PROJECT of the PEGASUS FAMILY

VERIFICATION VALIDATION METHODS

Learning Driven Product Lifecycle for Automated Driving Systems

Marcus Nolte, Institute of Control Engineering, TU Braunschweig

Based on: M. Haiber; T. Brade; T. Hoffmann; C. Lalitsch-Schneider; M. Nolte; J. Pott:
„Lerngetriebener Produktlebenszyklus für hochautomatisierte Fahrzeuge“,
Tag des Systems Engineering (TdSE), 2021

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Motivation

- Several industry players have recently started expanding services implemented by “automated vehicles”

- Safety remains key question
  - Needs to be **built-in**, not **bolt-on**!

- **“How safe is safe enough?”** is still not fully answered.

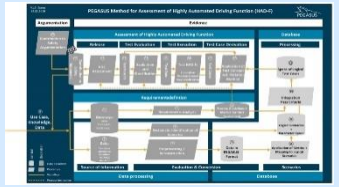
VV-METHODS PEGASUS family – Publicly-funded projects in Germany

- The **PEGASUS Family** focuses on development / testing methods and tools for AD systems on highways and in urban environments

PEGASUS

https://www.pegasusprojekt.de/en/home

- Scope: **Basic methodological framework**
- Use-Case: L3/4 on highways
- Partners: 17



PEGASUS FAMILY

VV-Methods

- Scope: **Methods, toolchains, specifications for technical assurance**
- Use-Case: L4/5 in urban environments
- Partners: 23 partners
- Timeline: 07/2019 – 06/2023

SET Level 4to5

- Scope: **Simulation platform, toolchains, definitions for simulation-based testing**
- Use-Case: L4/5 in urban environments
- Partners: 20 partners
- Timeline: 03/2019 – 08/2022

+ future projects of the PEGASUS Family

2016 2019 **Time**

VVM – Continuing the PEGASUS story of scenario-based testing

I. Systematic control of test space

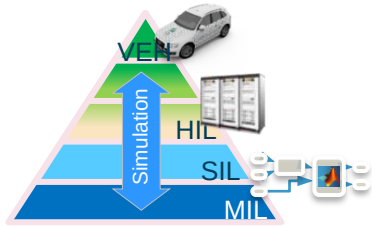
Methods to map the infinitely-complex open context onto a finite & manageable set of artifacts.

II. Consistent interfaces for systems and components

Definition of technical contracts, tests of systems and subsystems.

III. Significant shift from real-world testing to simulation

Methods for seamless testing across all test instances.

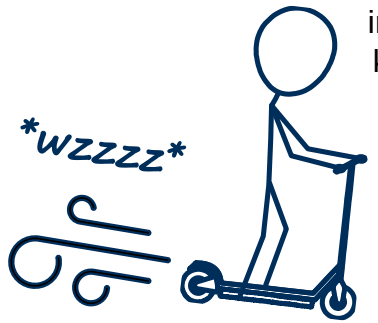


Added: IV Argumentation

- fulfillment of societal claims e.g safety, via law, standards, state of the art.

(Galbas 2022)

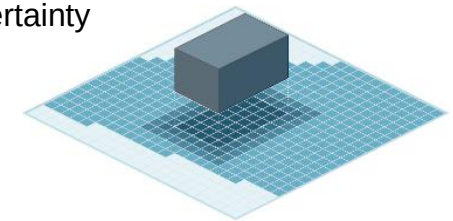
Open Context

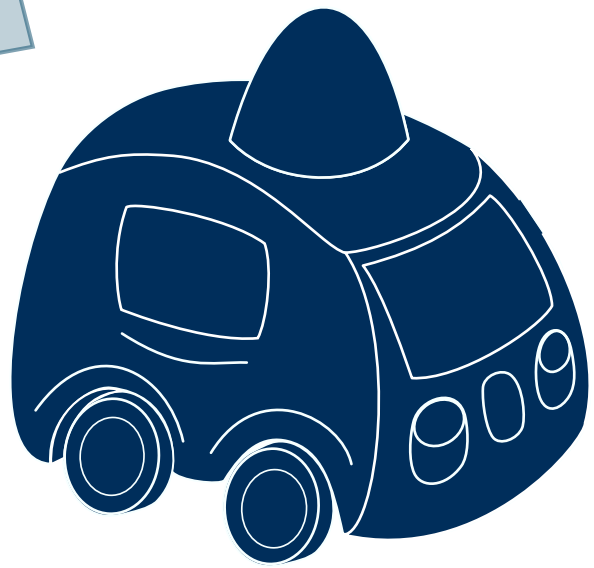


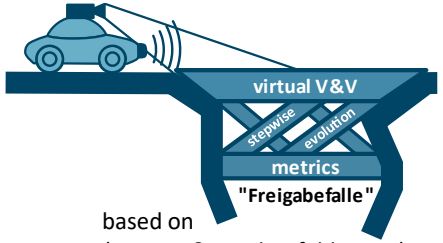
incomplete knowledge

incomplete requirements

measurement uncertainty

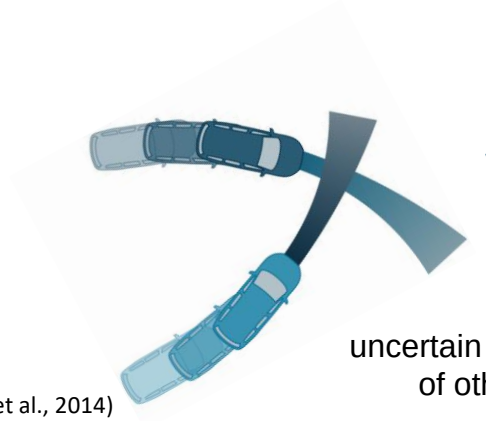






based on (Winner & Wachenfeld, 2013)

confidence in V&V process



uncertain behavior of others

based on (Lefèvre et al., 2014)

Risk

Challenges for a coherent assurance argument

How can we argue for the **abscence of unreasonable risk** in an open context?

…in a comprehensible manner for a variety of stakeholders?

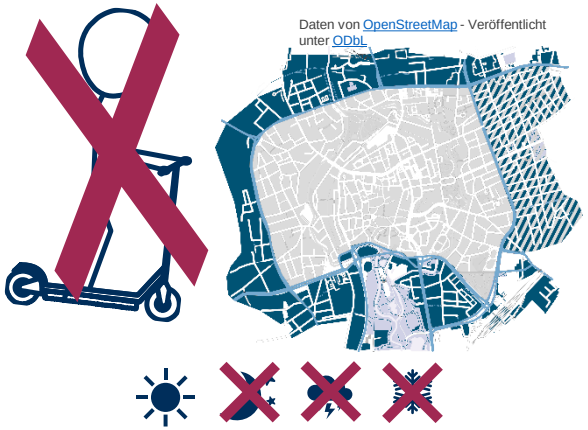
… to foster public trust in the technology?

…while lacking an exact interpretation of what „reasonable“ really means?

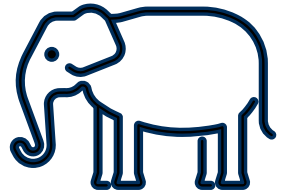
Traceable decomposition & continuous validation of claims

- Enable argumentation that safety case will remain valid, even if **system context changes**.
  - **Traceable** decomposition / interpretation of claims (assumptions)
  - Continuous **post-release** verification & validation w.r.t **new findings**: Do assumptions still hold?

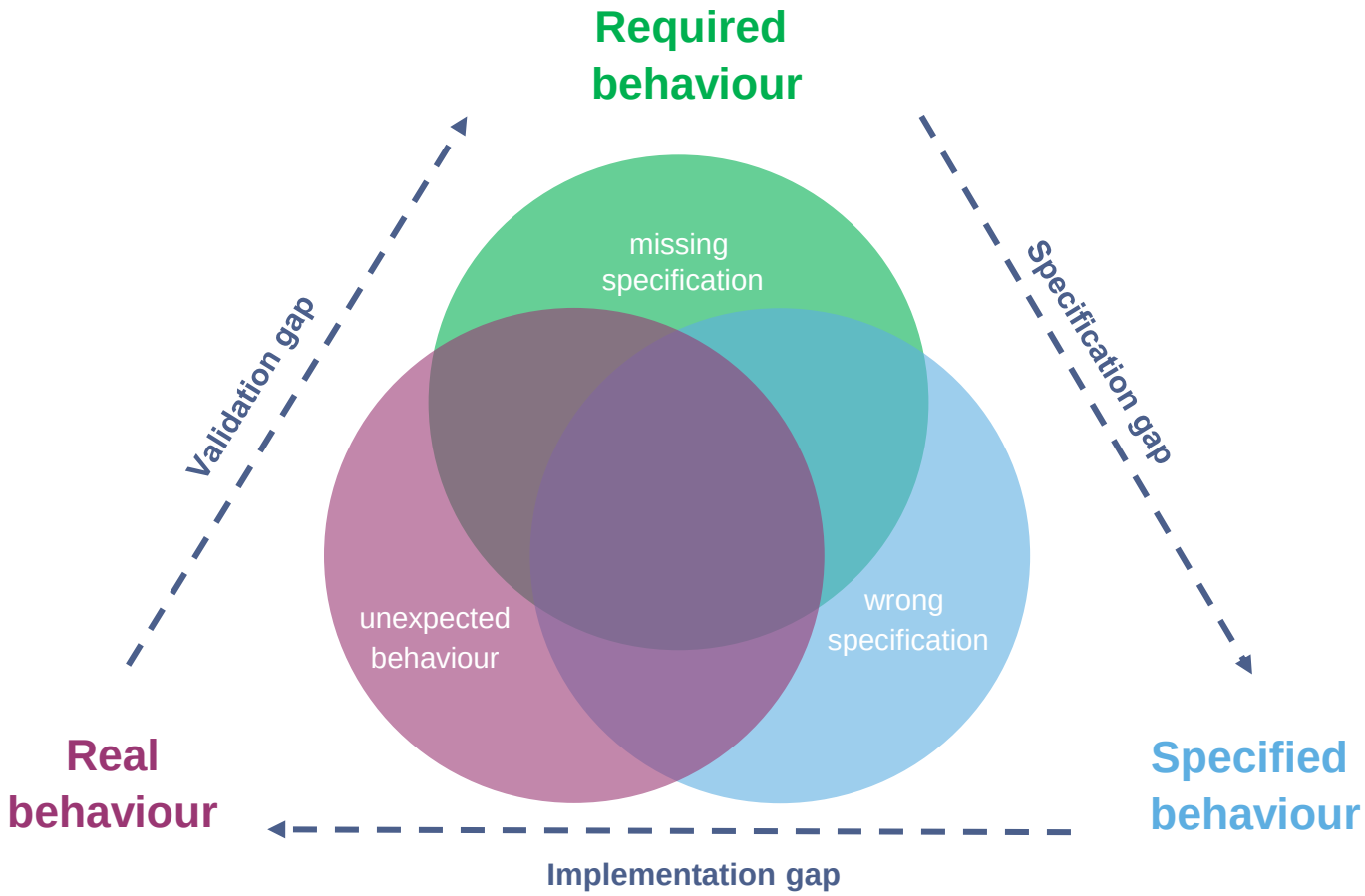
interpretation
of claims



continuous
V&V
of claims



Perspectives of argumentation



3-Circle-Model:
Stellet, J. E.; Brade, T.; Poddey, A.; Jesenski, S.; Branz, W.:
"**Formalisation and algorithmic approach to the automated driving validation problem**",
IEEE Intelligent Vehicles Symposium, 3rd Workshop on Ensuring and Validating Safety for Automated Vehicles (EVSAV), Paris, France, 2019

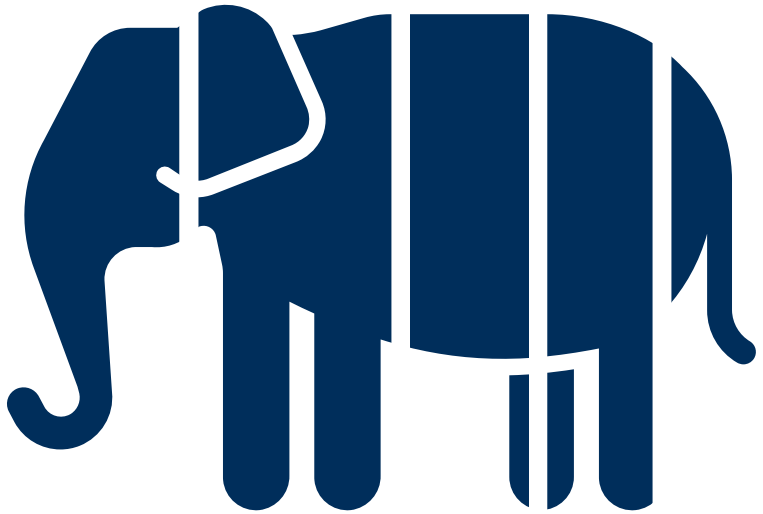
Assurance Framework

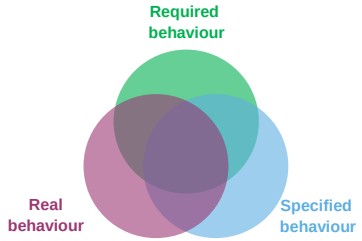
We must argue that the system in its environment is…

Specified, verfiable and validatable sufficiently complete & correctly

Designed, implemented, verified and validated correctly in a *controlled* environment

Safe under *uncontrollable* real-world conditions





(Reich, Nolte 2022)

Assurance Framework

We must argue that the system in its environment is…

Specified, verfiable and validatable sufficiently complete & correct

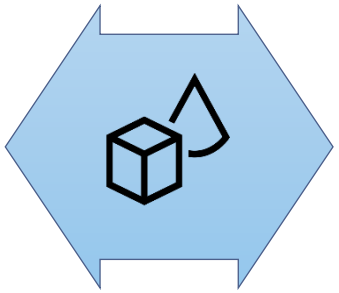
Designed, implemented, verified and validated correctly in a *controlled* environment

Safe under *uncontrollable* real-world conditions

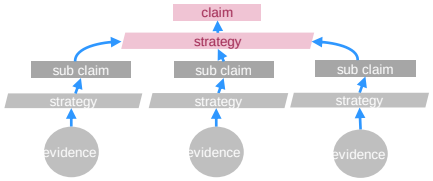
Capability Layer

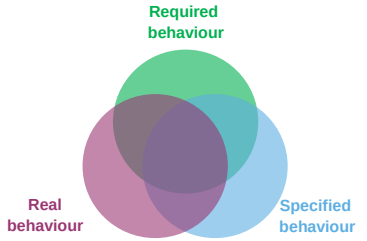
Engineering Layer

Real World Layer



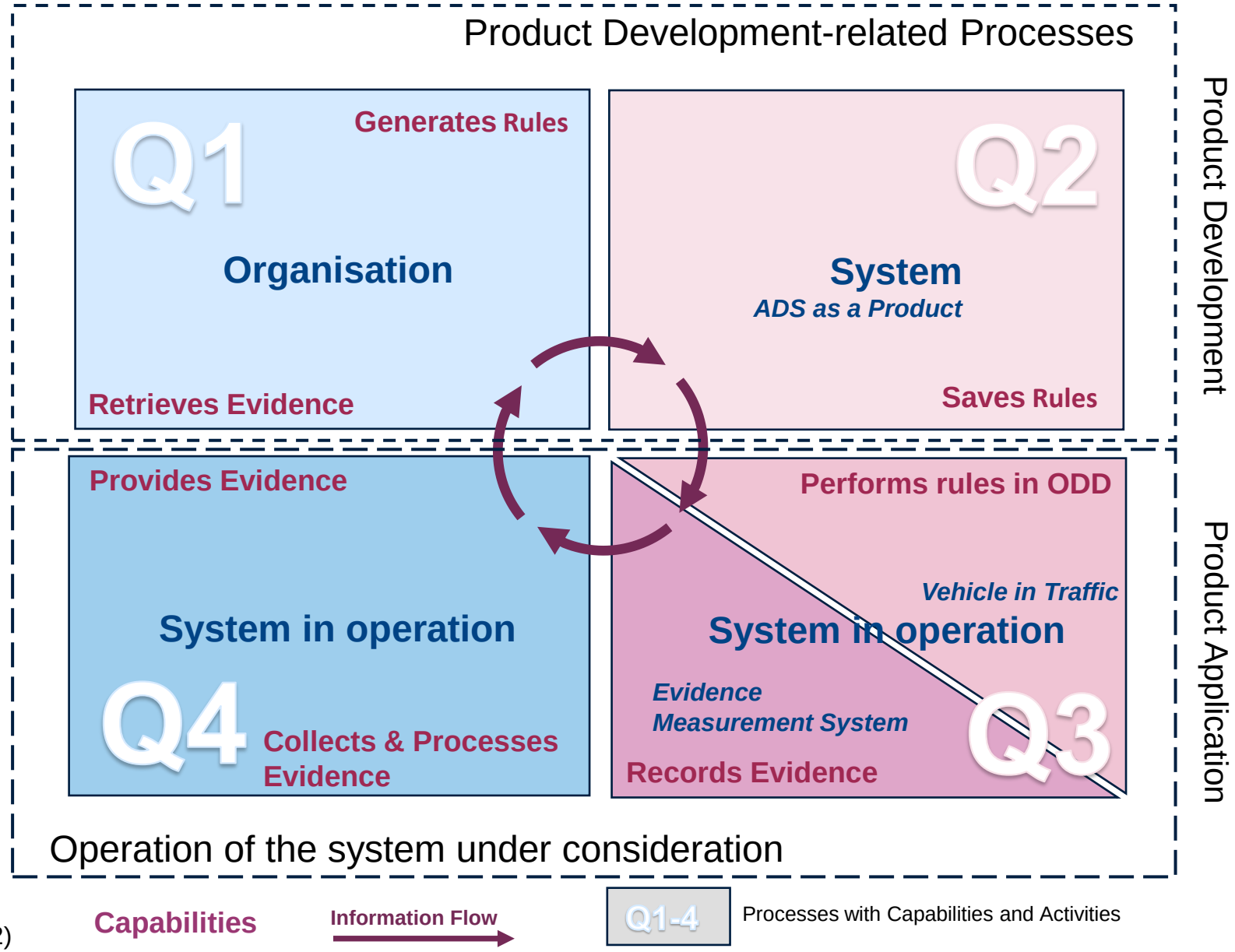
Assurance Case





(Reich, Nolte 2022)

Learning Driven Product Lifecycle



The Automated Driving System (ADS) is **diligently safeguarded** before release

(Haiber et al 2021, Corell 2022)

Learning Driven Product Lifecycle
“Four quadrant model”

VERIFICATION
VALIDATION
METHODS

- The Automated Driving System (ADS) is **proven safe at the time it is placed on the market**
- We monitor the systems to further **maintain safety** in the open context

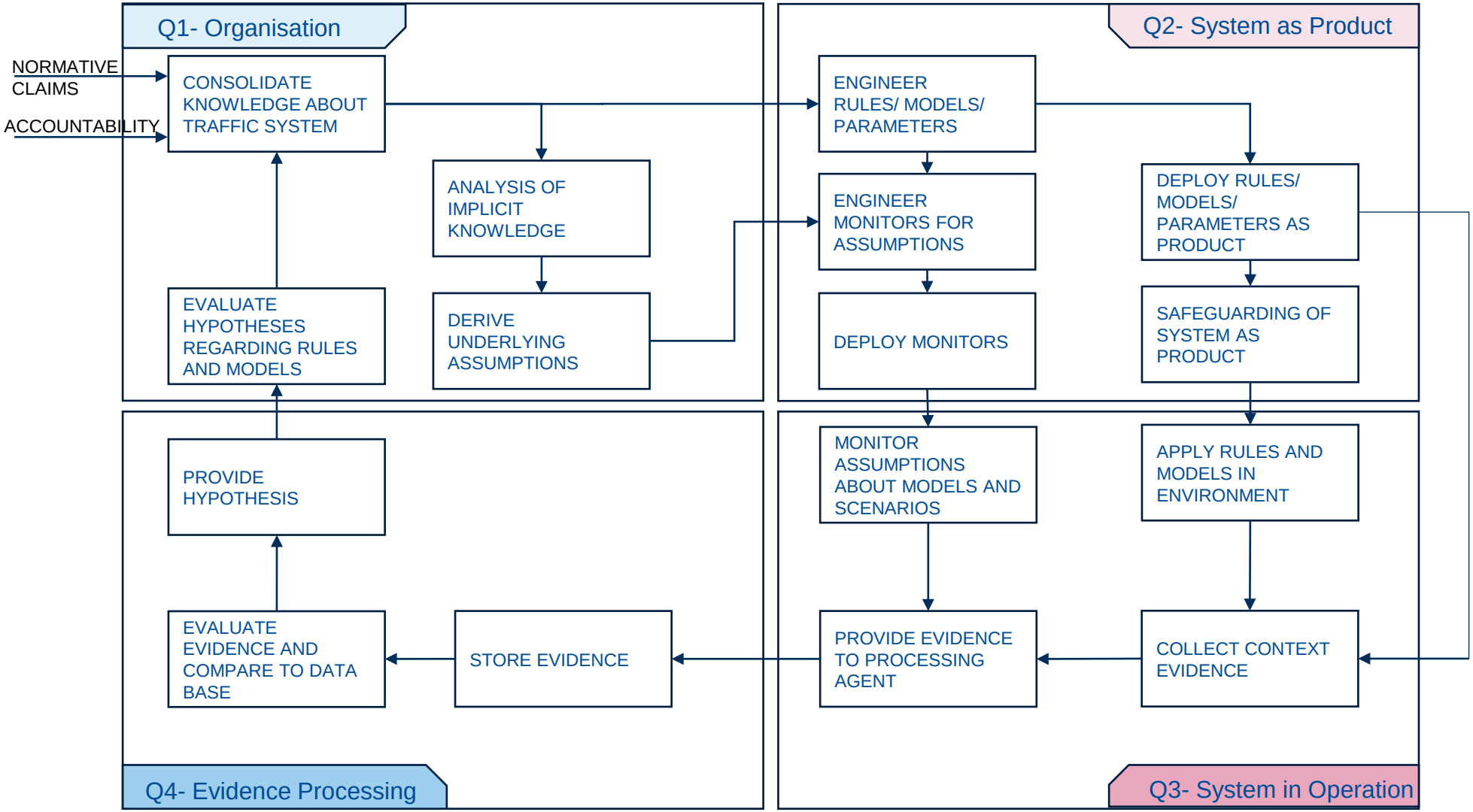
- Monitoring can take place via a **variety of paths**, e.g.
  - via **accident data analysis**
  - via observation of traffic flow
  - via fleet and sub-fleet
- **Monitoring must always be compliant with security and privacy laws!**

- ***We are testing during system development and not at the customer!***

(Haiber et al 2021, Corell 2022)

Learning Driven Product Lifecycle

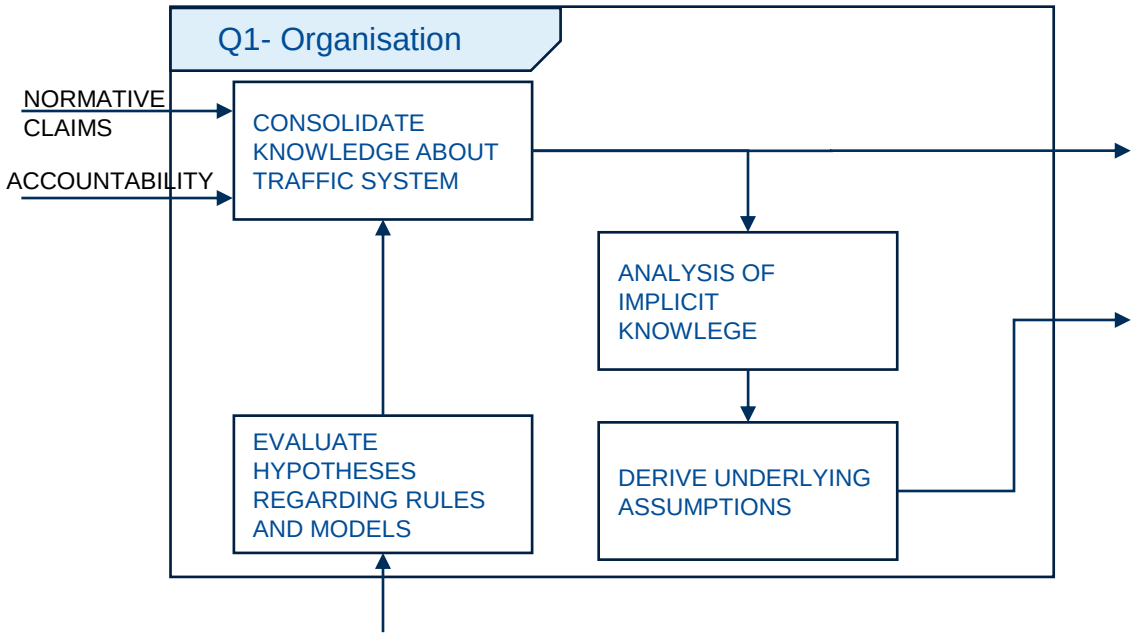
Activities in the “Four Quadrant Model”– Overview



Inspired by „Popper, Karl. Logik der Forschung. Springer Wien, 1935“

(Haiber et al 2021, Corell 2022)

Learning Driven Product Lifecycle
Activities in the “Four Quadrant Model”– Details Q1



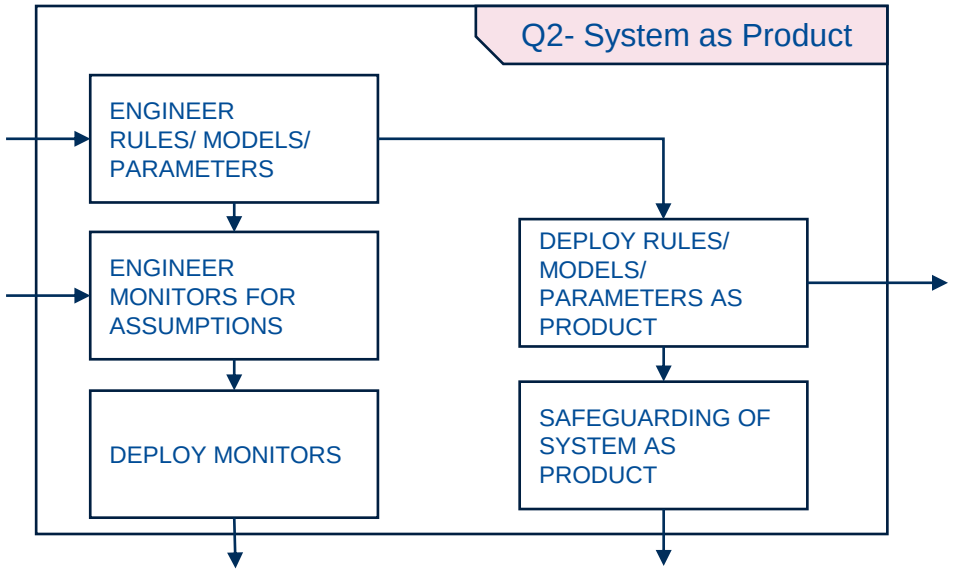
Q1 represents the Organization‘s „head“ with the accountability to normatives and its will to learn

- The **knowledge** of an organization enables the realization of a system as a product.
  Analyzing implicite knowledge and **deriving underlaying assumptions** enables the organization to define monitors
- Monitors initiate a learning process about system in opereration performance (reply on hypothesis)
- **Evaluating the hypothesis** regarding rules and models is the analysis activity for generating valuable knowledge for the organization

1 | 2 | Staffort Beer –Viable System Model, Cybernetics and Management, English Universities Press, Ltd., 1959

(Haiber et al 2021, Corell 2022)

Learning Driven Product Lifecycle
Activities in the “Four Quadrant Model”– Details Q2



Q2 represents the Organization‘s „body“ including the activities in development and production.

- **Engineering rules / models / parameters** is part of the design process of the system as a product
- The **rules / models / parameters** are **deployed** after design phases and before system operation
- The **engineering of monitors for assumptions** is running in parallel, based on the derived underlying assumptions
- **Monitors are deployed** before system operation

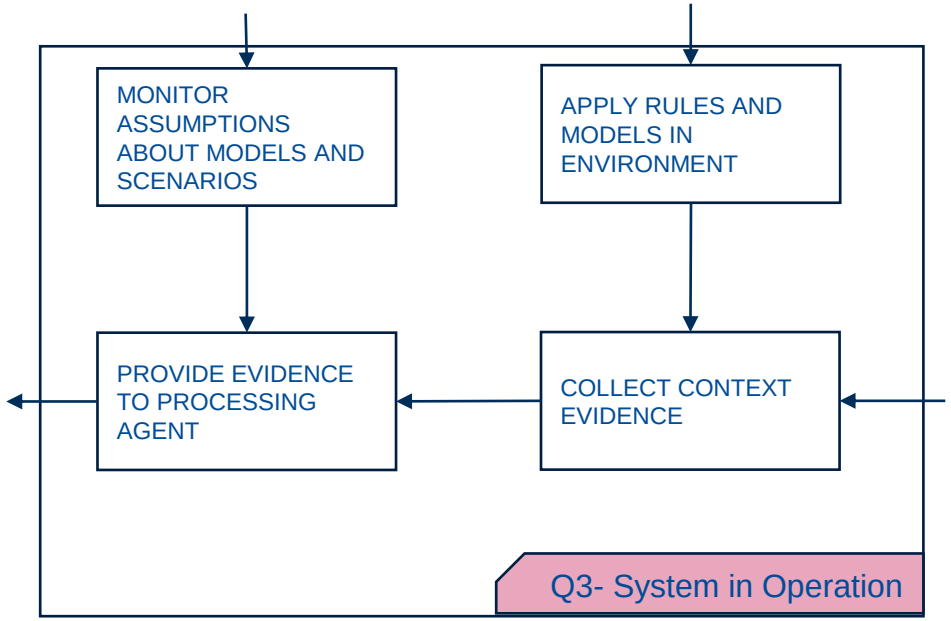
- **Safeguarding activity close the activities of Q2**

2 | Staffort Beer –Viable System Model, Cybernetics and Management, English Universities Press, Ltd., 1959

(Haiber et al 2021, Corell 2022)

Learning Driven Product Lifecycle

Activities in the “Four Quadrant Model” – Details Q3



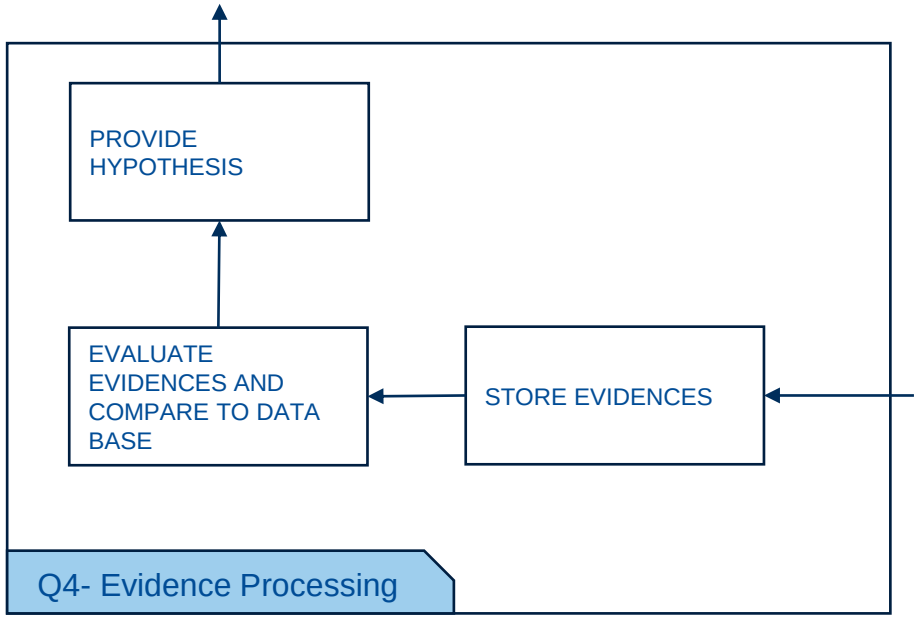
Q3 represents the System in Operation (SiO) applying the implemented rules, modes and parameters

- In parallel the system in operation is **monitoring** its assumptions about models and scenarios
- During mission run, the System in Operation is **collecting** relevant evidences in Operational Environment
- Both activities, applying and monitoring are **providing** relevant evidences (data) to a processing agent

3 | Evidence = Data used to confirm or refute the assumed rules, models and parameters

(Haiber et al 2021, Corell 2022)

Learning Driven Product Lifecycle
Activities in the “Four Quadrant Model” – Details Q4



Q4 represents the evidence processing agent

- The evidence processing agent is collecting and **storing** the relevant evidences
- And **evaluating** by comparing evidences to existing data within the data base.
  New hypothesis are formulated, which are
- **Provided** to the organization by the agent

3 | Evidence = Data used to confirm or refute the assumed rules, models and parameters

(Haiber et al 2021, Corell 2022)

Learning Driven Product Lifecycle

Summary

- The replacement of the human driver requires a shift of responsibility to cope with an open context
- A **dedicated learning process** supports the shift of responsibility, which allows an effective, sustainable knowledge and perspective on the world. Commonly established processes like conventional Market Observation and Quality Management are limited to cope with this challenge
- The **implementation of monitors** enables this shift of responsibility for an organization to refute or confirm assumptions made during the design process.
- Shadowing System is **one example** of implemented monitors.
- The results and new gained knowledge can be used to **improve the system**.
  This opportunity can increase the safety on fleet level, adding **positive value to the risk balance** by providing new findings and improvements to all systems in operation

(Haiber et al 2021, Corell 2022)

VERIFICATION
VALIDATION
METHODS

Thank you!

Marcus Nolte, *TU Braunschweig*

nolte@ifr.ing.tu-bs.de +49 531 391 3827

https://www.researchgate.net/profile/Marcus_Nolte

https://www.linkedin.com/in/marcus-nolte-95974a143/

PROJECT of the PEGASUS FAMILY

A project developed by the VDA Leitinitiative autonomous and connected driving

Supported by:

Federal Ministry for Economic Affairs and Climate Action

on the basis of a decision by the German Bundestag