PROJECT of the PEGASUS FAMILY

VERIFICATION VALIDATION METHODS

Mid-Term Presentation 15 / 16 March 2022

VVM Assurance Argumentation
How to systematically organize the approval concerns for safe AD systems in a structured framework?

Jan Reich, Fraunhofer Institute for Experimental Software Engineering IESE

Marcus Nolte, TU Braunschweig - Institute of Control Engineering

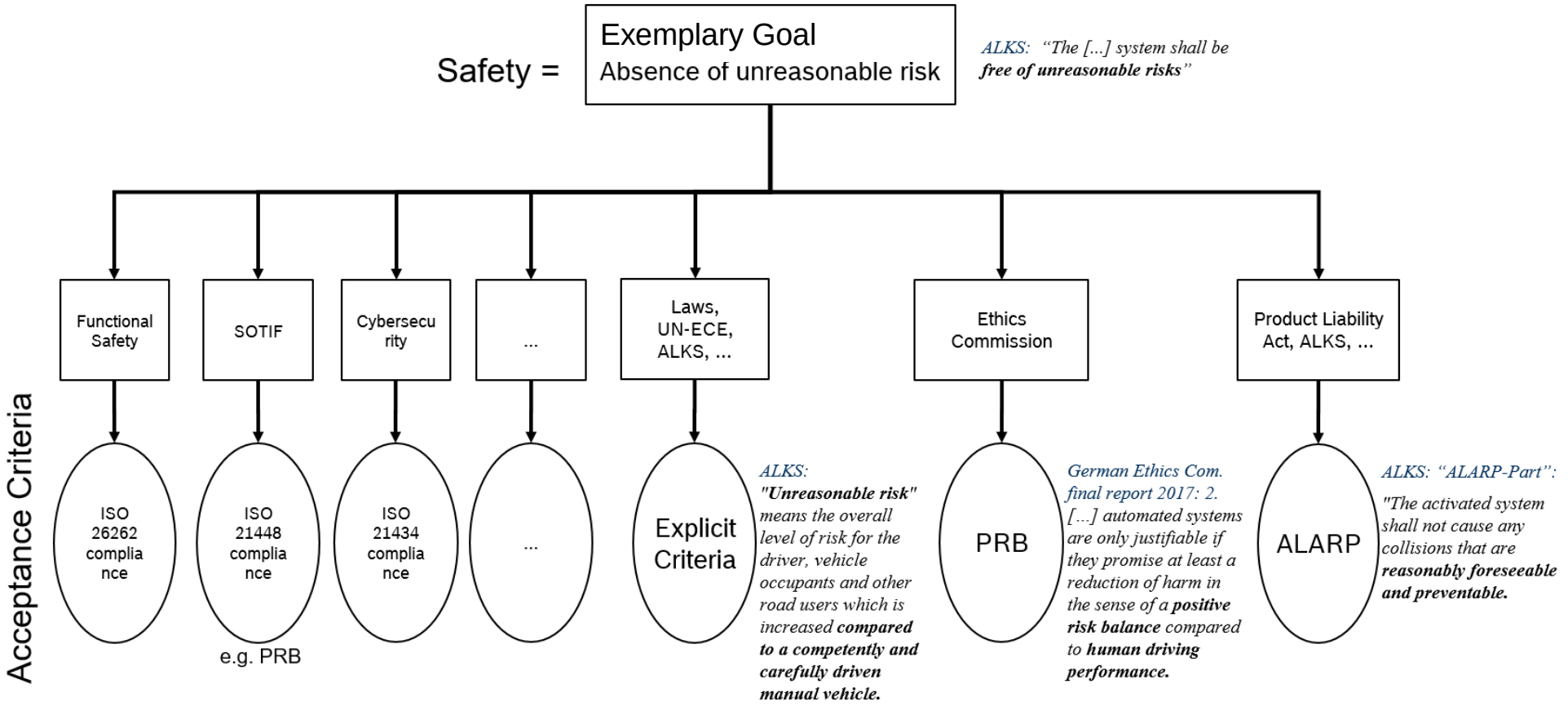
Supported by:

Federal Ministry for Economic Affairs and Climate Action

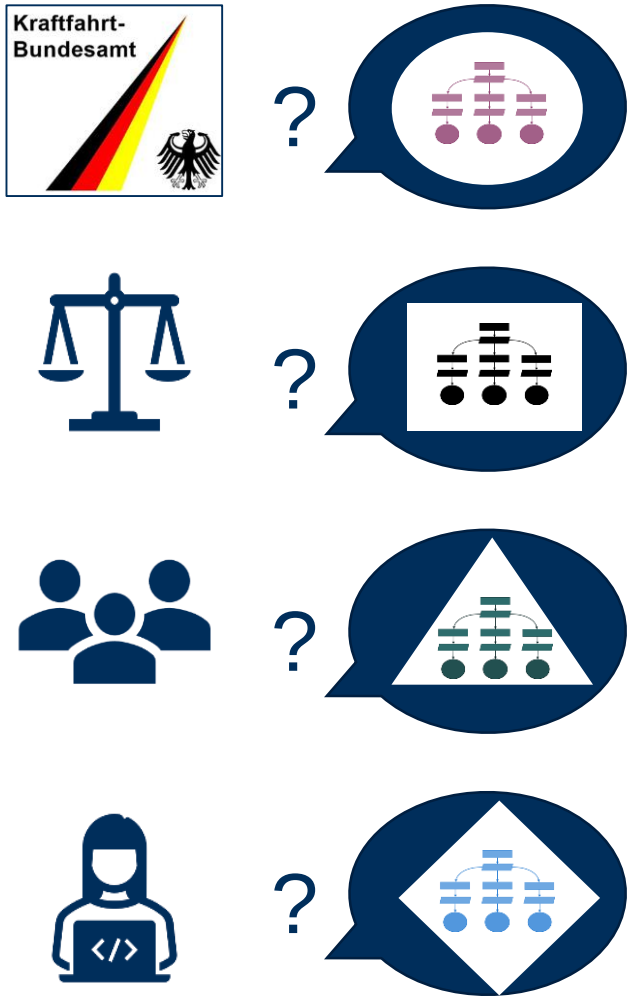
on the basis of a decision by the German Bundestag

Beyond Technology:
What do we mean by Safety or Acceptance Criteria?

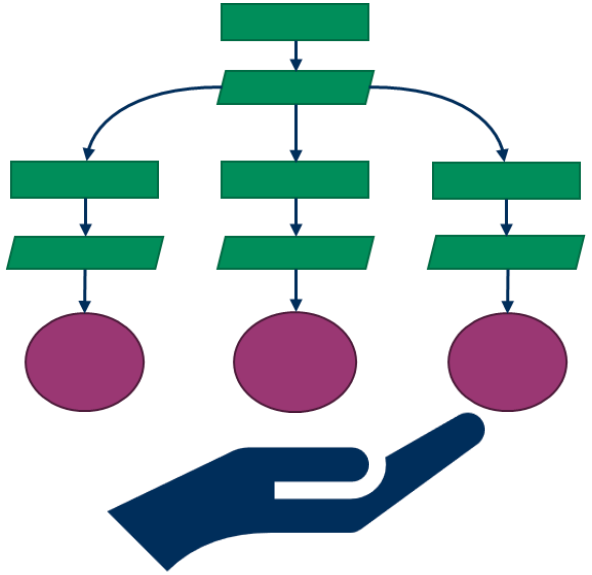
- Society, Standards, Regulations …



Different stakeholders and their requirements to argumentation

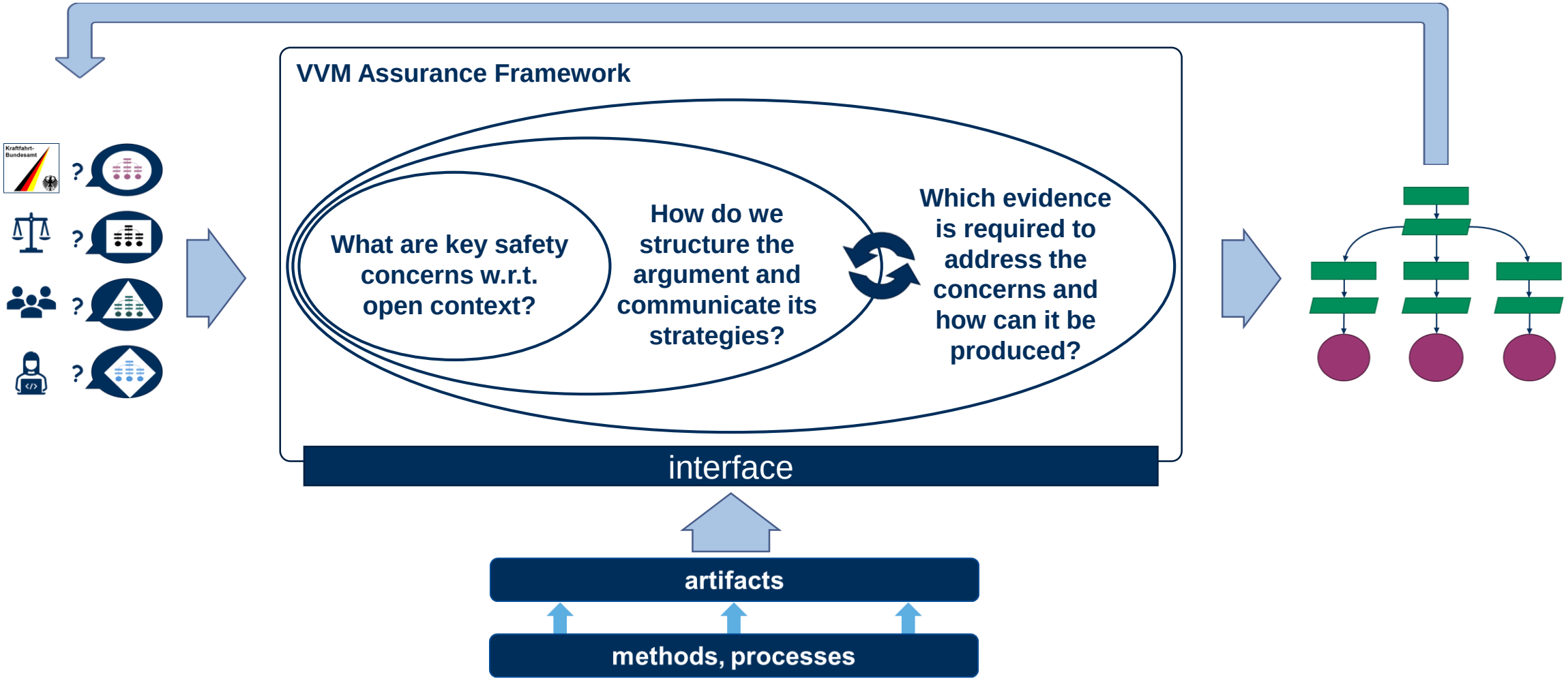


Argumentation of
Abscence of unreasonable risk in an open context…



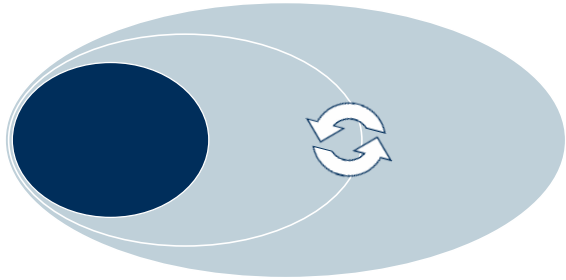
…satisfying varying concerns and needs of stakeholders?

The VVM Assurance Framework in context

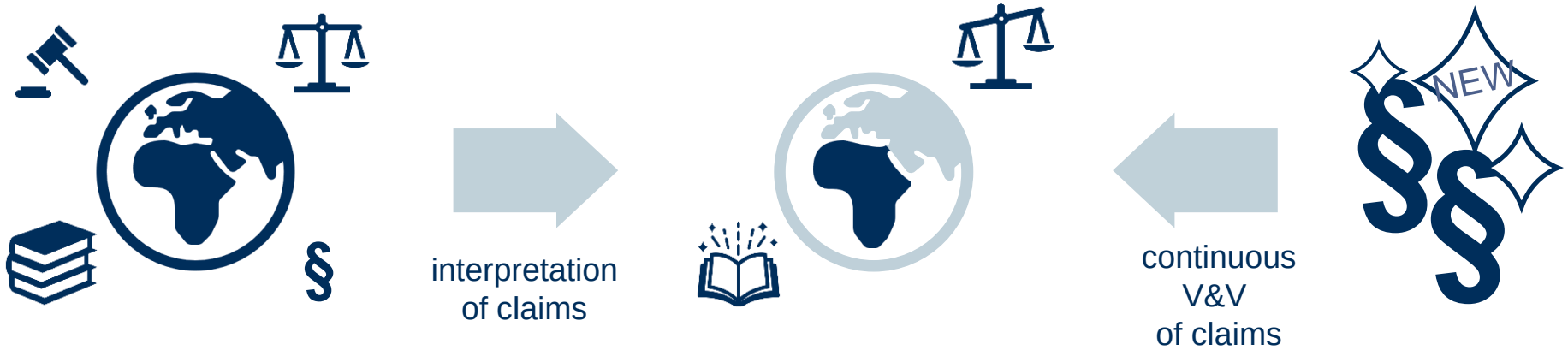


Traceable decomposition & continuous validation of claims

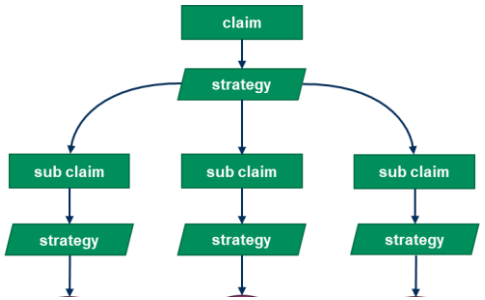
- Concern: Assurance case must remain valid, even when **system context changes**

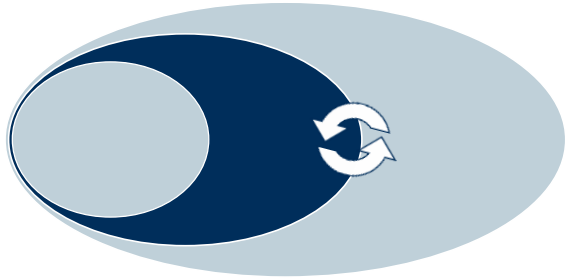


  - **Traceable** decomposition / interpretation of claims (assumptions)
  - Continuous **post-release** verification & validation w.r.t **new findings**: Do assumptions still hold?



Top-Level Argumentation Strategy





AD system is safe

normative

…**objective**

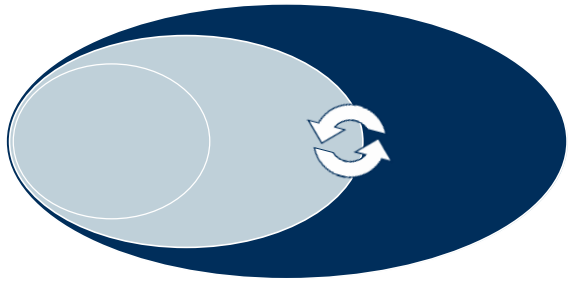
…**subjective**

adherence to normative aspects, e.g. law, standards

quantitative evidence to address residual uncertainty in normative branch

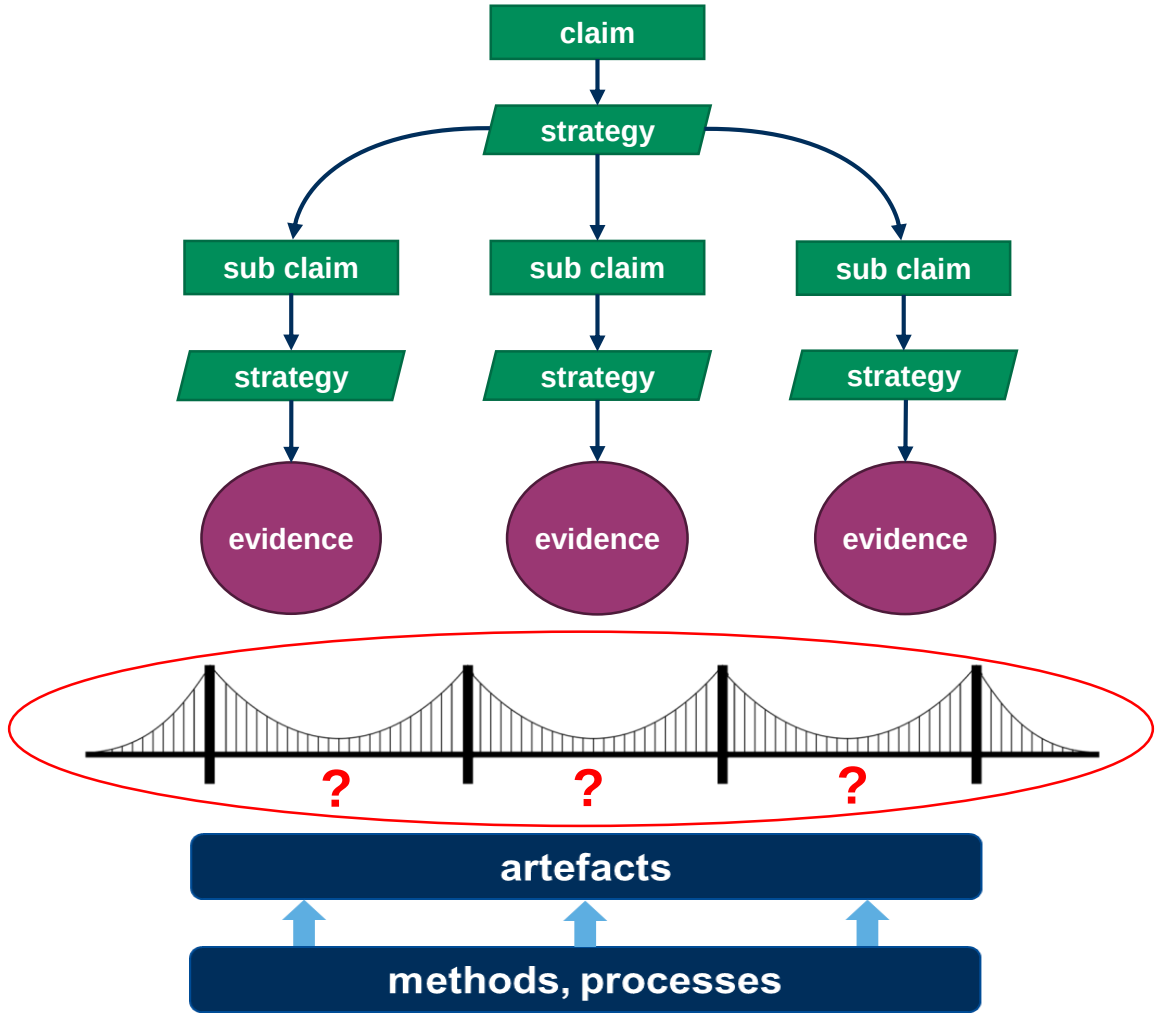
non-objective perspective, e.g. **qualitative** arguments addressing doubts of single experts

Interface between argumentation and methods



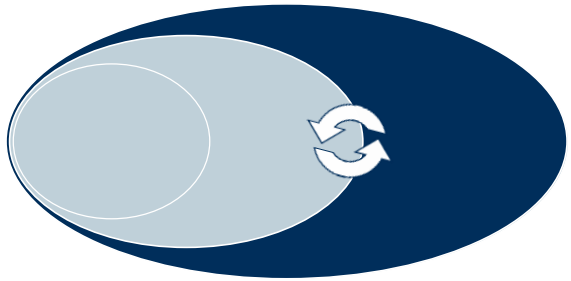
- Not necessarily self-explaining, i.e. accessible for every relevant stakeholder
- **No direct connection** between the argument's structure & processes for evidence generation

- Goal:
  - Order and address common **key concerns** and derive evidence that shall be realistically producible by methods, processes

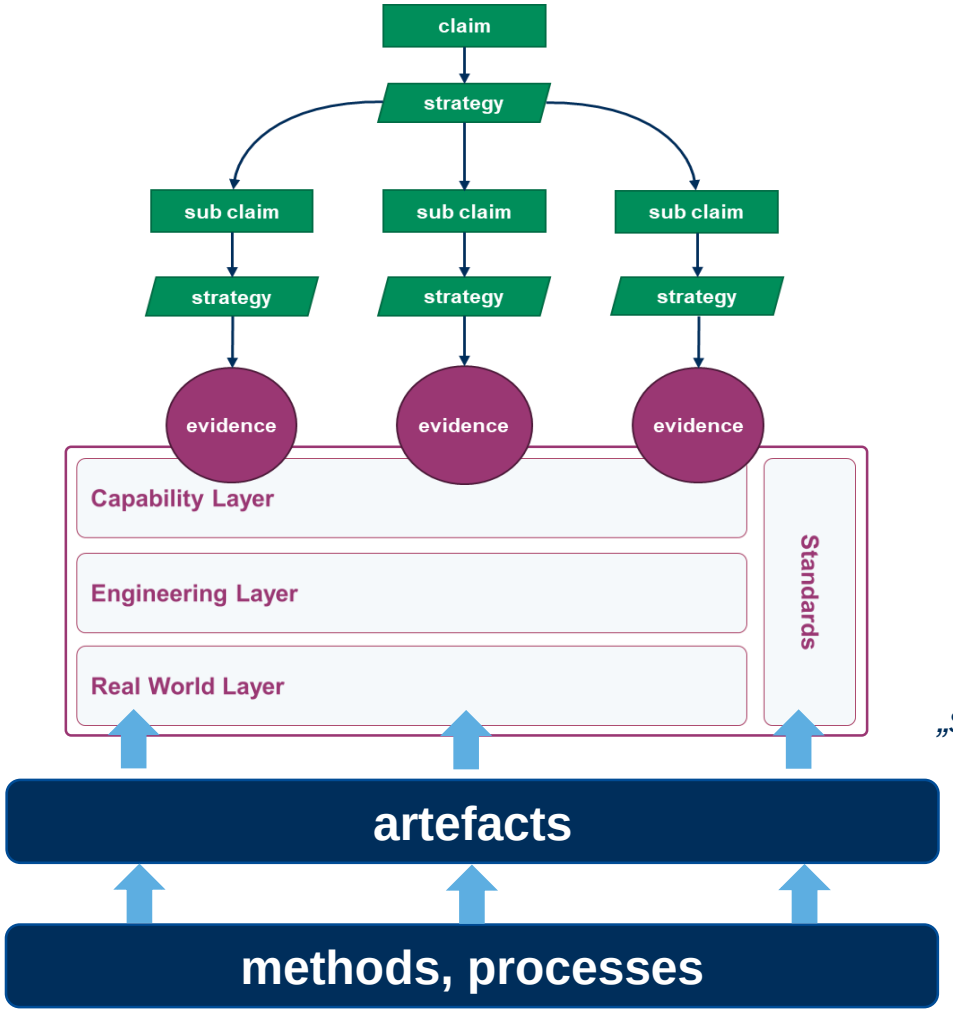


based on (Reich, 2021)

Principles for a coherent, comprehensible and traceable safety argument

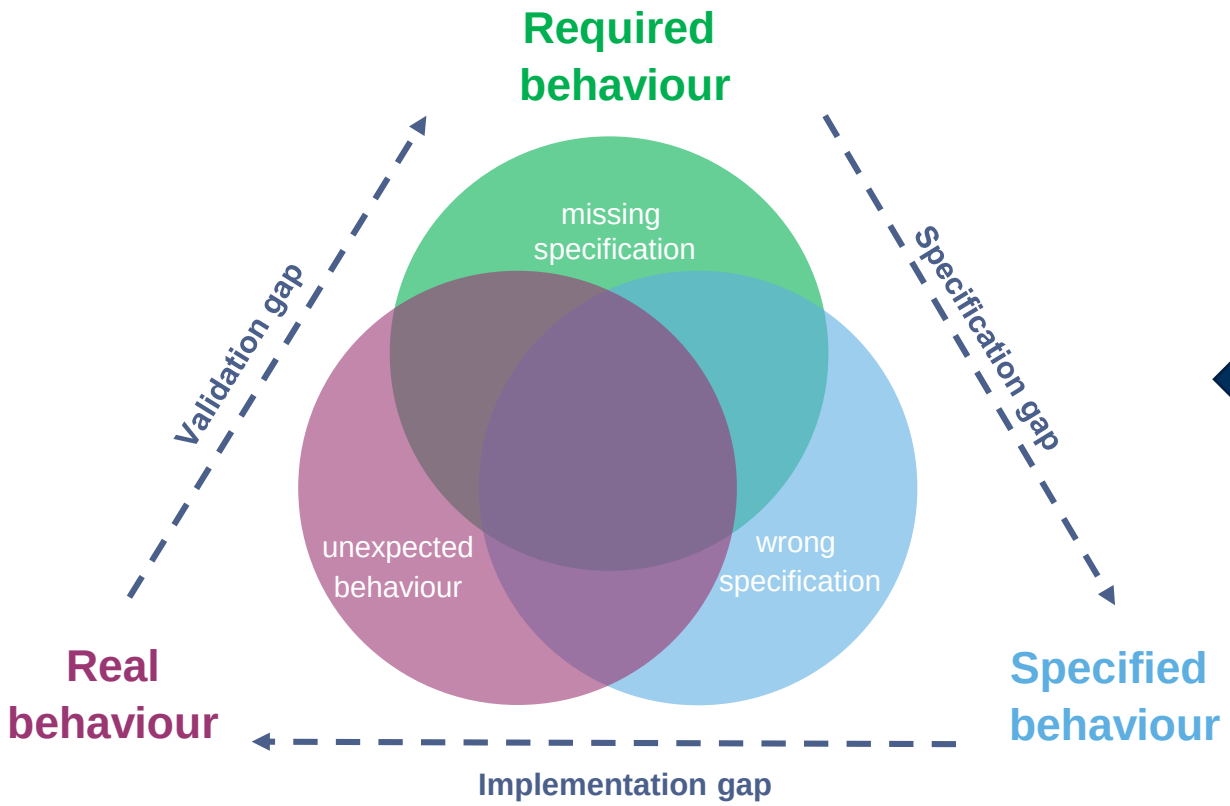


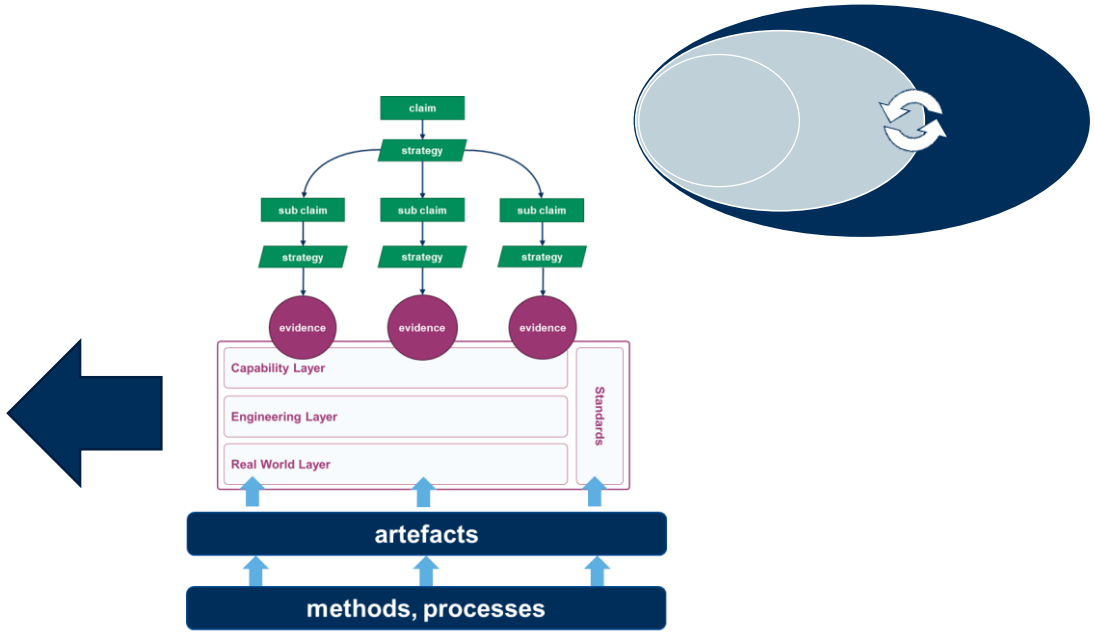
- We need to connect methods, artefacts, evidence & argumentation structure:
  - A **suitable level of abstraction** to argue the decomposition of the open context
  - **Architectural approach** as integral part of the safety argument to achieve traceability of artifacts, methods
  - Compatibility with **relevant industry standards**



„slicing the elephant“

Secondary argumentation strategy: 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

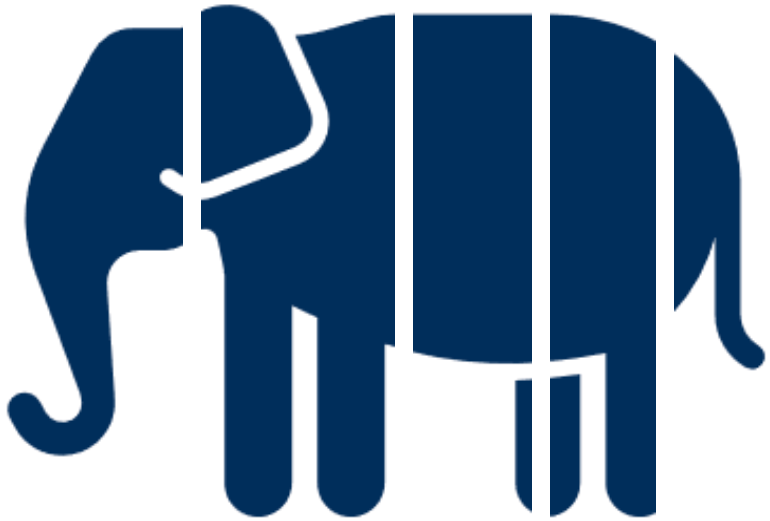
VERIFICATION
VALIDATION
METHODS

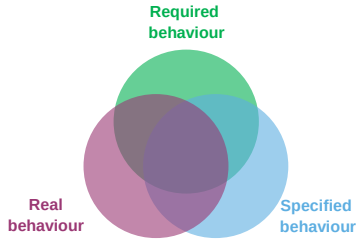
We must argue that the system in its environment is…

Specified, verfiable and validatable
sufficiently complete & correct

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

Safe under *uncontrollable* real-world conditions





Assurance Framework

We must argue that the system in its environment is…

Specified, verfiable and validatable sufficiently complete & correct

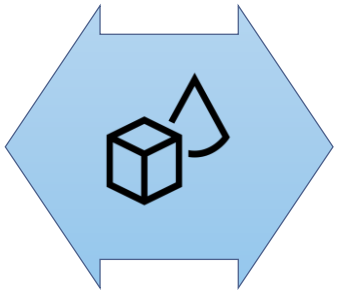
Designed, implemented, verified and validated correctly in a *controlled* environment

Safe under *uncontrollable* real-world conditions

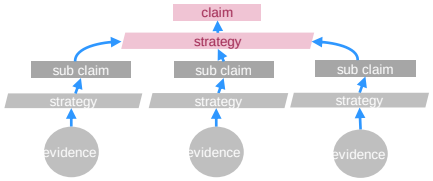
Capability Layer

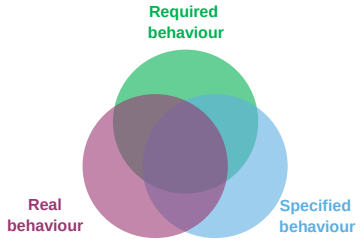
Engineering Layer

Real World Layer

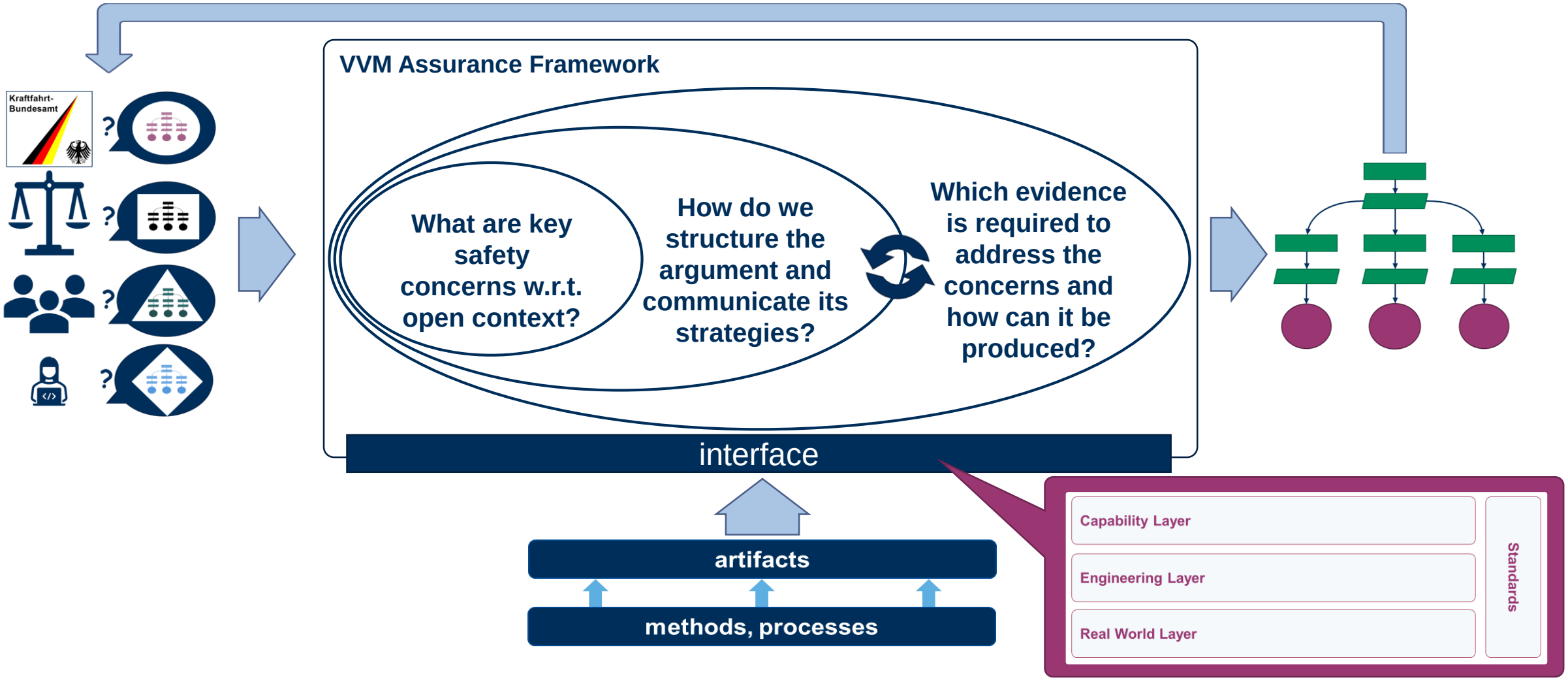


Assurance Case

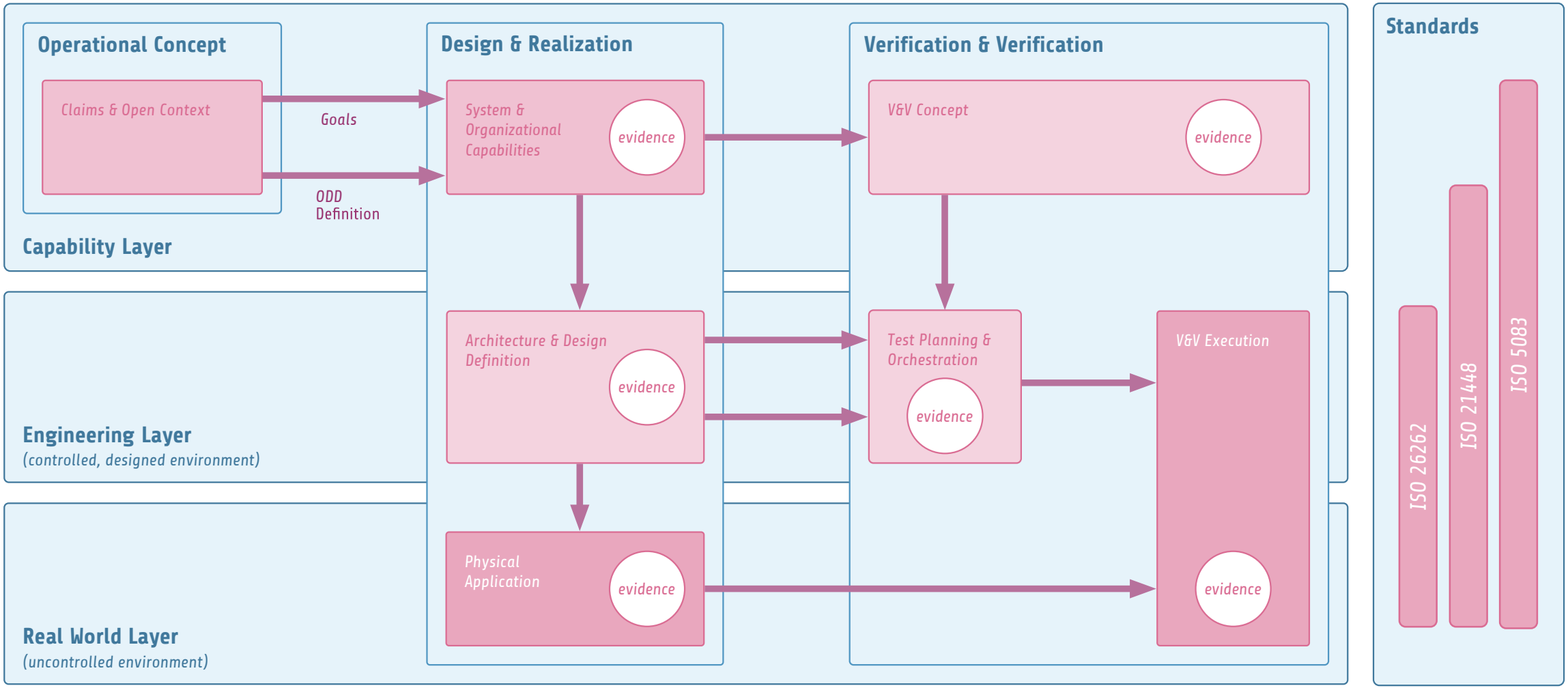




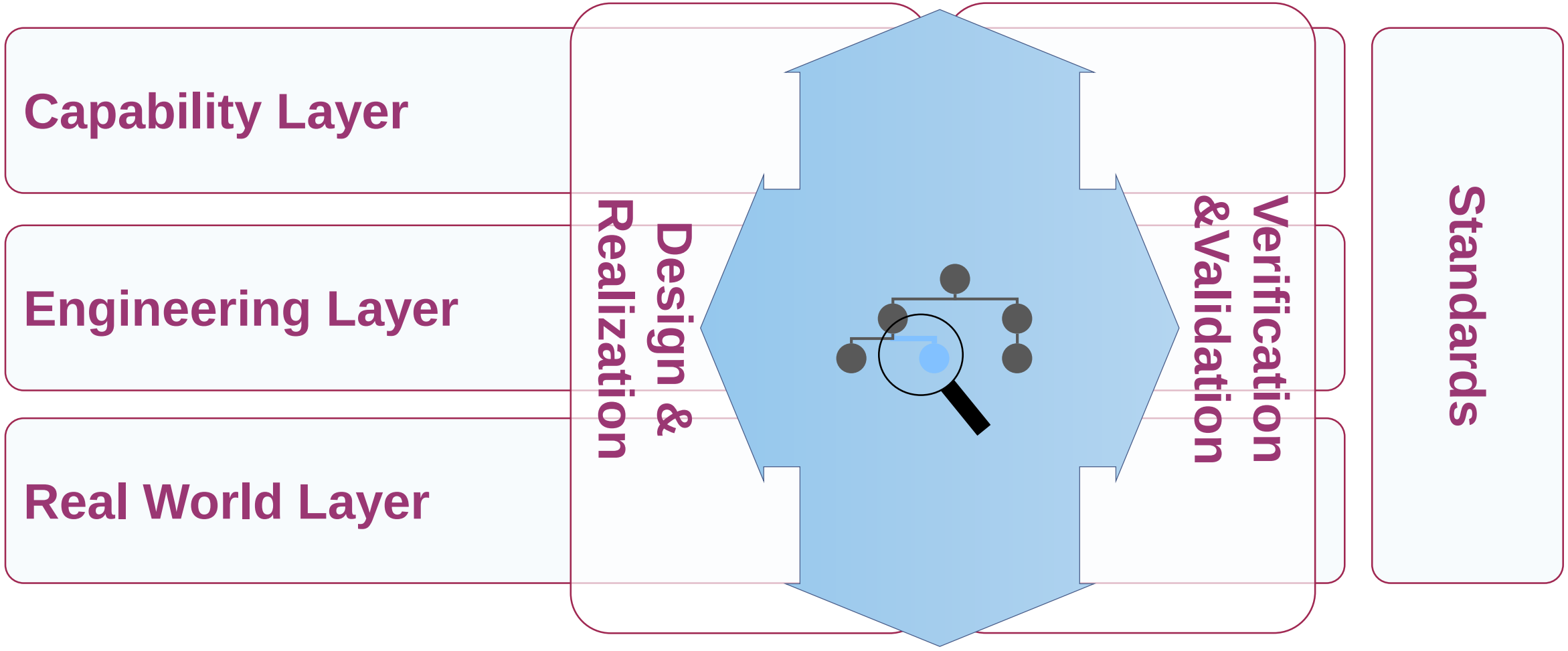
The VVM Assurance Framework in context



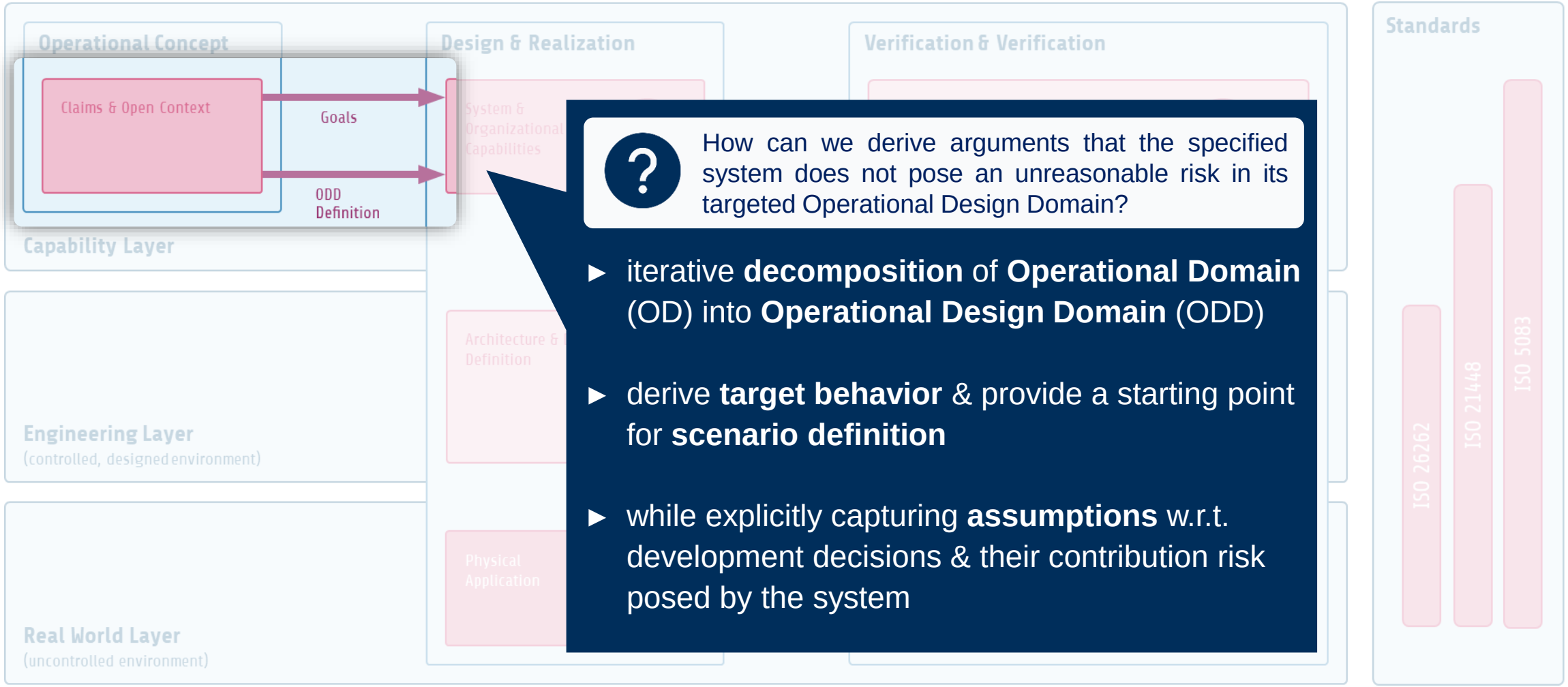
V&V Process in Assurance Framework



Assurance Framework



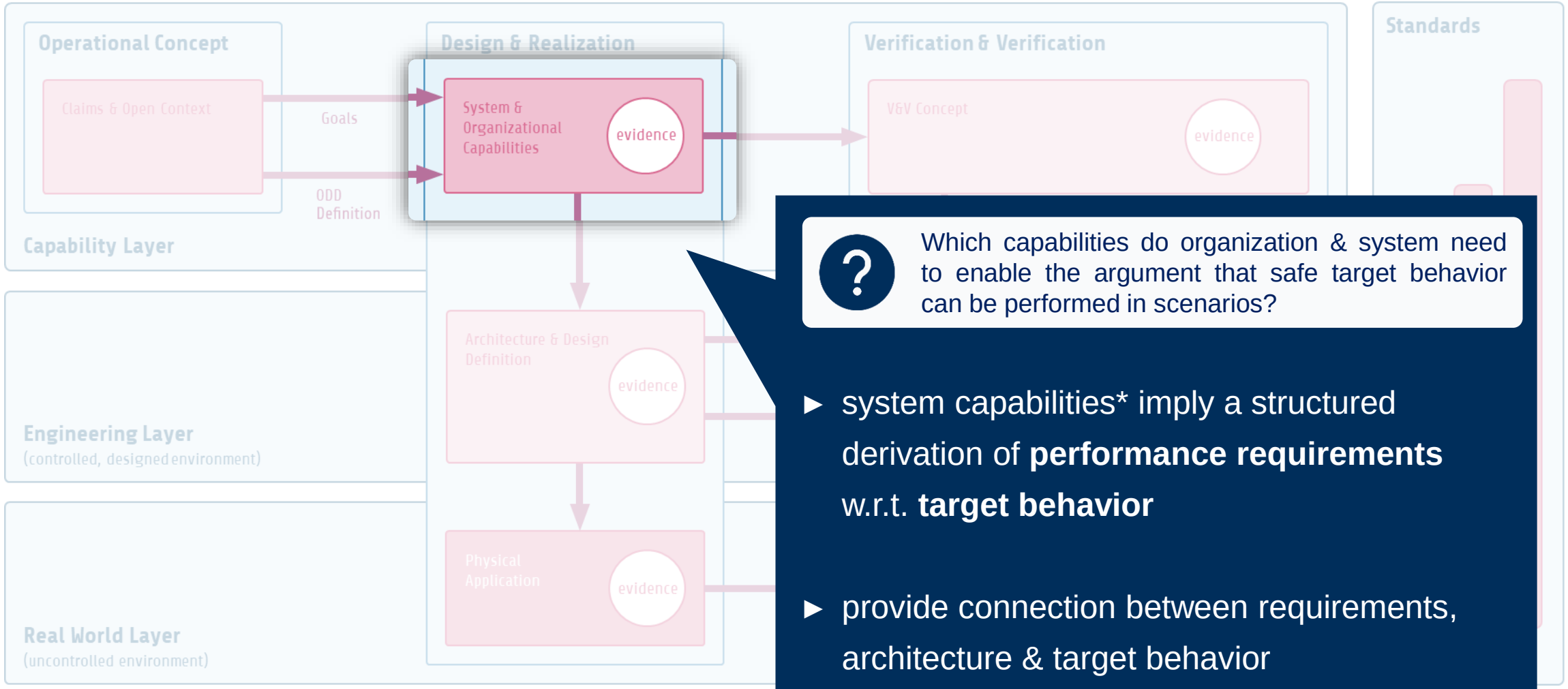
V&V Process in Assurance Framework



How can we derive arguments that the specified system does not pose an unreasonable risk in its targeted Operational Design Domain?

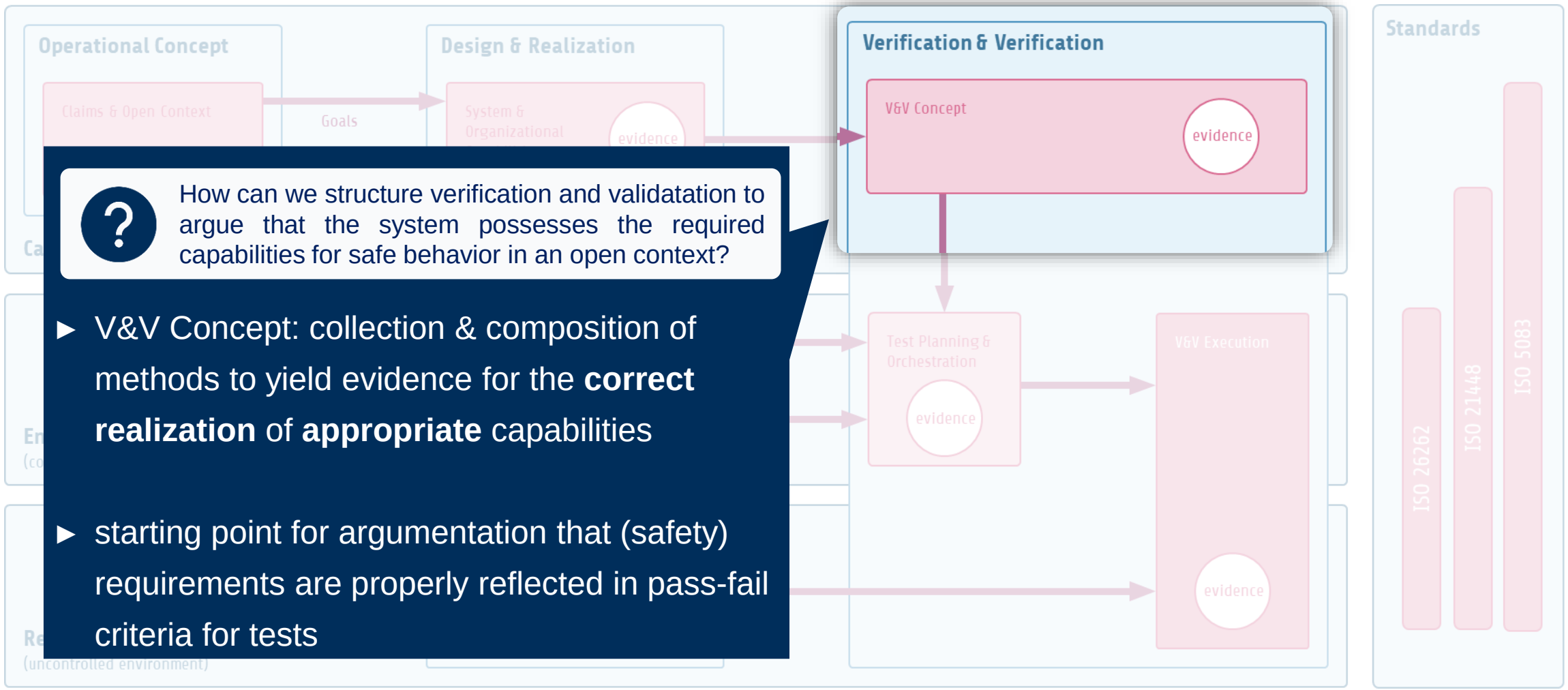
- iterative **decomposition** of **Operational Domain** (OD) into **Operational Design Domain** (ODD)
- derive **target behavior** & provide a starting point for **scenario definition**
- while explicitly capturing **assumptions** w.r.t. development decisions & their contribution risk posed by the system

V&V Process in Assurance Framework

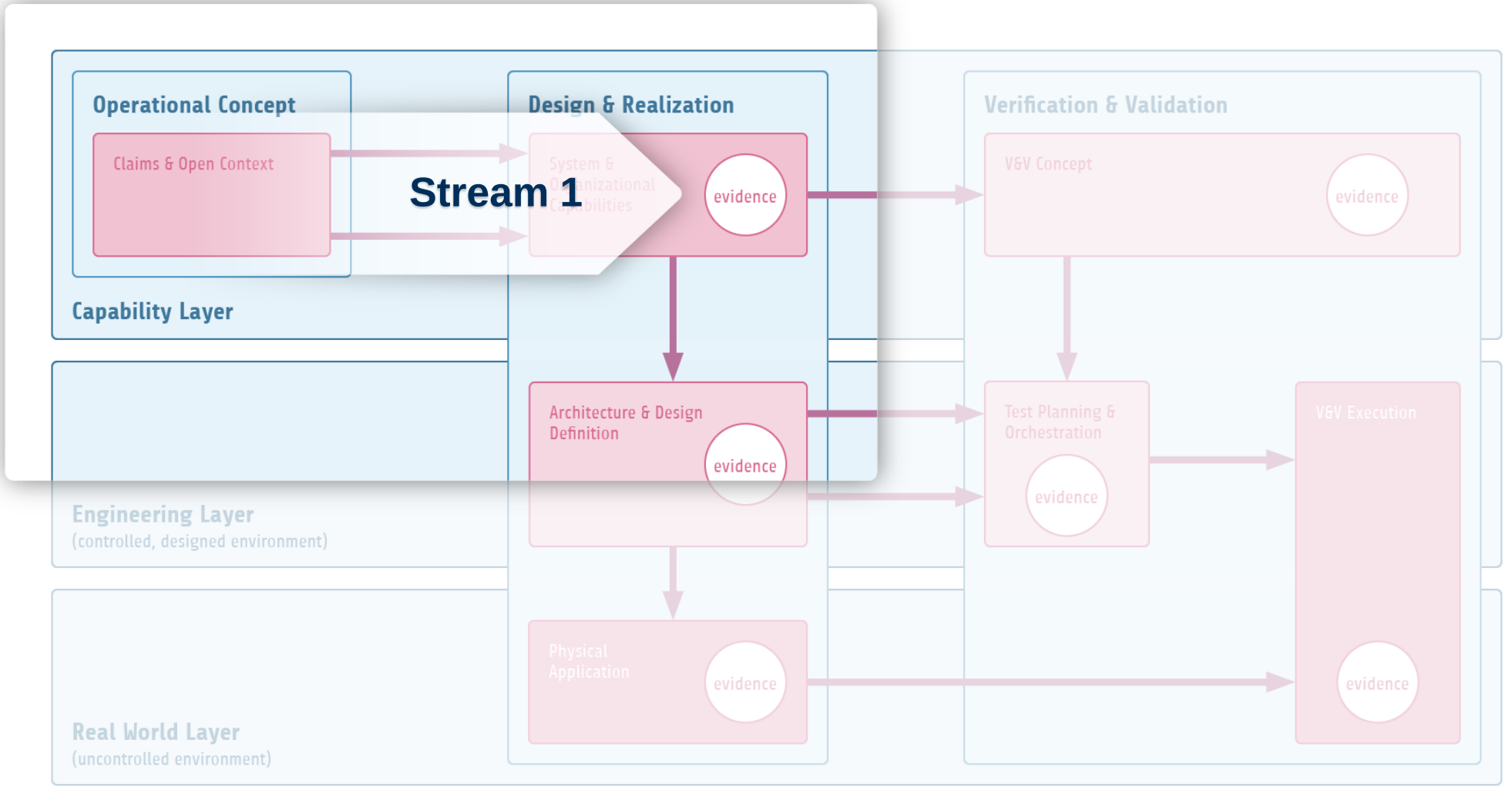


*capability: Potential to perform an outcome-based action (with a certain performance) – (based on Wasson, 2005)

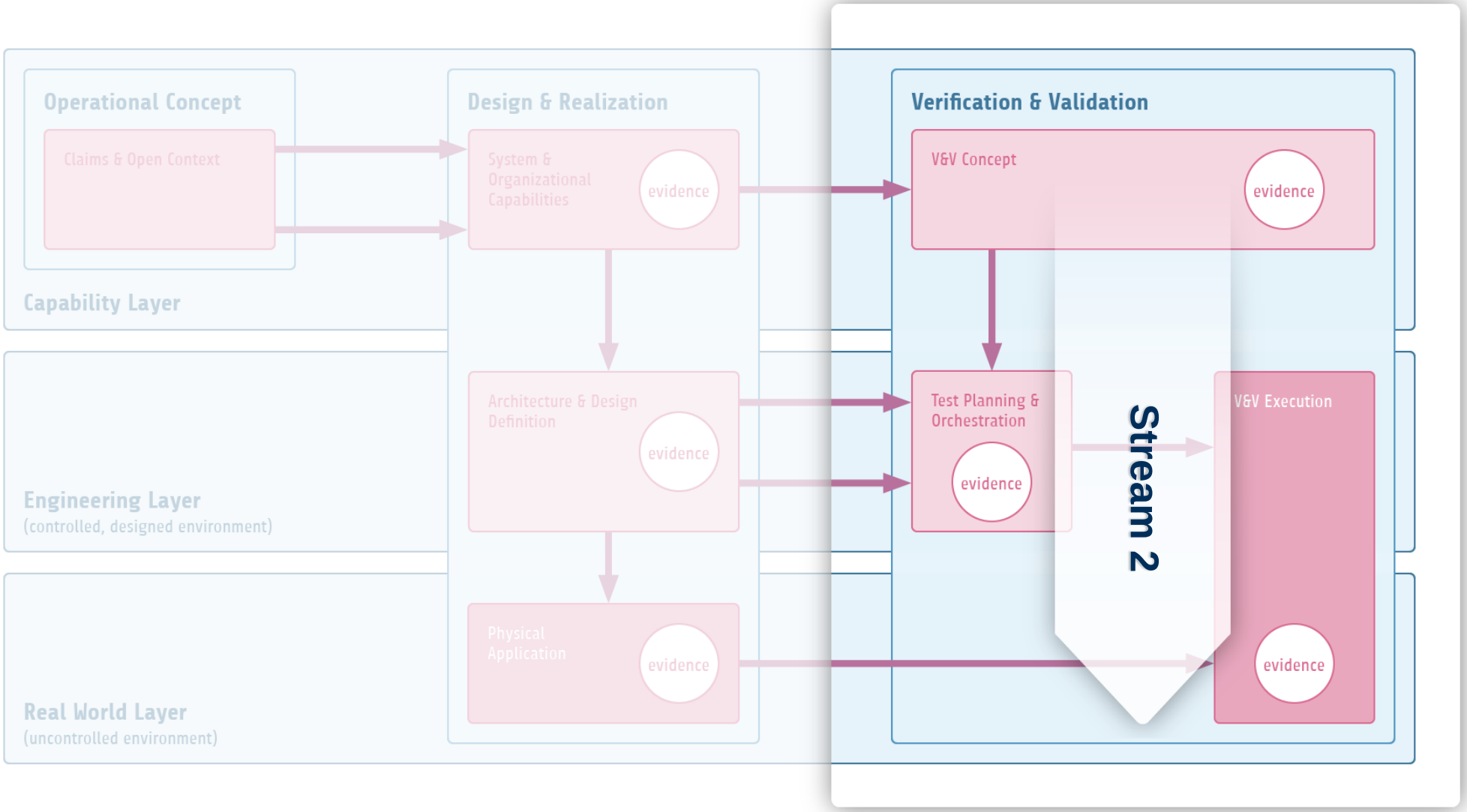
V&V Process in Assurance Framework



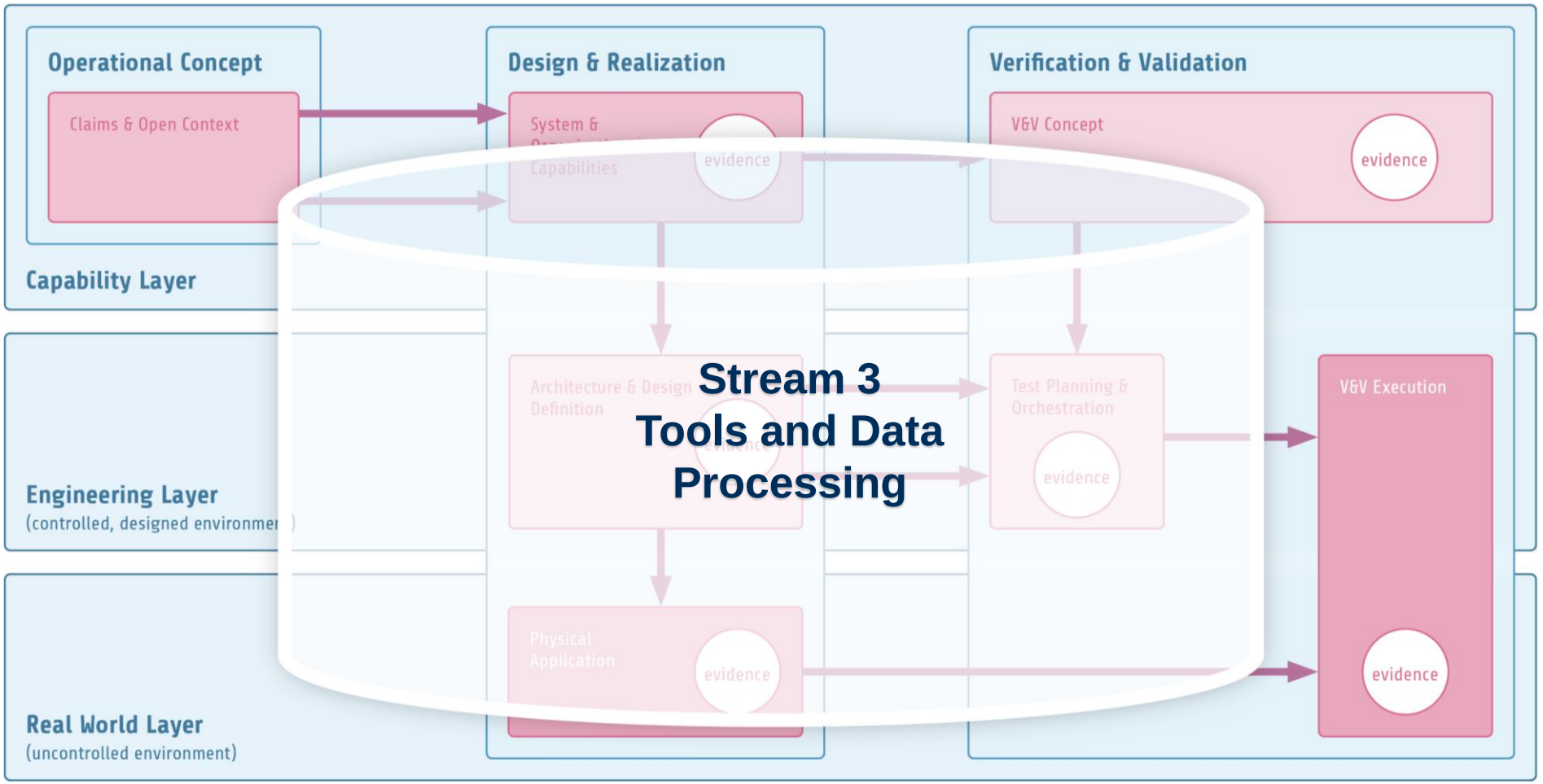
What‘s next?


Operational Concept
Claims & Open Context
Design & Realization
System & Organizational Capabilities
evidence
Verification & Validation
V&V Concept
evidence
Stream 1
Capability Layer
Architecture & Design Definition
evidence
Test Planning & Orchestration
evidence
V&V Execution
Engineering Layer
(controlled, designed environment)
Physical Application
evidence
evidence
Real World Layer
(uncontrolled environment)

What‘s next?


Operational Concept
Claims & Open Context
Capability Layer
Design & Realization
System & Organizational Capabilities
evidence
Architecture & Design Definition
evidence
Physical Application
evidence
Engineering Layer
(controlled, designed environment)
Real World Layer
(uncontrolled environment)
Verification & Validation
V&V Concept
evidence
Test Planning & Orchestration
evidence
V&V Execution
evidence
Stream 2

What‘s next?


Operational Concept
Claims & Open Context
Design & Realization
System &
Capabilities
evidence
Verification & Validation
V&V Concept
evidence
Capability Layer
Architecture & Design
Definition
Test Planning &
Orchestration
evidence
V&V Execution
Engineering Layer
(controlled, designed environmen
Physical
Application
evidence
evidence
Real World Layer
(uncontrolled environment)
Stream 3
Tools and Data
Processing

Summary

- VVM Assurance framework yields **structure for…**
  - tackeling the complexity of an ADS assurance argument by separation of (stakeholder) concerns
  - a systematic an traceable decomposition of the claim „absence of unreasonable risk“
  - systematically linking requirement definition to V&V efforts

- However:
  - VVM Assurance Framework is **no assurance argumentation** (in progress: second half of VVM)
  - We cannot build a convincing argument without **methods and tools** that generate the required evidences
    - Methodological approach: Next talk (Helmut Schittenhelm)
    - Tools: Stream 3

VERIFICATION
VALIDATION
METHODS

Thank you!

Jan Reich, *Fraunhofer IESE*

jan.reich@iese.fraunhofer.de +49 (0)631 / 6800 2254

https://www.researchgate.net/profile/Jan-Reich-2/

https://www.linkedin.com/in/jan-reich/

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