PROJECT of the PEGASUS FAMILY

VERIFICATION VALIDATION METHODS

Final Event 21 / 22 November 2023

This is how VVM argues safety and links to R&D processes

Thomas Kirschbaum, Robert Bosch GmbH

Supported by:

Federal Ministry for Economic Affairs and Climate Action

on the basis of a decision by the German Bundestag

How VVM handles Risk and links to Development Processes
What you will experience

- Central **Role of the Risk Management Core**
- **Process Integration** of the Risk Management Core **and Application example**
- Interface to **Safety Argumentation**

VERIFICATION
VALIDATION
METHODS

Central Role of the Risk Management Core

Risk Management Core
Central Role

- Risk Management Core: **Process Framework** - assessing **Risks explicitly** in an **iterative Control Loop**
- Risk Management Core **works as a central collector** for

- **Hazards** → Hazard Log
- **Risks**
- **Safety Goals**

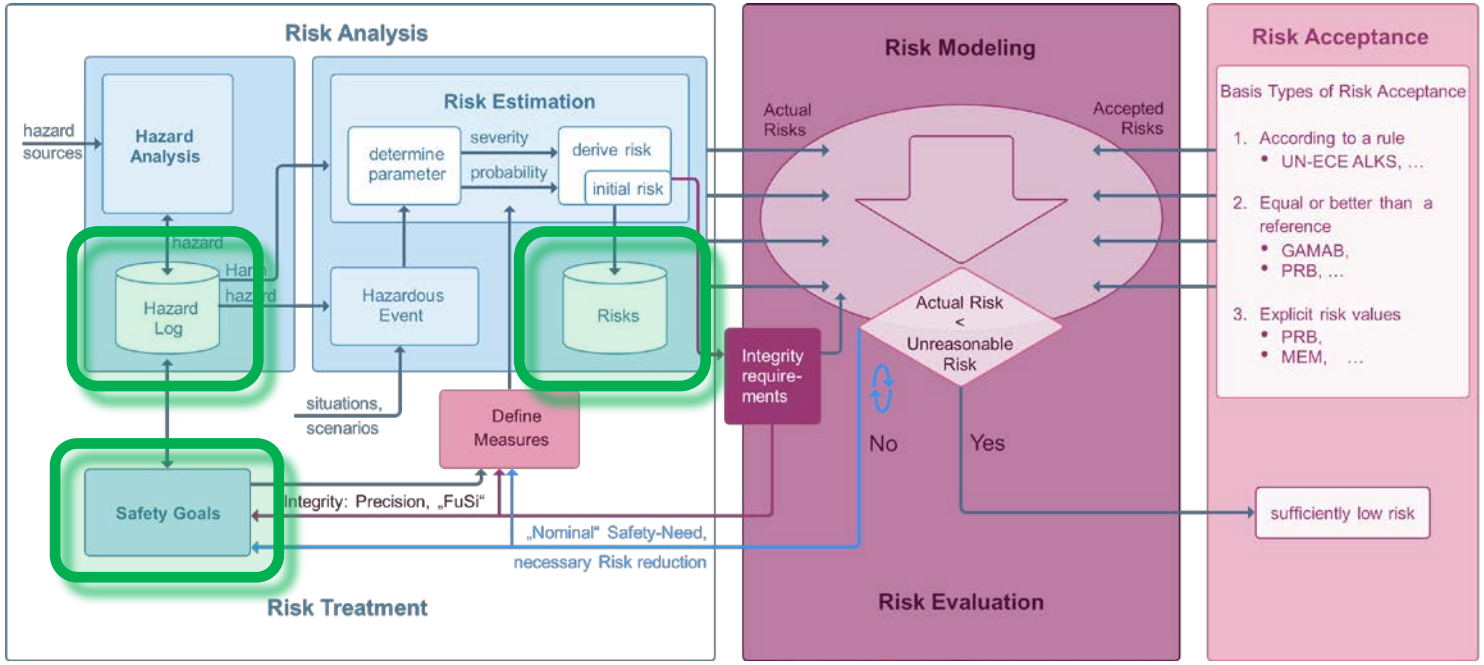


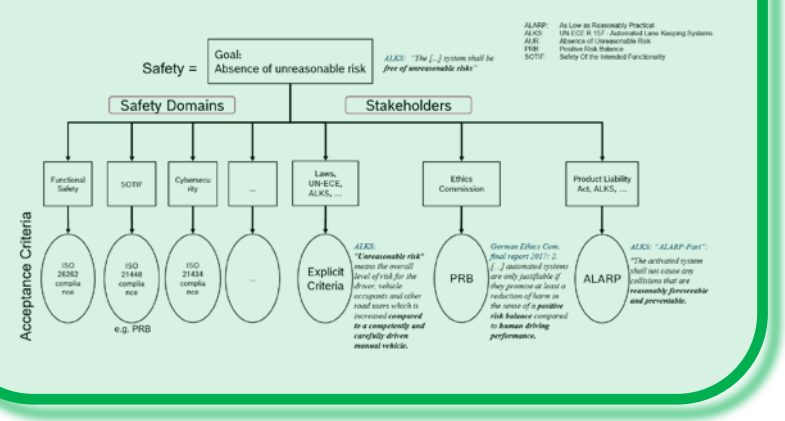
Figure 1: Risk Management Core

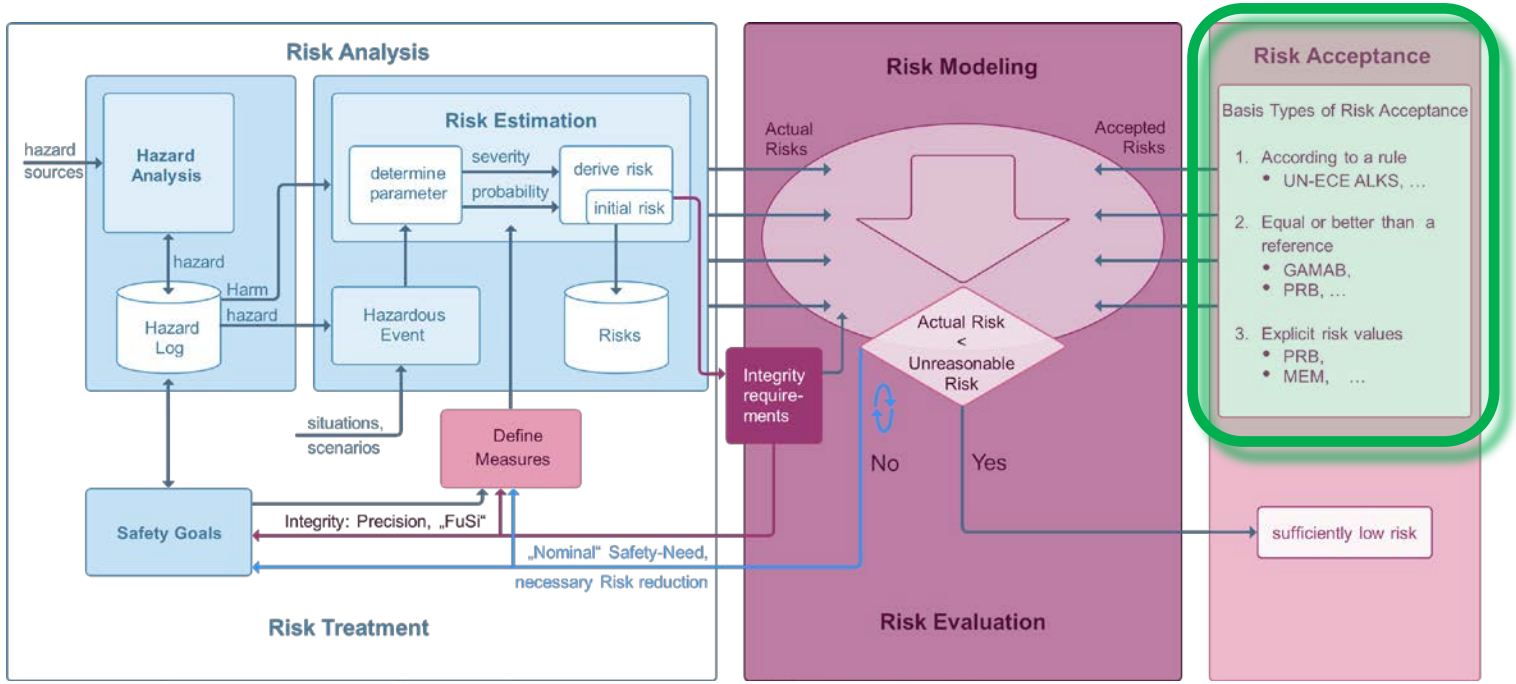
The Risk Management Core collects all Hazards and manages Risk from all Sources

Risk Management Core
Central Role

- Risk Management Core: **Process Framework** - assessing **Risks explicitly** in an **iterative Control Loop**
- Risk Management Core **works as a central collector** for

Risk Acceptance Criteria



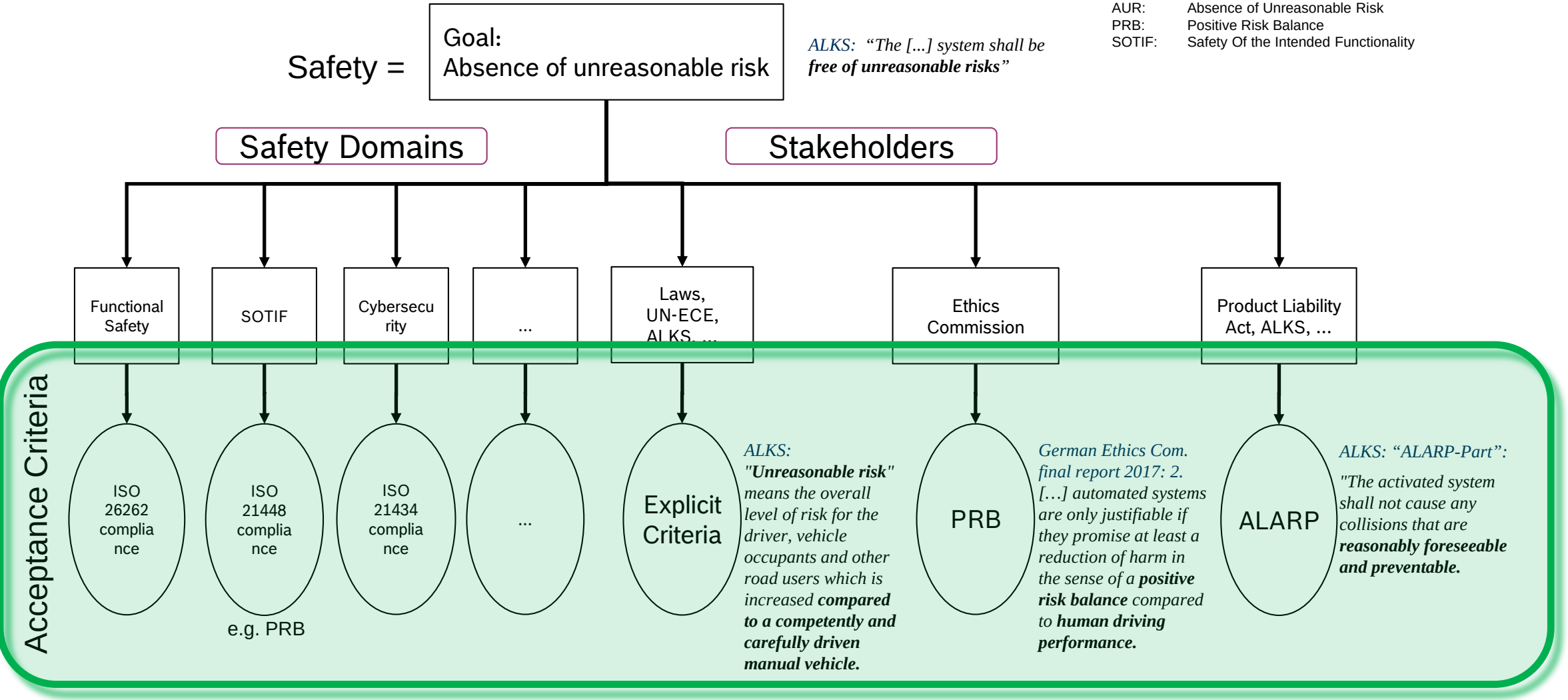


Risk Management Core

The Risk Management Core collects Risk Acceptance Criteria

Safety: one goal multiple risk criteria

ALARP: As Low as Reasonably Practical
ALKS: UN-ECE R 157 - Automated Lane Keeping Systems
AUR: Absence of Unreasonable Risk
PRB: Positive Risk Balance
SOTIF: Safety Of the Intended Functionality

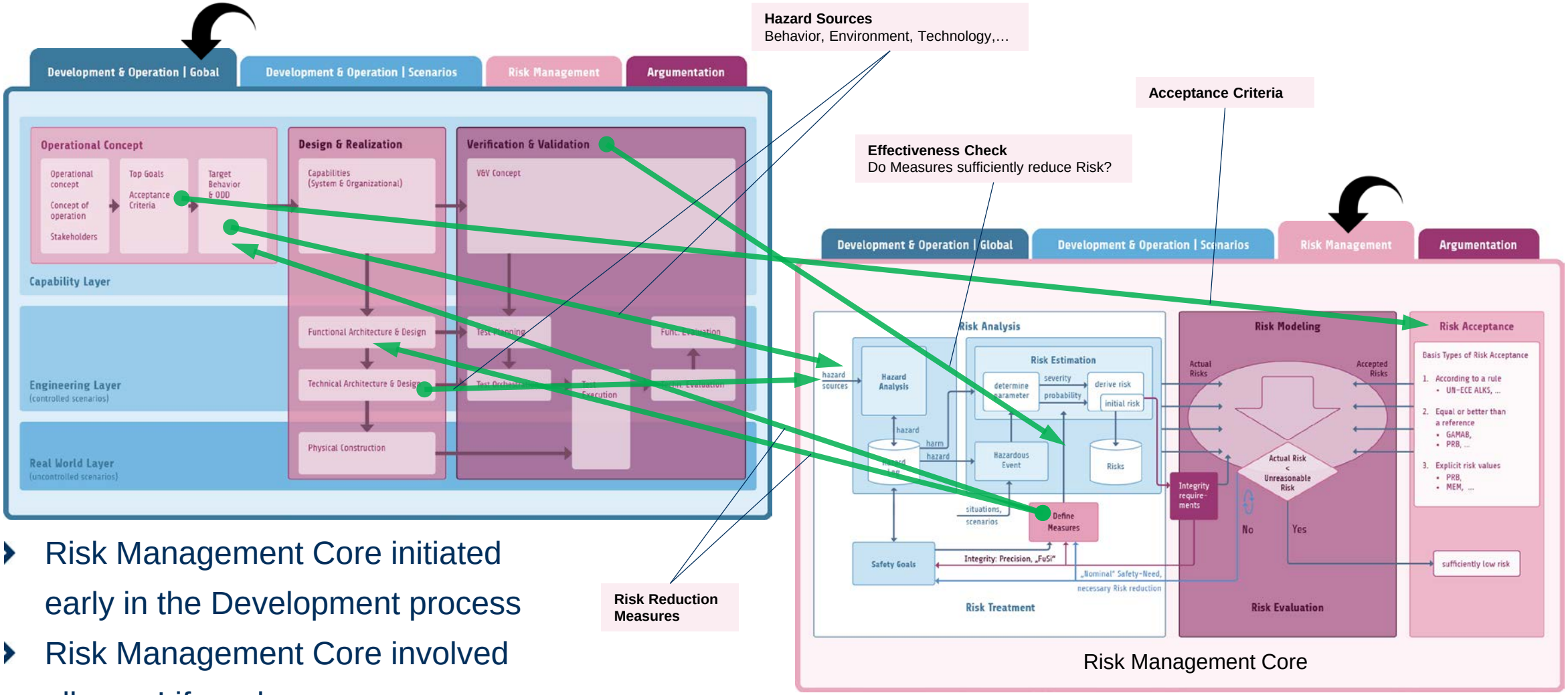


There are different parallel Sources for Risk Acceptance Criteria

VERIFICATION
VALIDATION
METHODS

Process Integration of the Risk Management Core and Application example

Risk Management Core
Link to Development Process | Global



Risk Management Core

- Risk Management Core initiated early in the Development process
- Risk Management Core involved all over Lifecycle

Application example of the Risk Management Core

Creation of a Safe Target Behavior

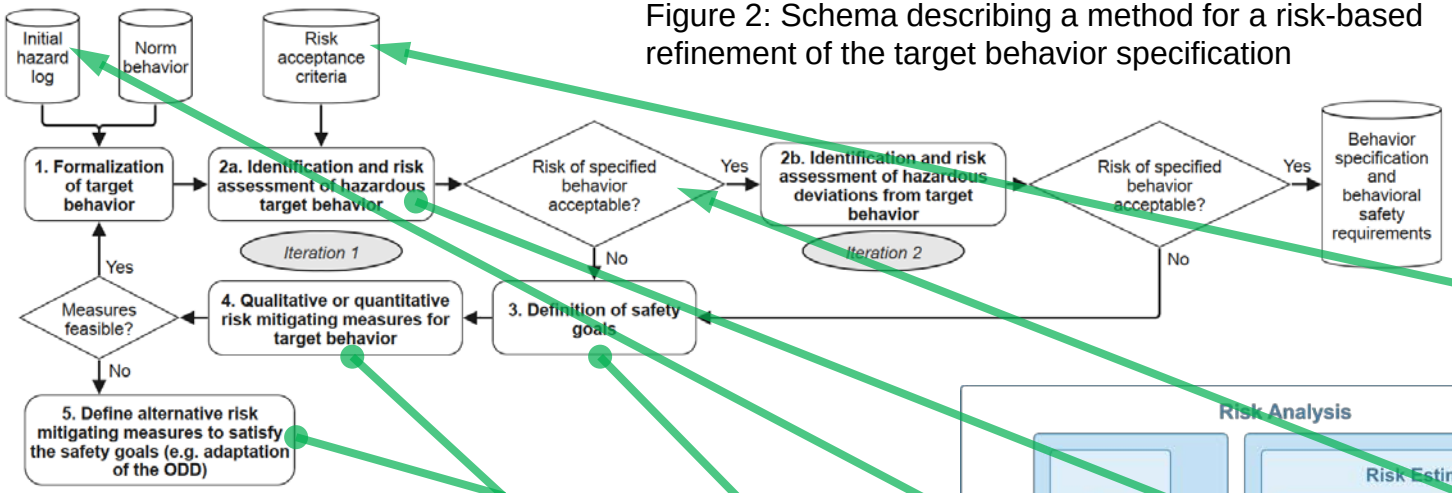


Figure 2: Schema describing a method for a risk-based refinement of the target behavior specification

#3.7 #10.4

Details on Posters

Creation of a **Safe Target Behavior**
by applying the **Risk Management Core**

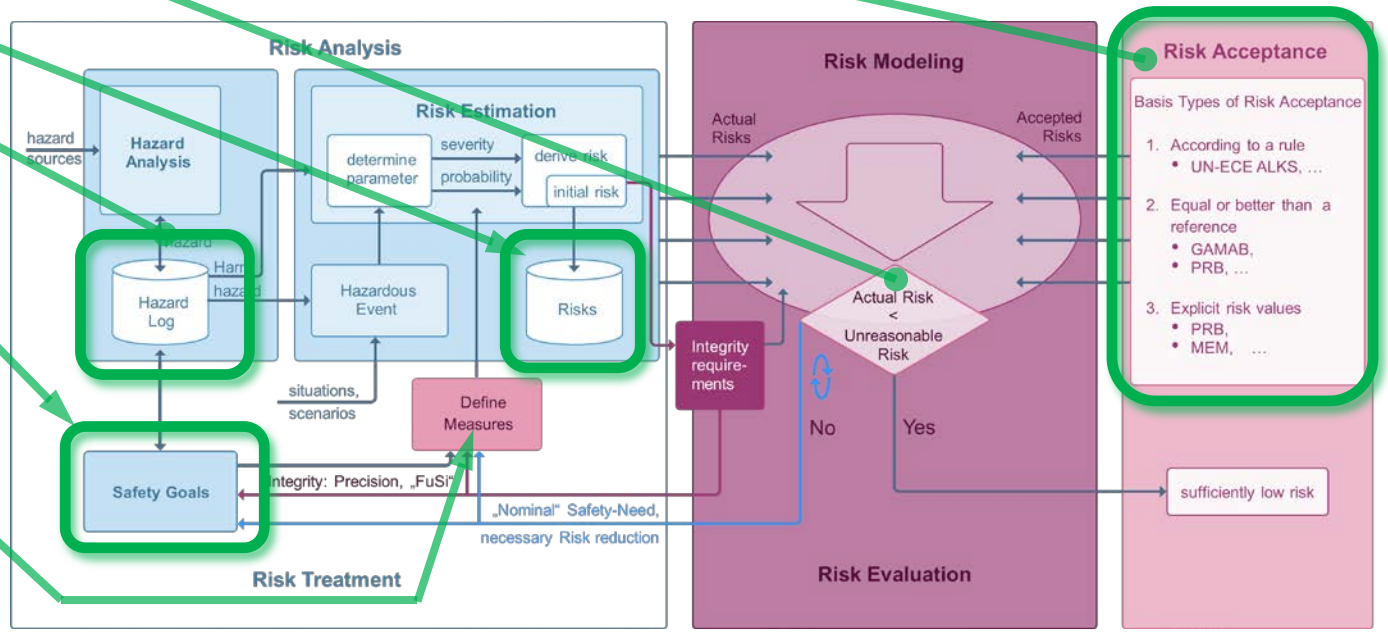
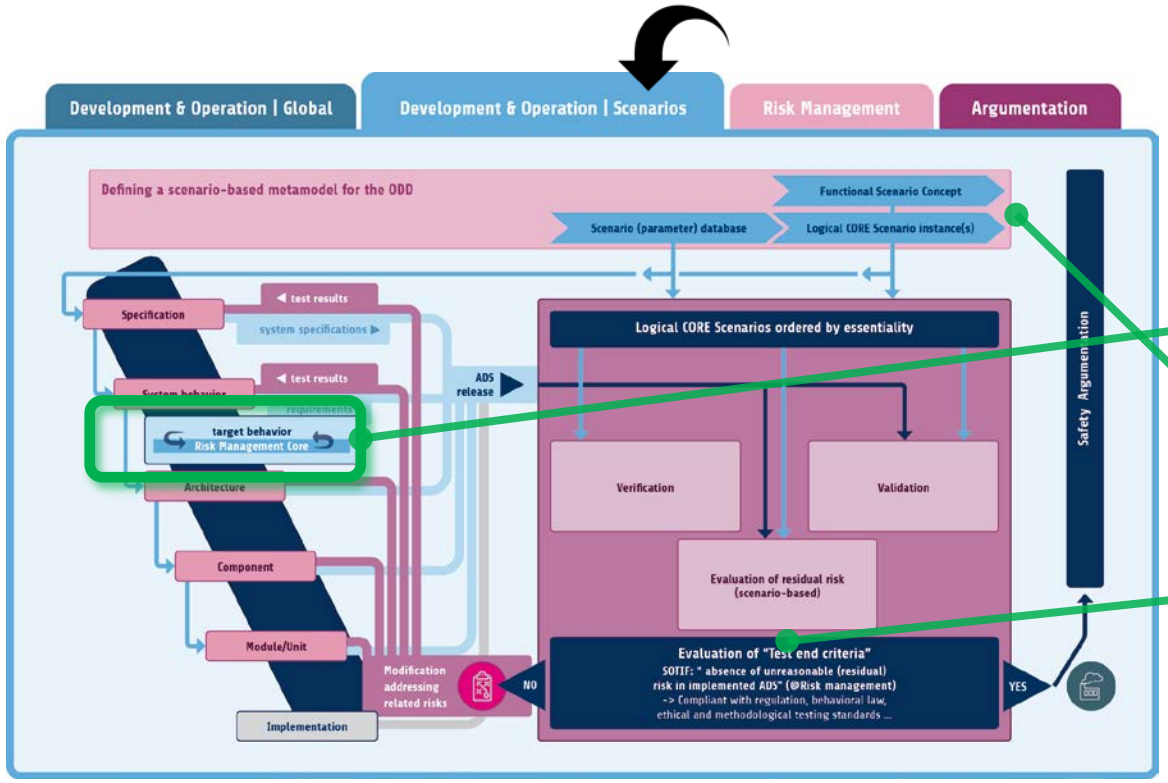
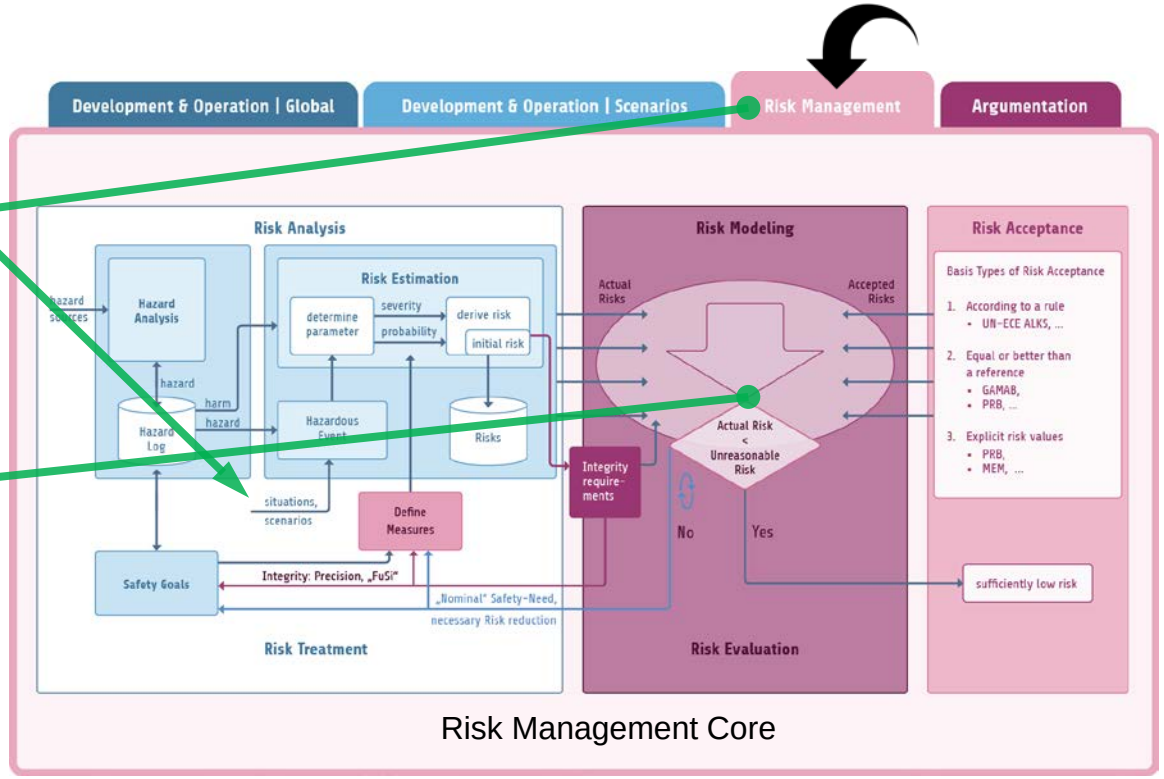


Figure 3: Risk Management Core

Risk Management Core (RMC)

Link to Development Process | Scenarios





Risk Management Core

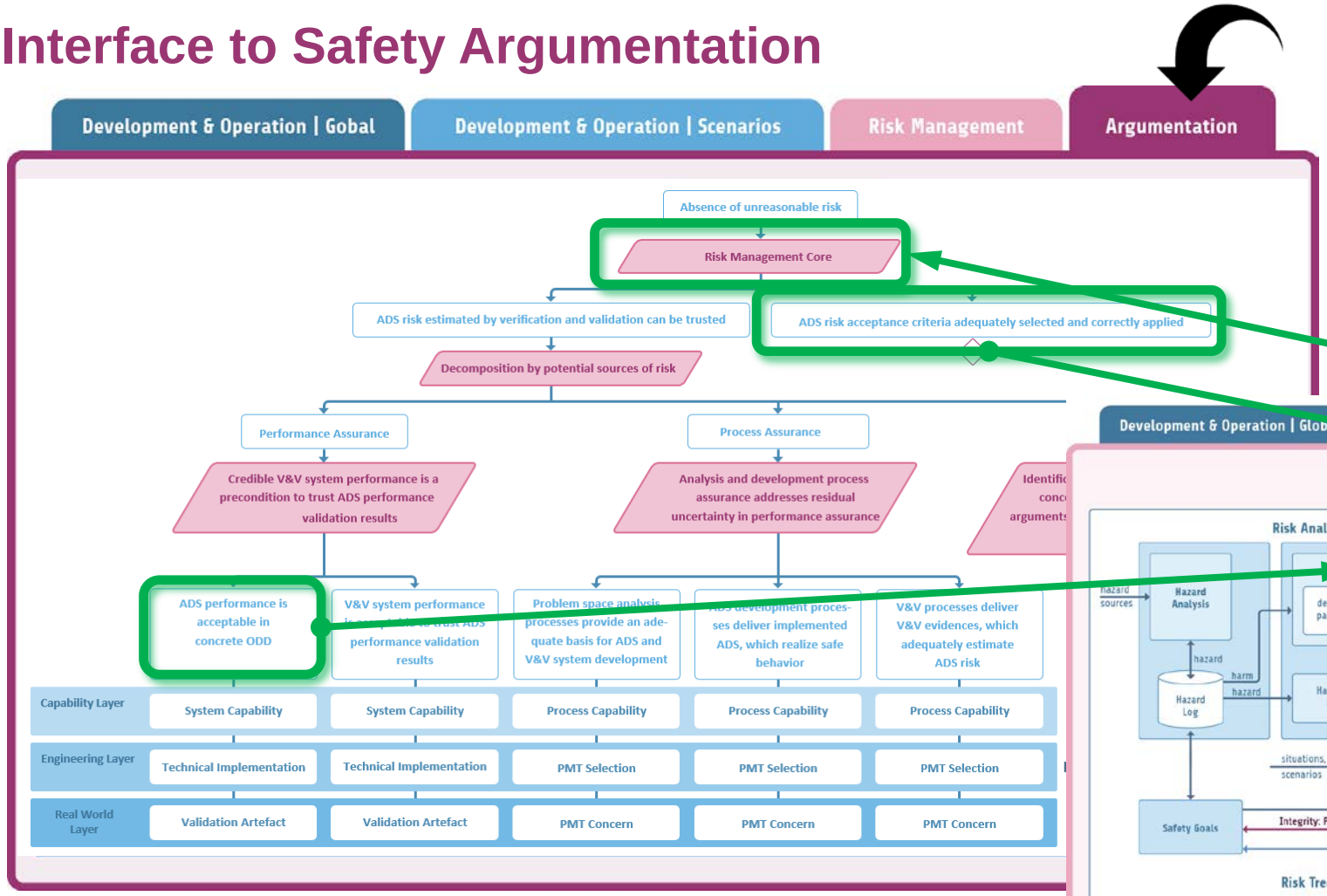
- **Scenarios are an essential input** for the RMC
- RMC **interacts** with the Process **in multiple Places**

VERIFICATION
VALIDATION
METHODS

Interface to Safety Argumentation

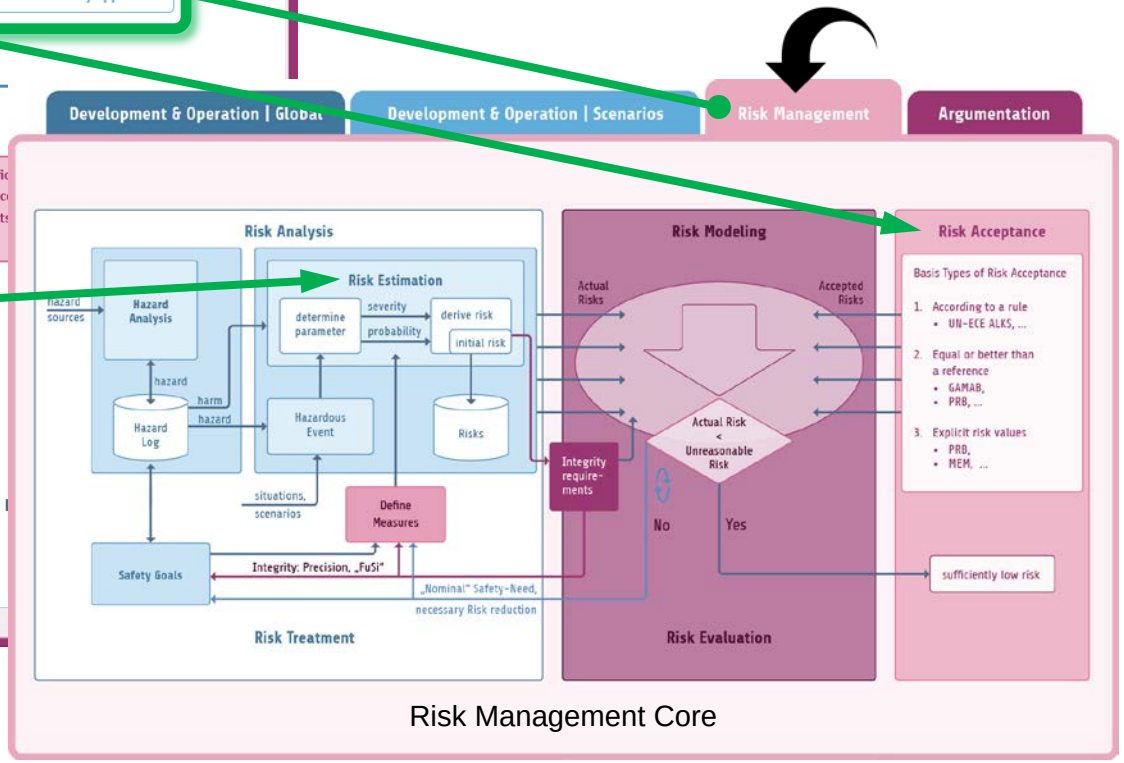
Risk Management Core (RMC)

Interface to Safety Argumentation



Details on Poster

#3.8



Risk Management Core

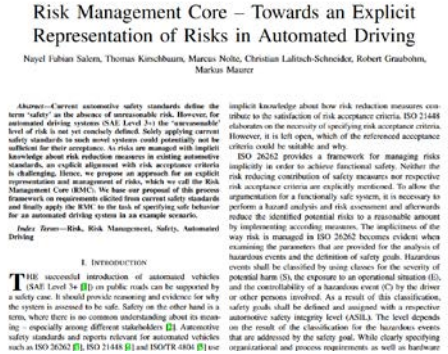
- Safety Argumentation includes the Risk Management Core
- RMC provides data for Safety Argumentation

Transition

Interested in the topic?

- **Details on Posters**
  - Poster #3.7 – The Risk Management Core
  - Poster #3.8 – The VVM Safety Argumentation Structure
  - Poster #10.4 – Behavioral Safety Concept

- **Read the Pre-Print**
  - Risk Management Core – Towards an Explicit Representation of Risks in Automated Driving



Risk Management Core – Towards an Explicit Representation of Risks in Automated Driving

Nayel Fabian Salem, Thomas Kirschbaum, Marcus Nolte, Christian Lalitsch-Schneider, Robert Graubohm, Markus Maurer

Abstract—Current automotive safety standards define the term "safety" as the absence of unreasonable risk. However, for automated driving systems (SAE Level 3+) the "unreasonable" level of risk is not yet concisely defined. Solely applying current safety standards to such novel systems could potentially not be sufficient for their acceptance. As risks are managed with implicit knowledge about risk reduction measures in existing automotive standards, an explicit alignment with risk acceptance criteria is challenging. Hence, we propose an approach for an explicit representation and management of risks, which we call the Risk Management Core (RMC). We base our proposal of this process framework on requirements elicited from current safety standards and finally apply the RMC to the task of specifying safe behavior for an automated driving system in an example scenario.

Index Terms—Risk, Risk Management, Safety, Automated Driving

I. Introduction

THE successful introduction of automated vehicles (SAE Level 3+ [1]) on public roads can be supported by a safety case. It should provide reasoning and evidence for why the system is assessed to be safe. Safety on the other hand is a term, where there is no common understanding about its meaning – especially among different stakeholders [2]. Automotive safety standards and reports relevant for automated vehicles such as ISO 26262 [3], ISO 21448 [4] and ISO/TR 4804 [5] use implicit knowledge about how risk reduction measures contribute to the satisfaction of risk acceptance criteria. ISO 21448 elaborates on the necessity of specifying risk acceptance criteria. However, it is left open, which of the referenced acceptance criteria could be suitable and why.

ISO 26262 provides a framework for managing risks implicitly in order to achieve functional safety. Neither the risk reducing contribution of safety measures nor respective risk acceptance criteria are explicitly mentioned. To allow the argumentation for a functionally safe system, it is necessary to perform a hazard analysis and risk assessment and afterwards reduce the identified potential risks to a reasonable amount by implementing according measures. The implicitness of the way risk is managed in ISO 26262 becomes evident when examining the parameters that are provided for the analysis of hazardous events and the definition of safety goals. Hazardous events shall be classified by using classes for the severity of potential harm (S), the exposure to an operational situation (E), and the controllability of a hazardous event (C) by the driver or other persons involved. As a result of this classification, safety goals shall be defined and assigned with a respective automotive safety integrity level (ASIL). The level depends on the result of the classification for the hazardous events that are addressed by the safety goal. While clearly specifying organizational and process requirements as well as hardware

- Authors:

  Nayel Fabian Salem, Thomas Kirschbaum,
  Marcus Nolte, Christian Lalitsch-Schneider,
  Robert Graubohm, Markus Maurer, Jan Reich

VERIFICATION
VALIDATION
METHODS

Thank you!

Thomas Kirschbaum, Robert Bosch GmbH

Thomas.Kirschbaum@de.bosch.com

PROJECT of the PEGASUS FAMILY

VDA LEITINITIATIVE

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