With funding from the:

Federal Ministry of Research, Technology and Space

ConnRAD – Connectivity and Resilience for Automated Driving

ConnRAD
Connectivity & Resilience for automated Driving Functions in Germany

Final Presentation **23.10.2025**

Resilience-by-Design: Approach for the design of resilient systems

Isaac Mpidi Bita – Fraunhofer IEM

Definition of concept

Systems Resilience

The ability of an automotive system or mobility system to ensure availability and reliability under disruptions by detecting disruptions, adapting dynamically and returning to a functional state after a disruption.

Resilience-by-Design

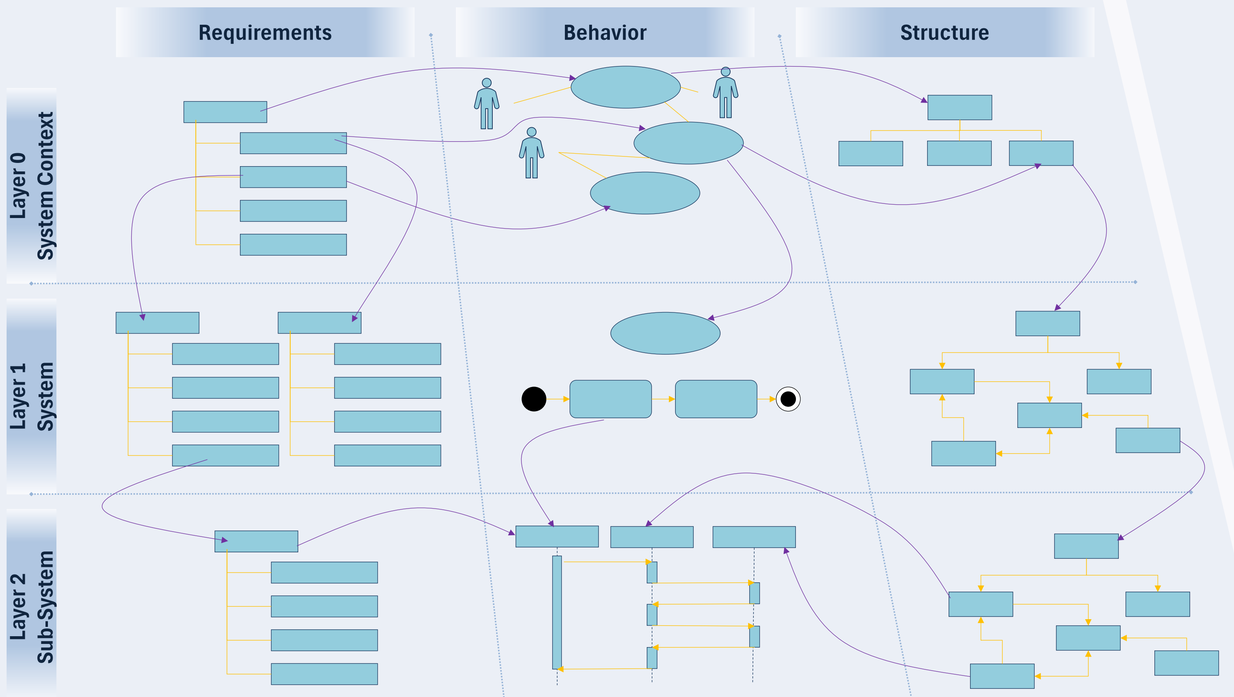
A methodical approach in which resilience is already anchored in the system architecture and the development process. This is achieved by integrating mechanisms such as fault detection, recovery strategies, redundancy and trust mechanisms in the early concept phase

Resilience-in-Operation

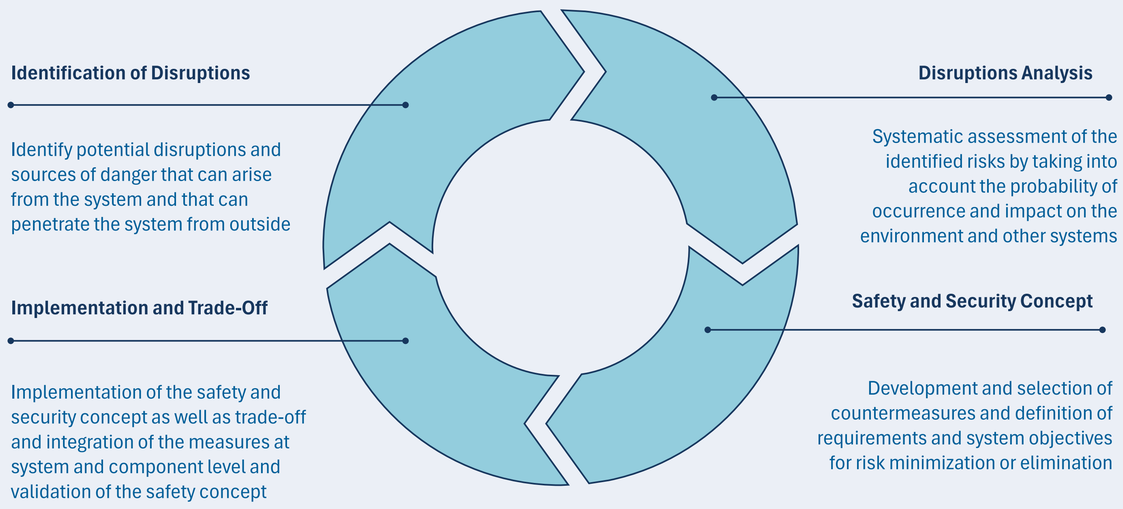
Maintaining continuous and reliable system function during operation under uncertain conditions by applying strategies defined in the resilience-by-design and enabling real-time detection and adaptation and, if necessary, learning to ensure availability and reliability over the entire operating time

General process model

Systems Design



System analysis



Localization of the methods and tools used and developed in the project

(1) Creation of the reference architecture

Create a common understanding of the system across the three different, use case-specific architectures

(2) Resilience Maturity Model

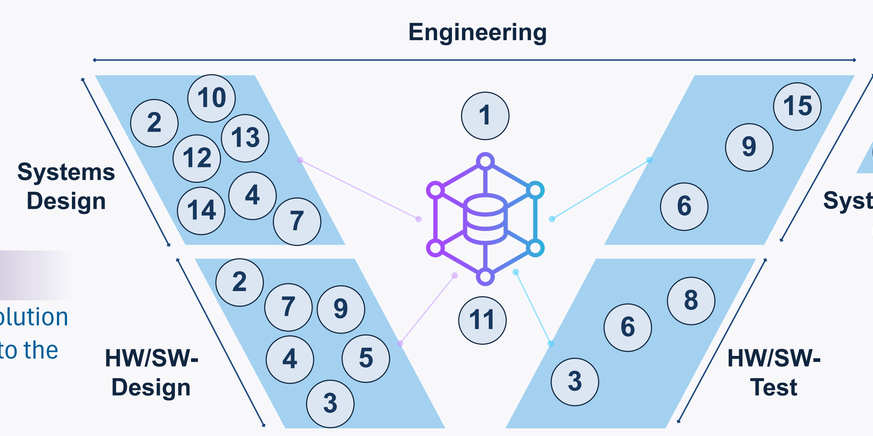
for the evaluation of the resilience maturity level of system architectures and development processes along defined stages

(3) Plausibility Check & Extention of CAM/DENM

Adds redundant data to CAM and DENM messages so that receivers can check their consistency and create more confidence and trust in the messages

(4) Resilience Design Pattern

Were used to systematically integrate proven solution modules for typical resilience requirements into the architecture in a reusable manner



(10) Minimal Resilience Factor (MRF)

The MRF lets system partners add security information to exchanged data, enabling recipients to accept or reject it based on their security requirements.

(9) Quality of Service

Ensures that the necessary bandwidth and very low latency are reliably available during teleoperation

(8) Trust opinion calculation

Concurrent, event-driven framework that processes events from V2X messages and trust sources to create trust scores

(5) Kafka communication

is a distributed streaming platform that enables asynchronous, event-driven communication between independent components

(6) Resilience KPIs

For the quantifiable evaluation of the resilience properties of technical systems in order to identify vulnerabilities and support targeted improvement measures based on data

(7) Trust model design

Graph-based model based on a system model that depicts the relevant components and data flows for a function

Other methods used:

- (11) Creation of a single source of truth
- (12) TARA according to ISO 21434
- (13) HARA according to ISO 21448 & 26262
- (14) System-Theoretic Process Analysis (STPA)
- (15) Trust Assessment Framework

Legend:

- Methods
- Methods aids

Conclusion:

Holistic integration of resilience into the development process

The process model shows how resilience can be integrated holistically into the development process through a combination of methods, tools and standards-based approaches.

Linking resilience-by-design and resilience-in-operation

From the systematic analysis of disruptions (TARA, HARA, STPA) and model-based architecture development to plausibility checks and trust mechanisms, both preventive measures in the resilience-by-design phase and operational approaches for resilience in operation are taken into account.

Methodological basis for the approval of distributed driving functions

For the approval of distributed driving functions, we use proven and established methods which, in combination with Model-Based Systems Engineering (MBSE), ensure improved documentation, end-to-end traceability and increased consistency.