VERIFICATION
VALIDATION
METHODS

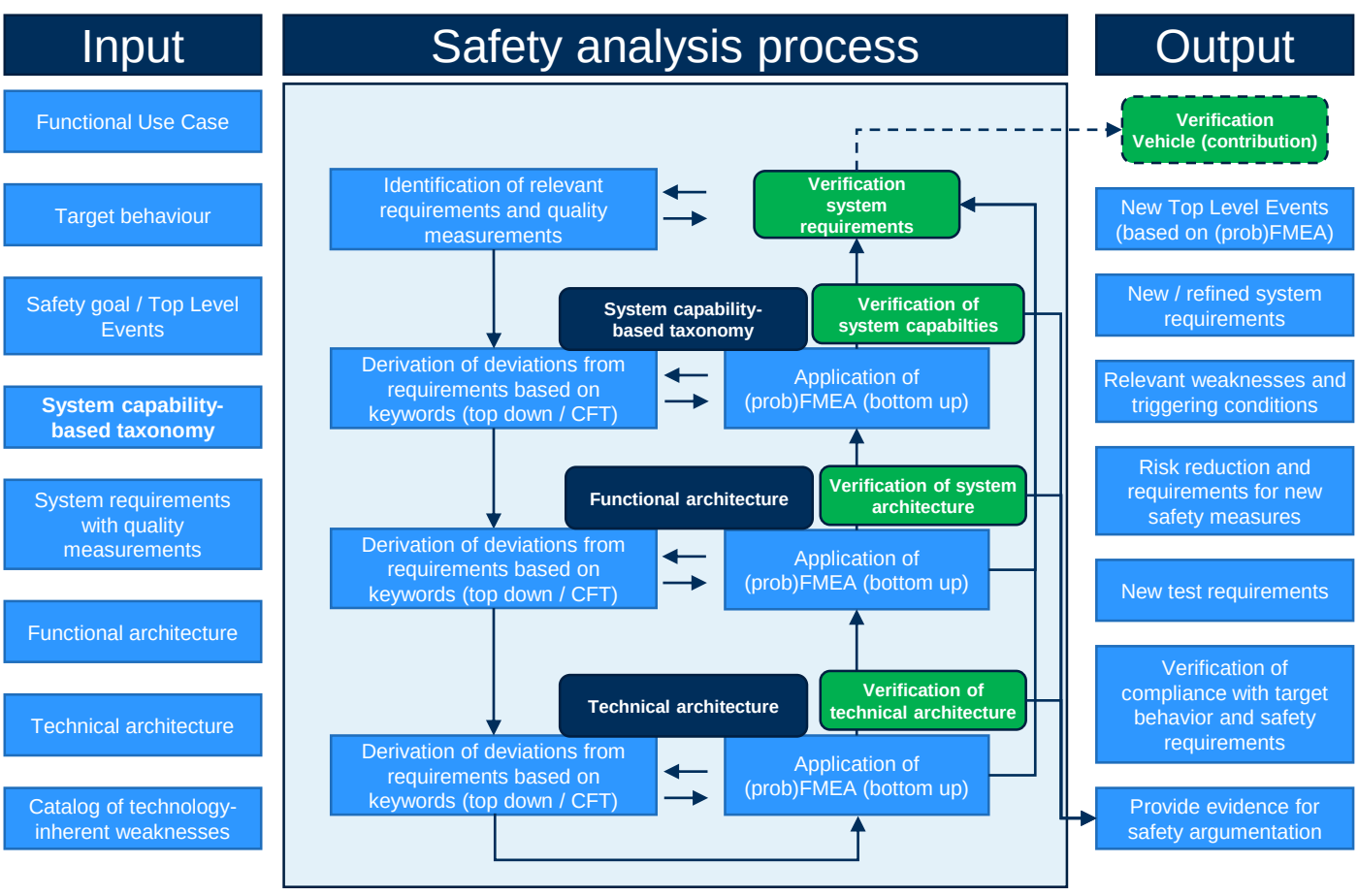
PROJECT of the PEGASUS FAMILY

# A SAFETY ANALYSIS METHOD REGARDING (IN)CAPABILITIES, WEAKNESSES AND COMPONENT FAILURES

## Methodical approach for safety analysis in the context of use cases by a combined Top-Down and Bottom-up analysis approach

Tobias Braun, Matthias Rauschenbach, Christian Wolschke, Fraunhofer LBF Darmstadt; Jan Reich, Simon Kupjetz, Fraunhofer IESE Kaiserslautern

The presented approach combines a Top-Down analysis approach based on component fault trees (CFT) with the bottom-up technique probFMEA allowing systematic safety analysis considering classical functional safety and SOTIF (Safety Of The Intended Functionality) aspects on different abstraction levels supporting the whole development cycle.




Safety analysis enables a direct link and traceability to the elements of the system architecture

- Applicable on different abstraction levels: system capability-based taxonomy, functional and technical architecture
- Derivation and refinement of safety requirements and identification of top level events

SafeTbox: Extension for Enterprise Architect supporting the modelling of the architecture, safety analysis, GQM and safety case description (using the Structured Assurance Case Metamodel - SACM)

- support for functional safety and SOTIF, connectors for safety analysis (Cut-Sets and Bayesian networks)
- supports tracing between different models and their elements
- usage of analysis results as a contribution of evidence to safety case

**Contact**
**Tobias.Braun@iese.fraunhofer.de**
**Matthias.Rauschenbach@lbf.fraunhofer.de**

www.vvm-projekt.de Twitter @vvm-project LinkedIn VVM Project

Projektpartner

**A project developed by the VDA Leitinitiative autonomous and connected driving**

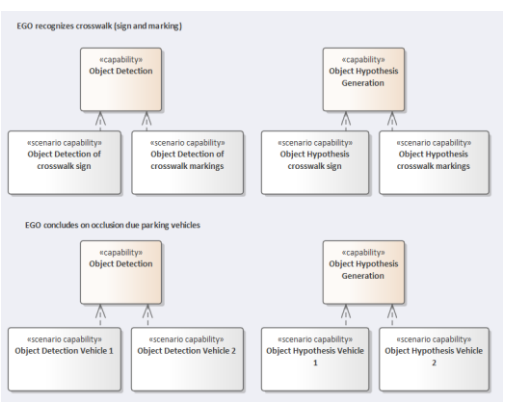
Supported by:
Federal Ministry for Economic Affairs and Climate Action
on the basis of a decision by the German Bundestag

VERIFICATION
VALIDATION
METHODS

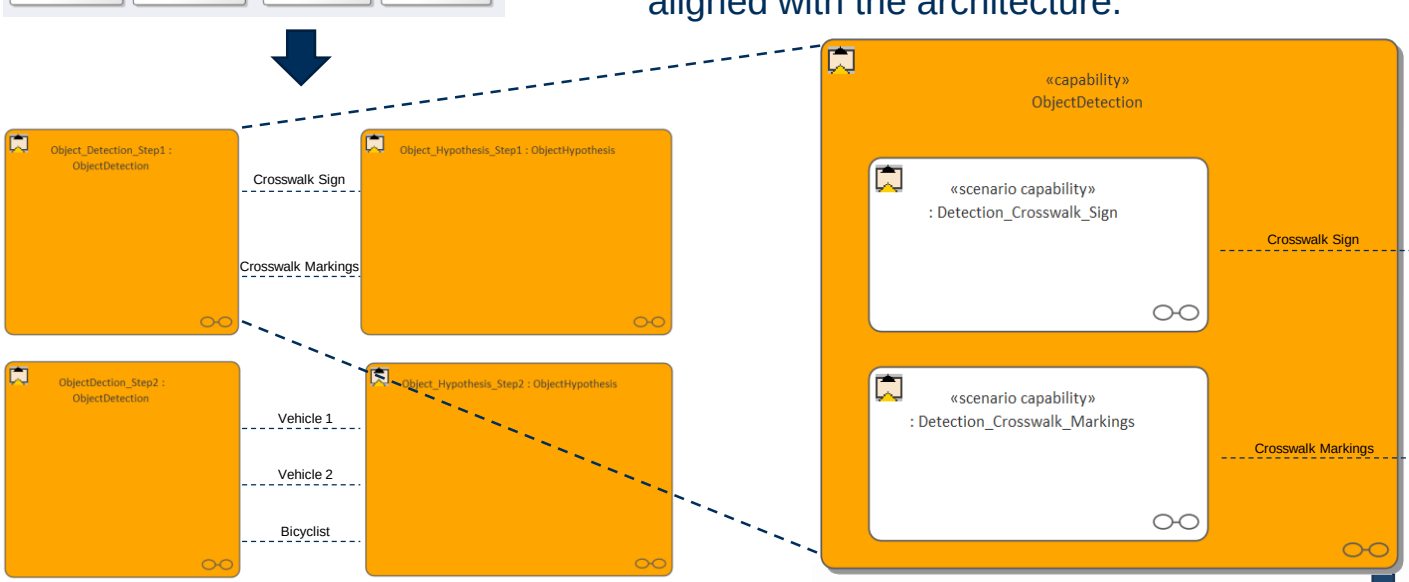
PROJECT of the PEGASUS FAMILY

Starting point of the presented methodology is the system architecture on the addressed complexity level (capability, logical or technical). The Phenomenon-Signal-Model (PSM) is used as basis for identification of the functional use case and the required capabilities as well as criticality phenomena.

## Step 1: Analysing of system capability-based taxonomy for the concrete functional use case




- System capability-based taxonomy as main prerequisite provides system capabilities and analyses the active capabilities functions for the use case based on the PSM.
- Dependencies between the capabilities are modelled as ports. This structure is used as input for the modelling of failure propagation aligned with the architecture.



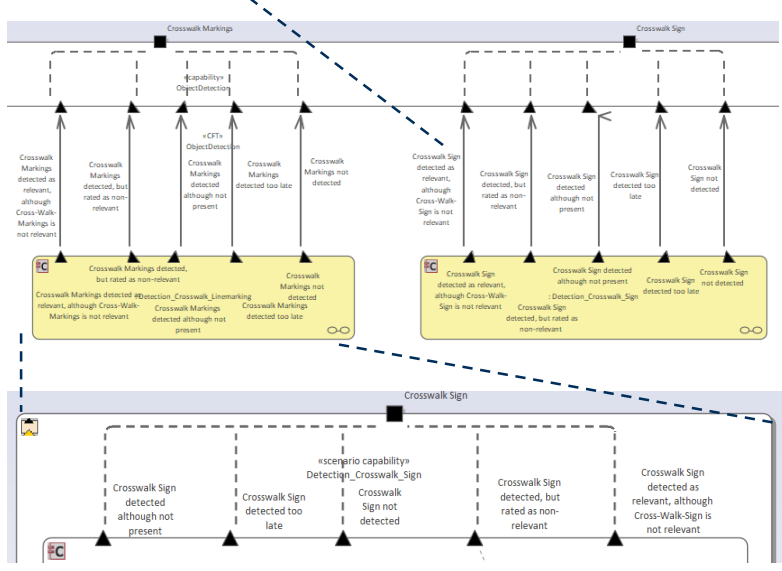

## Step 2: Modelling of failure propagation based on the dependencies

Analysis starts with a top level element (TLE) such as the violation of a safety goal or safety requirement formulated for one specific use case

- Causes for the violations are tracked down using the modelled dependencies to the atomic element of the analysed abstraction level.
- Application of keywords at the level of dependencies to enable systematic identification of failure causes. An identified failure not leading to the TLE can be analysed to identify missing TLEs.

Generic Failure Type System Specification

| Name | Description |
|---|---|
| NONE | Indicates that no failure types is defined |
| No | Service or Signal is not delivered |
| Less | Service or Signal provides a lower value than expected |
| More | Service or Signal provides a higher value than expected |
| Too early | Service or Signal is delivered earlier than expected |
| Too late | Service or Signal is delivered later than expected |
| Non existent | Elemente refered to does not exist |
| Too large | Service or Signal provides too large values resp results |
| Too small | Service or Signal provides too small values resp results |
| Too many | Service or classification returns too many elements |
| Too few | Service or classification returns too few elements |
| Not relevant | Elemente refered to is not relevant |
| Falsely relevant | Elemente refered to is classified falsely as relevant |




www.vvm-projekt.de Twitter @vvm-project LinkedIn VVM Project

Projektpartner

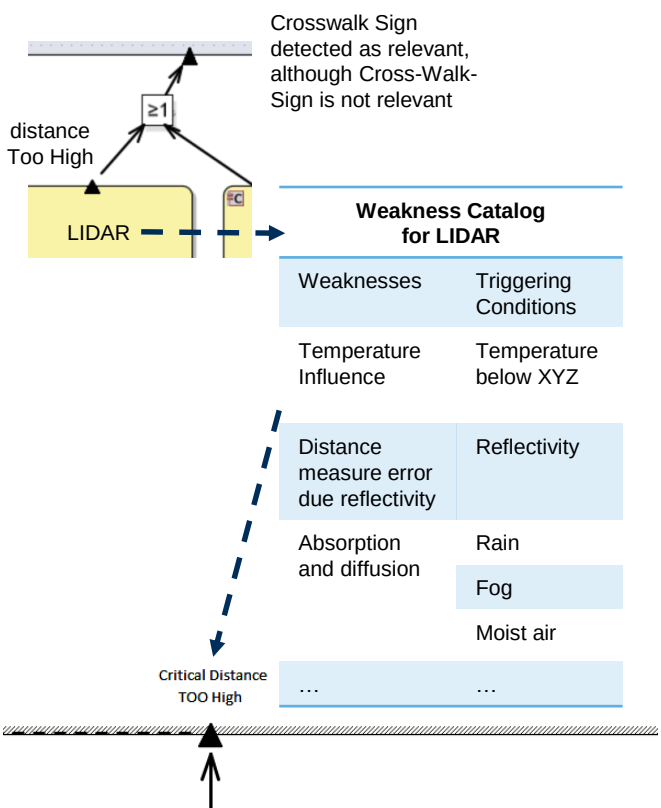
A project developed by the VDA Leitinitiative autonomous and connected driving

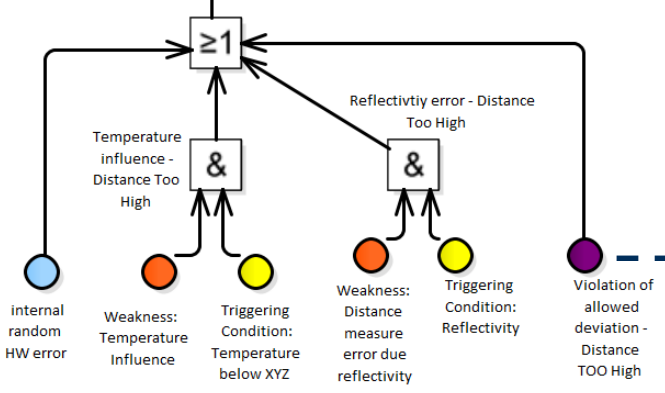
Supported by:
Federal Ministry for Economic Affairs and Climate Action
on the basis of a decision by the German Bundestag

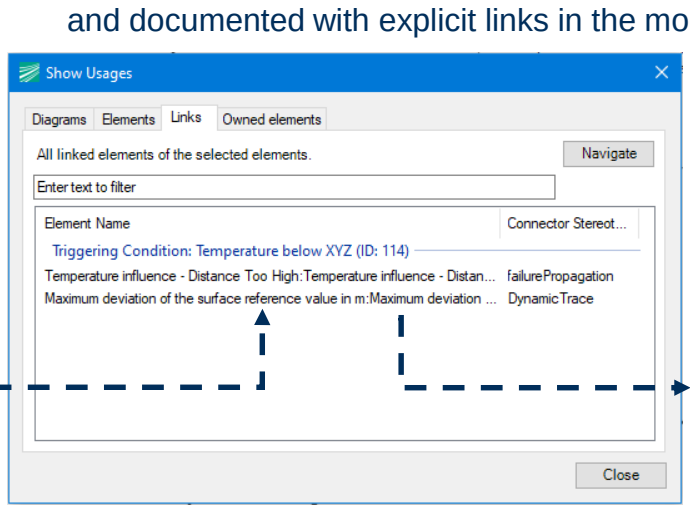
VERIFICATION
VALIDATION
METHODS

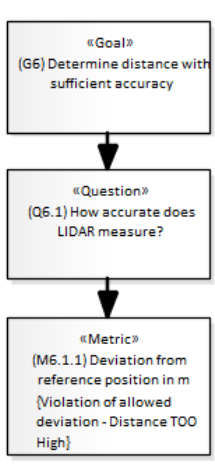
PROJECT of the PEGASUS FAMILY

## Step 3: Modelling failure causes with regard to functional safety and SOTIF aspects considering quality measurements and metrics



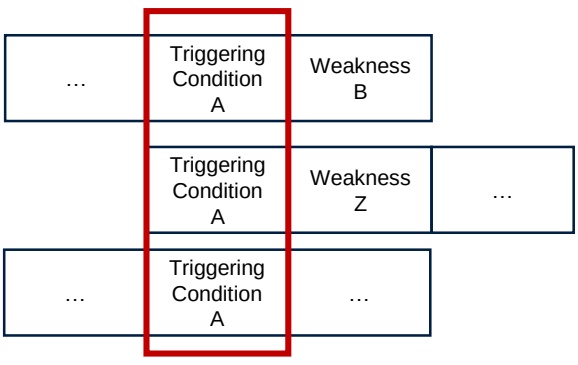




- Influence of used technologies to specific use case is modelled
- Failure mode on ports can be further refined using well-known modelling elements of Fault-Trees
- The concept of classic basic events has been extended to express SOTIF aspects such as triggering conditions and weaknesses. Support for sensor specific catalogues with weaknesses and triggering conditions within the tool is intended.
- Violations of quality measurements derived with Goal Question Metric (GQM) can also be modelled in the shown tool environment. The traceability to the derived quality measurements can be expressed and documented with explicit links in the model.

## Step 4: Analyse developed failure propagation model to identify issues, derive countermeasures and provide evidences for the safety argumentation

Minimal cut-set (MCS) as output of the Fault Tree Analysis (FTA) can be used to identify critical combination of events and conditions causing a violation of the safety goal or safety requirements under investigation as TLE

- Triggering Conditions which are part of multiple MCS indicate a critical environment condition which requires special attention also regarding testing
- MCS consisting of single Weakness and Triggering Condition combination corresponds to Single Point Faults in the classical functional safety and must be handled
- Approach allows to analyse impacts of classical functional safety topics as well as SOTIF aspects and to derive safety measures. These measures can be functional and technical measures but also adaptions on the behaviour of the vehicle and capability level.
- CFTs can automatically be translated into Bayesian Networks (BN). These BNs can be used for extended quantitative analyses




Qualitative and quantitative analysis results from probFMEA, FTA and BN are evidences supporting the safety argumentation (e.g. documenting the robustness of a system with MCS order or the probability of safety goal /safety requirement violation from BN analysis).

www.vvm-projekt.de Twitter @vvm-project LinkedIn VVM Project

Projektpartner


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