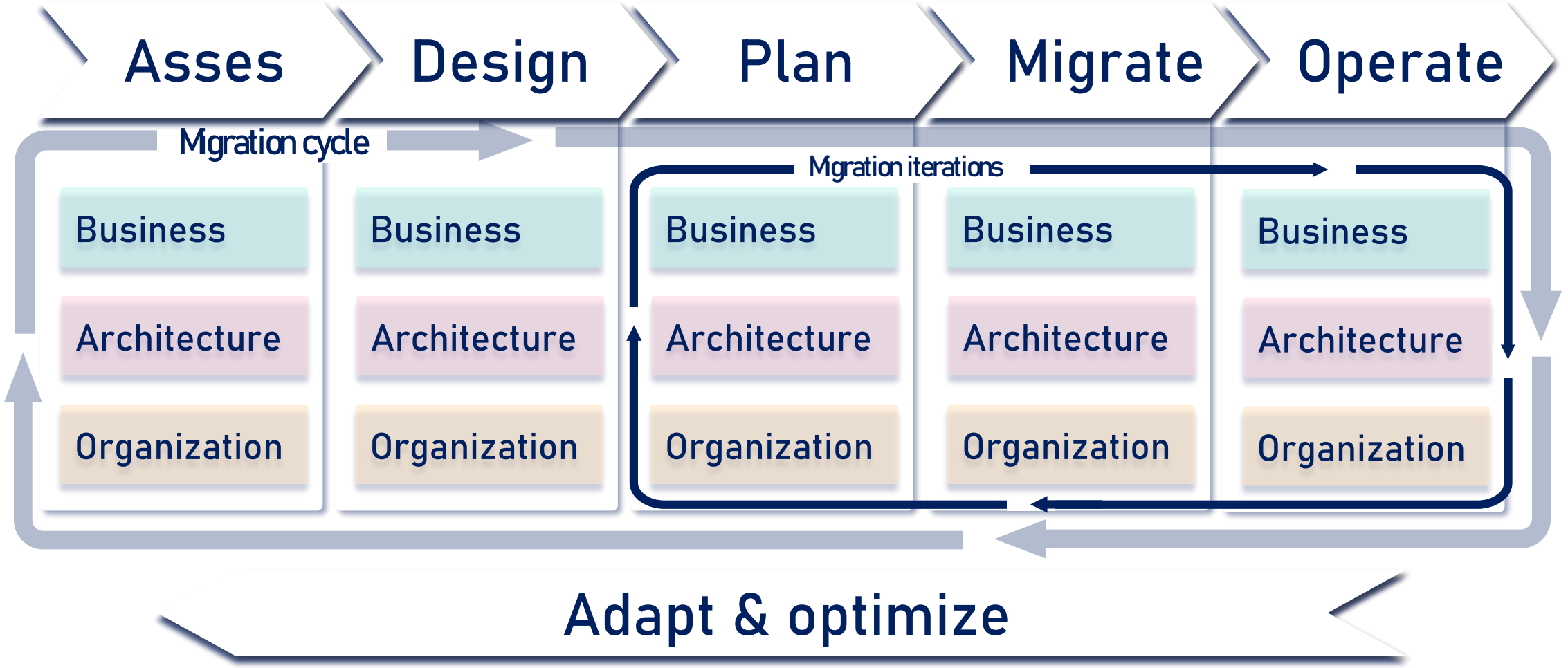
Organization

Cross-cutting aspects

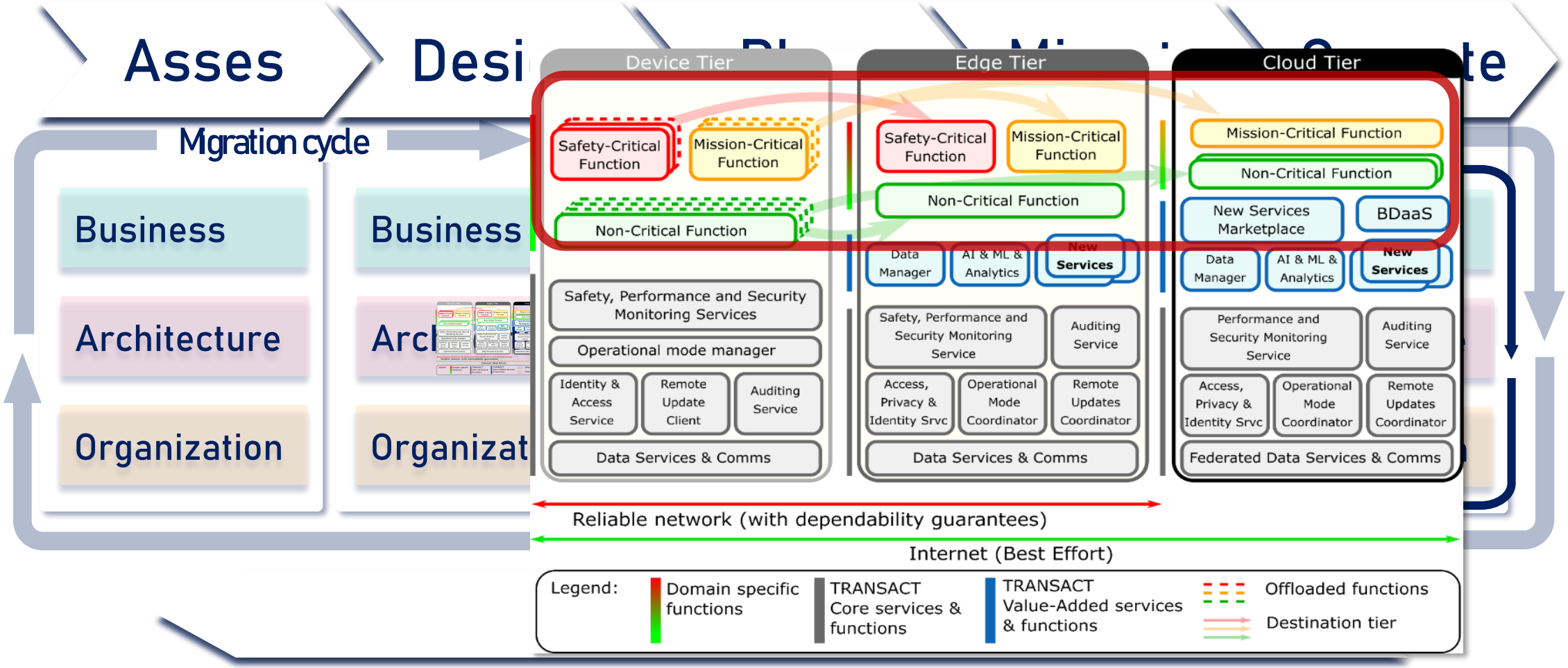
- Safety
- Performance
- Security & privacy
- Regulatory & certification

HOW?
to answer transition questions for Business/Architecture/Organization?

Transition methodology execution

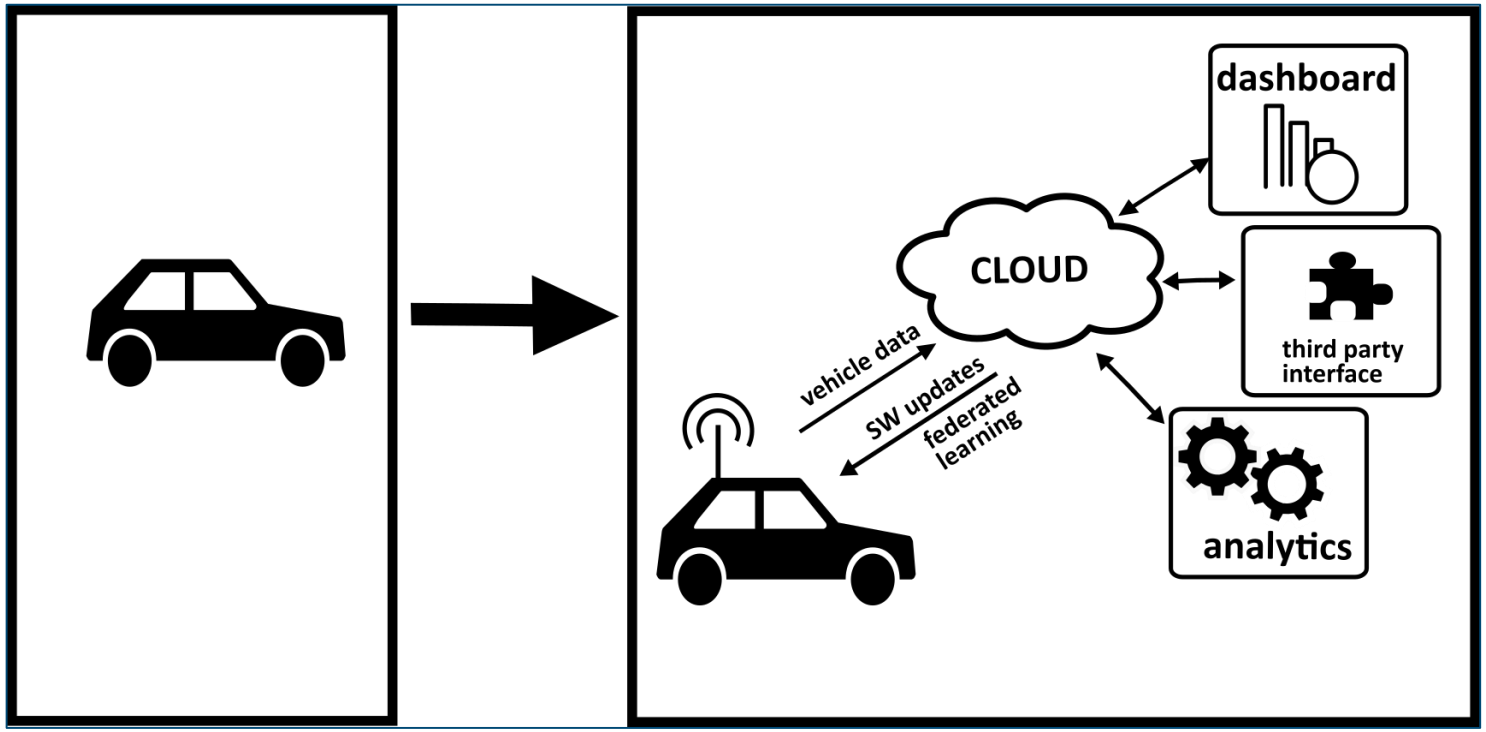


Transition methodology execution

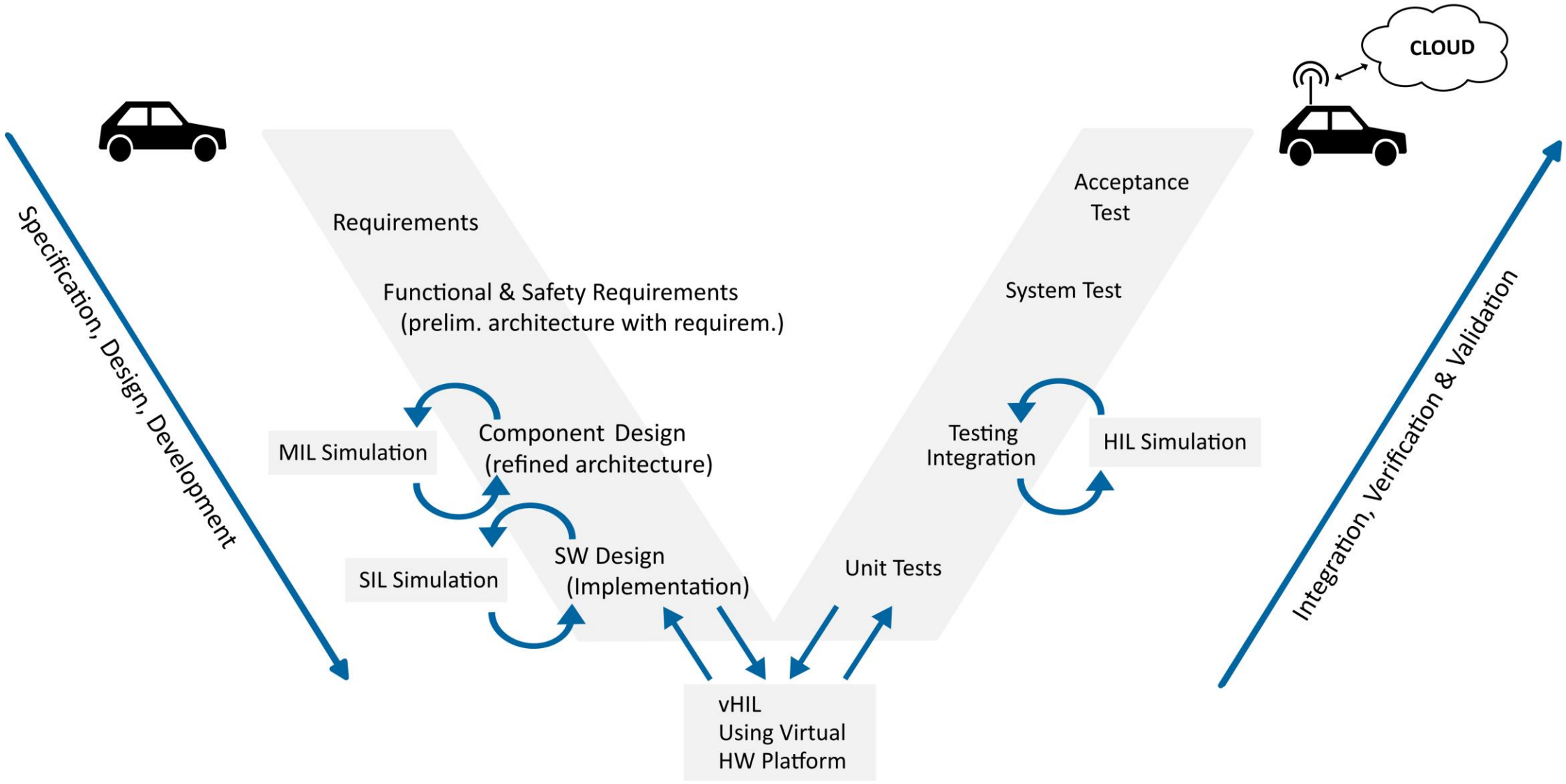


Approach for Validation & Verification

How to derive a distributed & trustworthy solution and exploit that a trustworthy initial system has been developed?



Development Approach for the Transition



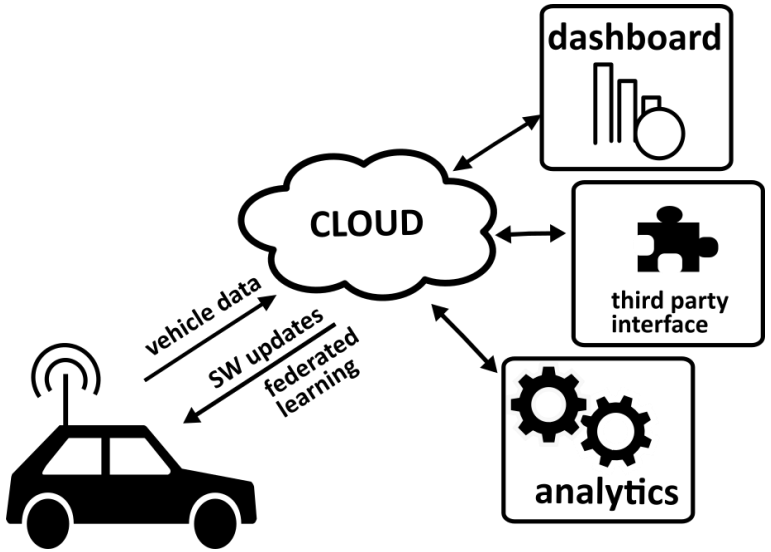
Exploiting the New & the Old

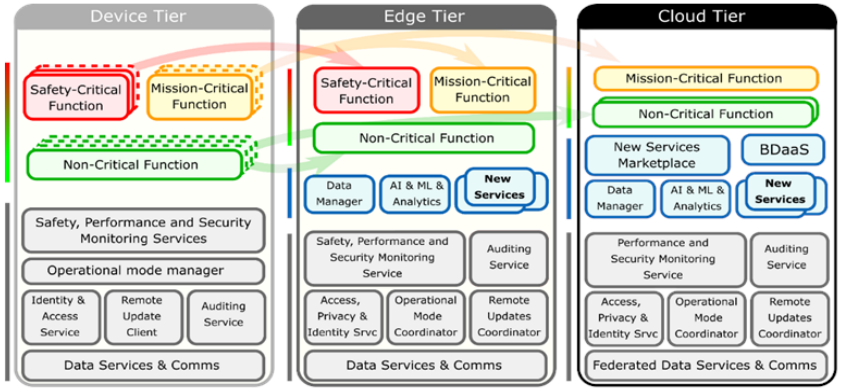
\+

requirements

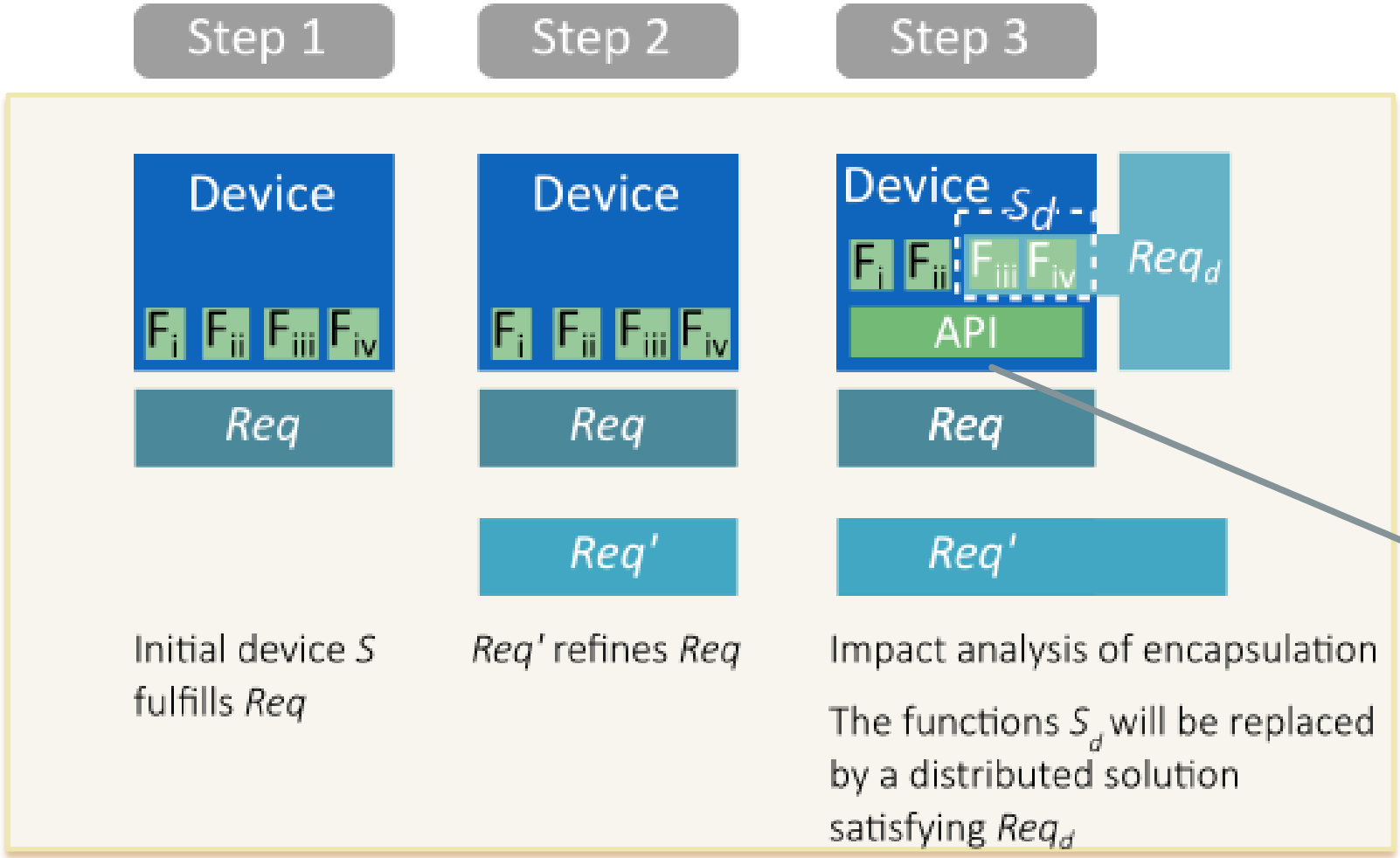
- Structured Design Space Exploration & Documentation
- Design Space: Architecture & Solutions (Off-The-Shelf)
- Verification & Validation
  - Front-Loading: Model-Based Design
  - Reuse of Previously Established Results

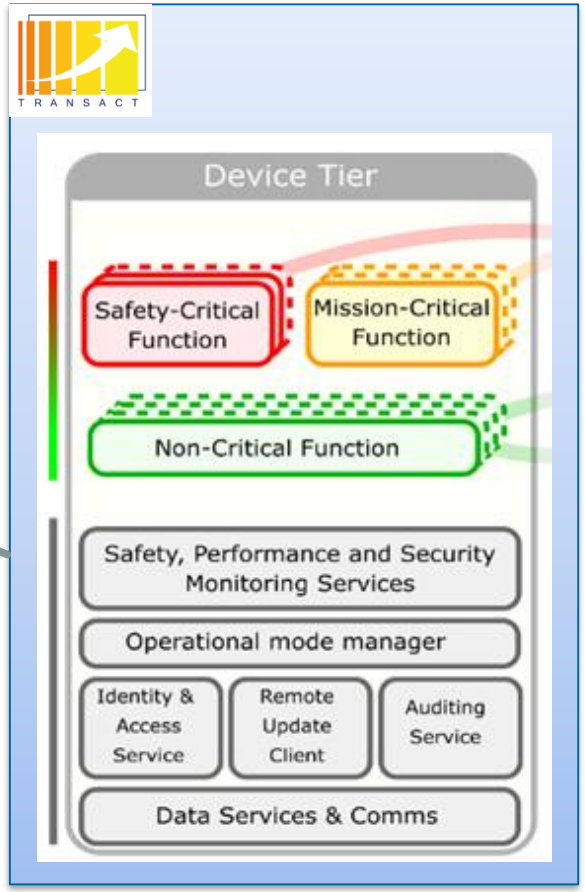
T&V Methodology



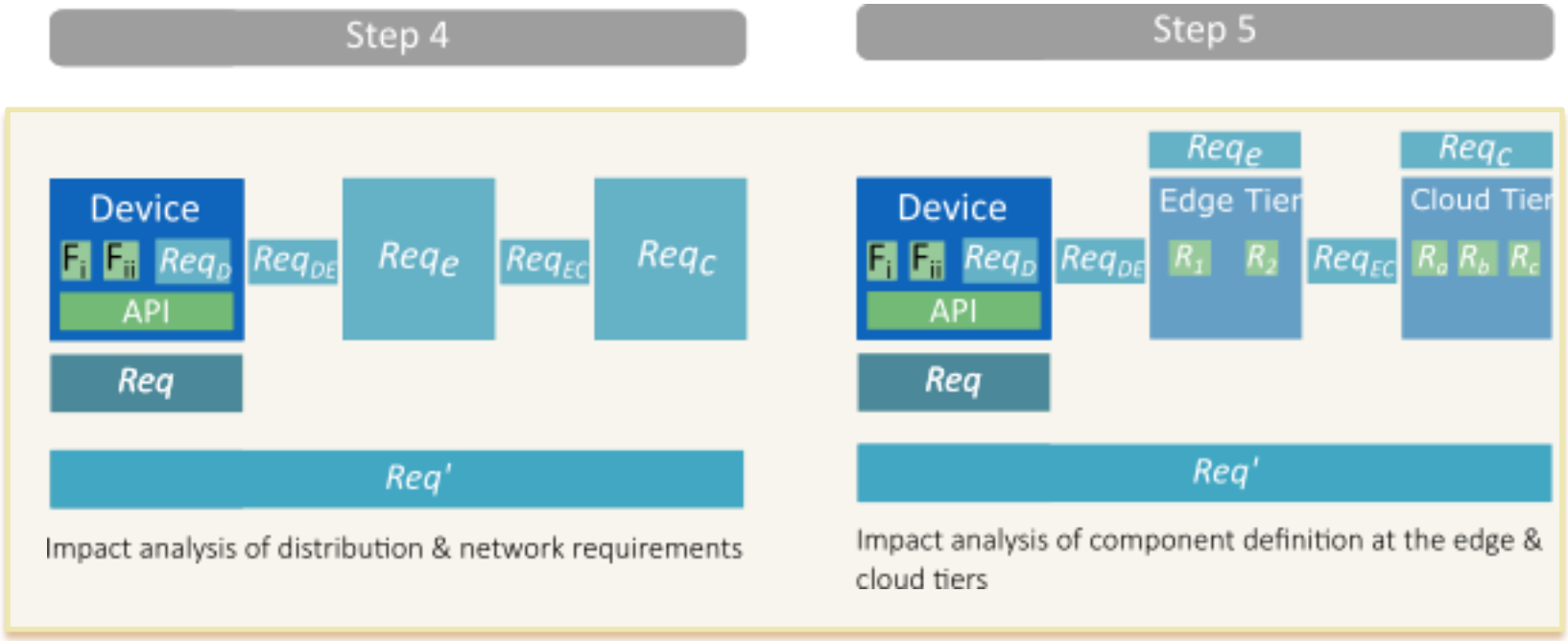


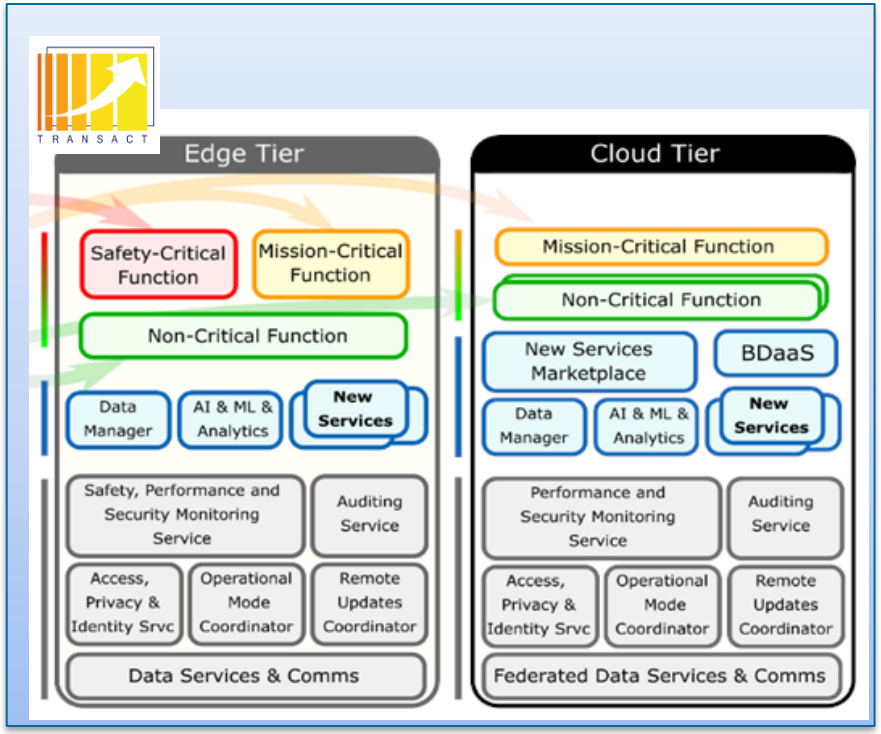
Stepwise Development of Requirements



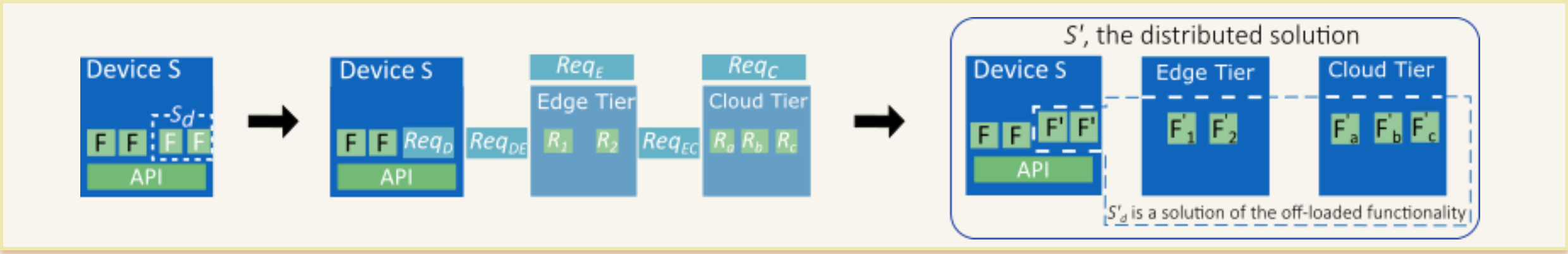


Stepwise Development of Requirements





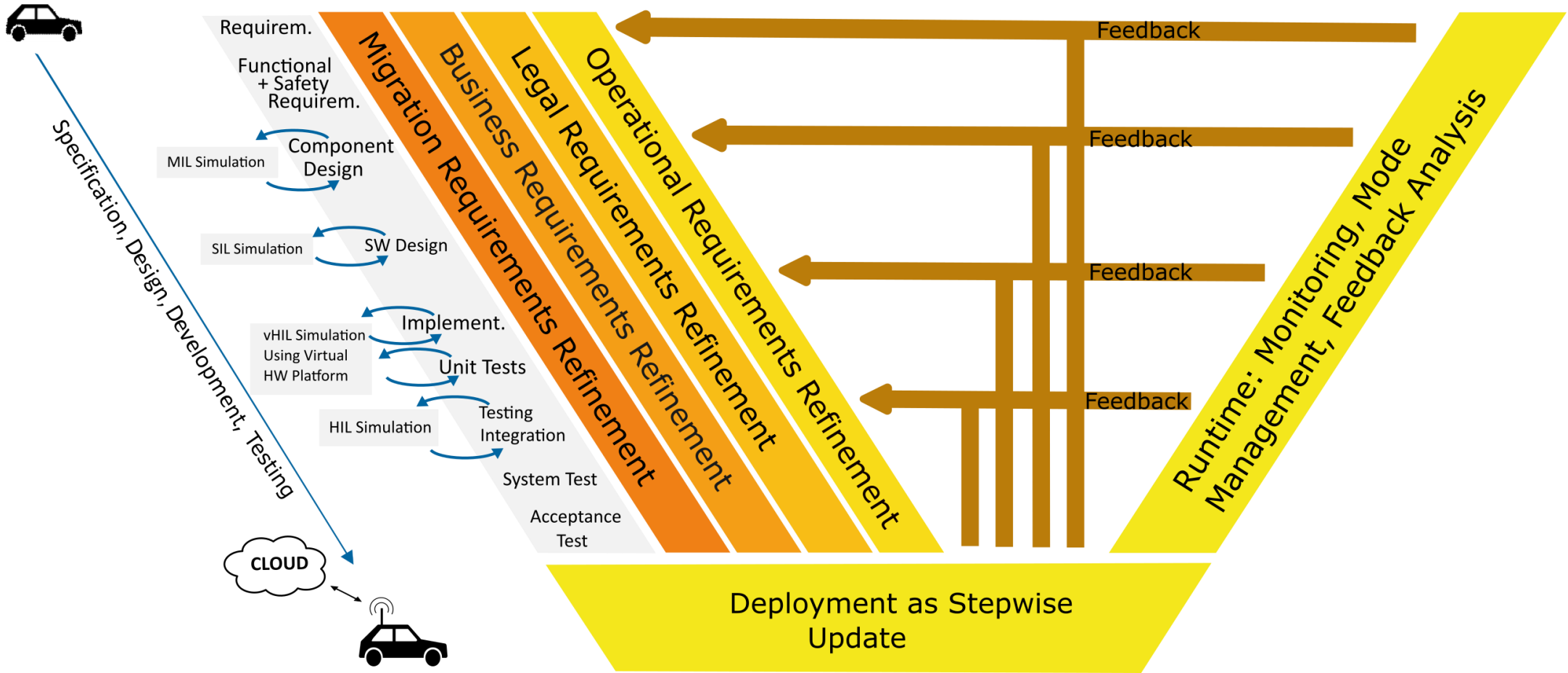
In a Nutshell:



- Structures
  - design space exploration &
  - documentation / recertification
- Early identification
  - of what to offload and
  - whether offloading is feasible

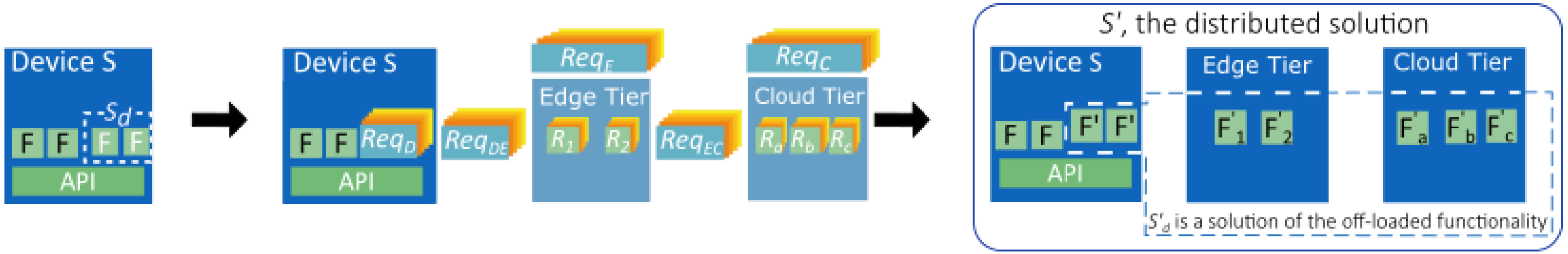
- Supporting the design of
  - interfaces and
  - mitigation strategies
- Verification & Validation
  - front-loading: models & contracts
  - reuse of "old" results

Development of the technical solution as part of the transition



⇨ Requirements on the migration activities

Development of the technical solution as part of the transition



- Strategy for design space exploration:
  - Check realizability of most critical decision first.
- Criticality
  - Criticality depends on multiple dimensions.
  - The dominant dimension(s) may vary for different design steps/solutions/companies.
- Verification
  - Evidences do not only refer to technical properties but also to the other dimensions.

Conclusions

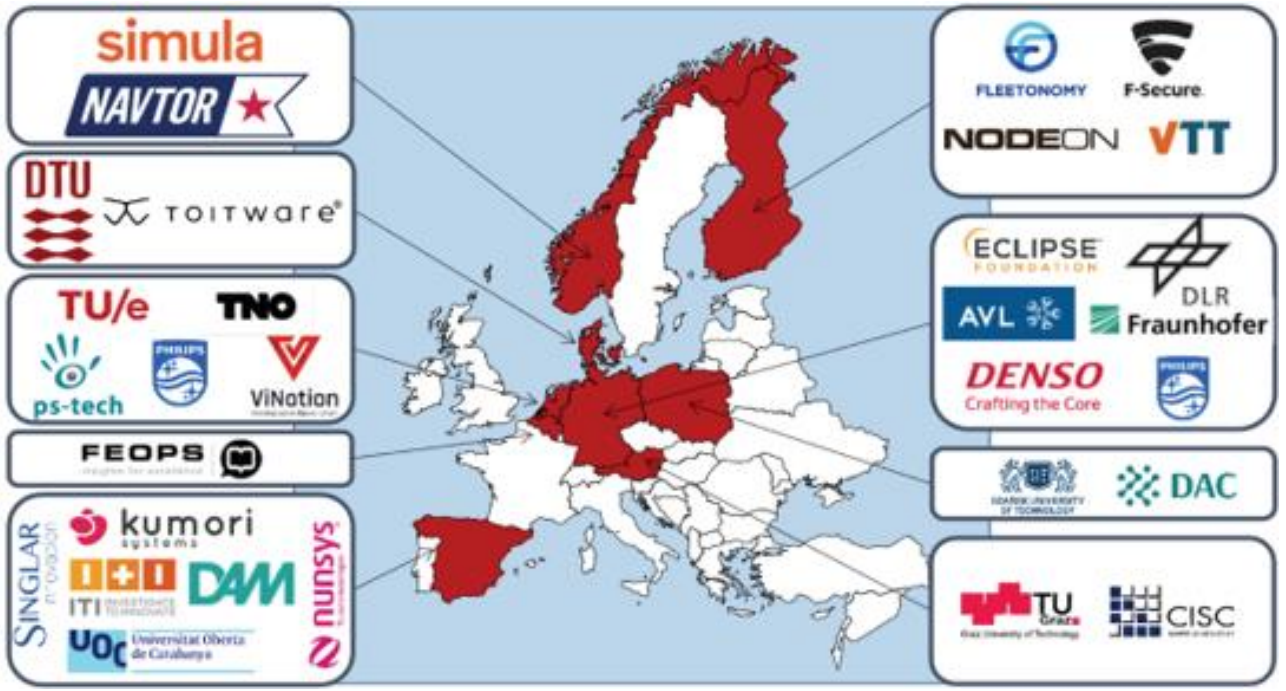
- Proposed transition methodologies are complementing the TRANSACT Reference Architecture
- Transformation from on-device safety critical CPS towards a distributed solution involves not only *architecture* but also *business* and *organization* aspects
- T&V methodology
  - helps ensuring trustworthiness of the new distributed solution
  - emphasizes the multidimensional strategic aspects of the transition

TRANSACT PROJECT

towards safe and secure distributed cyber-physical systems

https://transact-ecsel.eu/

Krzysztof Oborzyński
krzysztof.oborzyski@philips.com
(Philips)
&
Astrid Rakow
astrid.rakow@dlr.de
(German Aerospace Center)



https://transact-ecsel.eu/

Thank you!