

VERIFICATION
VALIDATION
METHODS

Final Event 21 / 22 November 2023

The Role of Risk for Safety Assurance in Development and Operation

Thomas Kirschbaum, Robert Bosch GmbH

Supported by:



on the basis of a decision
by the German Bundestag

The Role of Risk for Safety Assurance

What you will experience

1. Why do we use **Risk as Measure for Safety**?
2. What is the **Mechanism to achieve Safety**?
3. How did VVM assemble the **Method 'Risk Management Core'**?
4. See the **Advantages of the Method 'Risk Management Core'**

Why do we use Risk as Measure for Safety?

Hazard, Harm, Safety, Risk

Why do we use Risk as Measure for Safety?

Primary control point:
Eliminate the causes

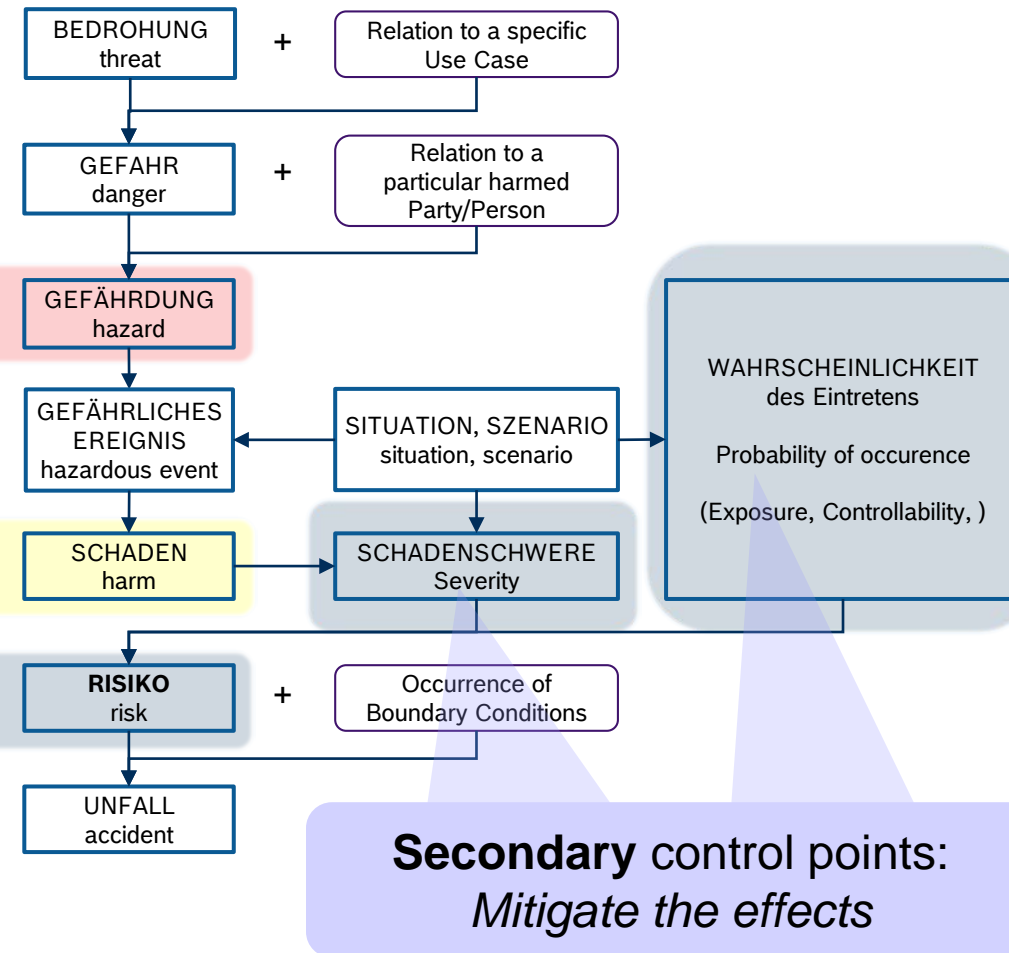
2. Hazard: source of harm

1. No Harm at no time = Absolute Safety (*not realistic*)

3. Risk: $f(\text{Severity, Probability}) = \text{Measure for Safety}$

- Advantage I : Can represent small increments of harm
- Advantage II: measurable level of safety
- Advantage III: Enables threshold definition:




Safety := absence of unreasonable risk

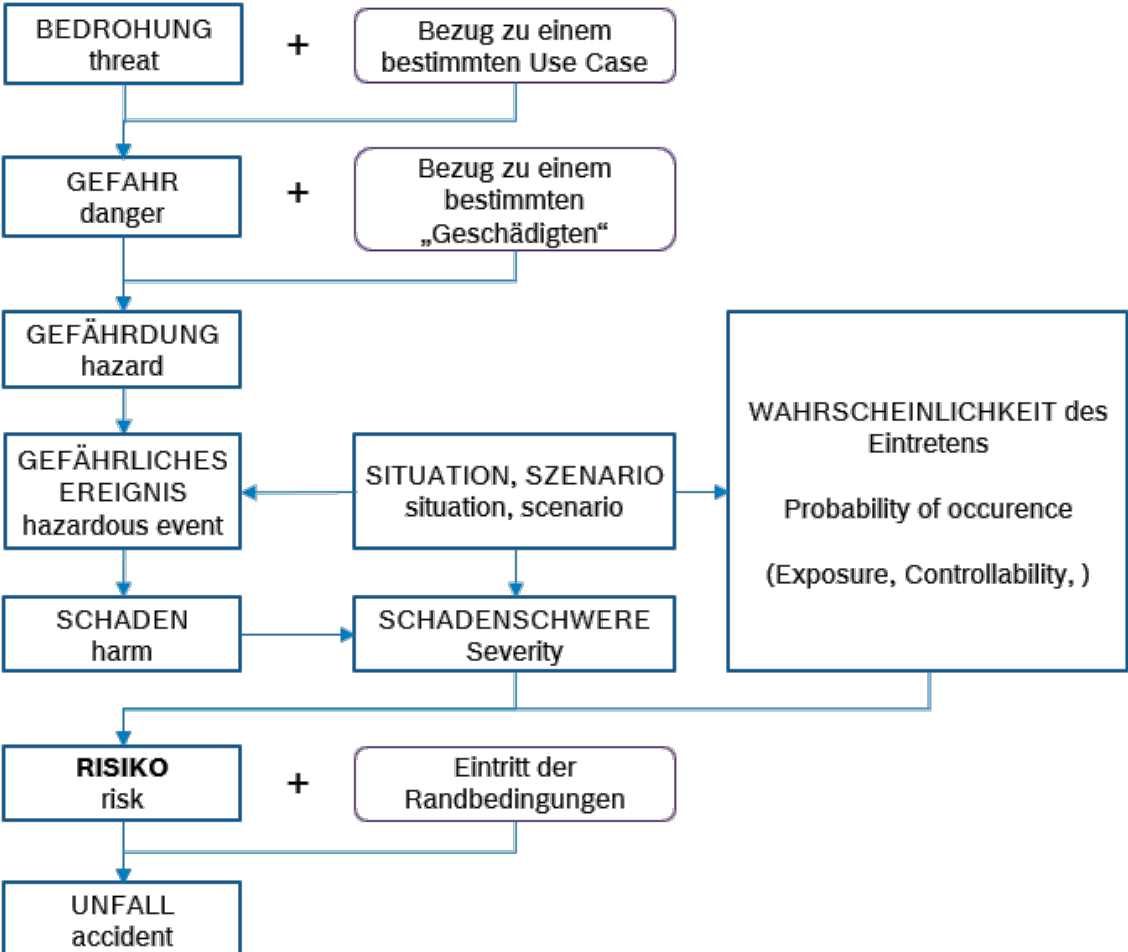


Secondary control points:
Mitigate the effects

Figure: Term-relation-graph developed in VVM based on existing standards

Definition and relations of term based on existing standards

Definition	Beispiel
Bedrohung (threat): mögliche Ursache eines unerwünschten Ereignisses, der einem System oder einer Organisation Schaden zufügen kann [ISO/TR 18638]	Steiles Gebirge in der Nähe der Straßenführung bedroht die Unversehrtheit der Beteiligten 
Gefahr (danger): gefährliche Situation, die, wenn sie nicht vermieden wird, zum Tod oder zu schweren Verletzungen führen kann [ISO 26513]	A: Steinschlag gefahr B: Gefahr von Eisglätte  
Gefährdung (hazard): potential source of harm [ISO 26262, ...] (for a specific stakeholder)	Hz1A: Beschädigung der Fahrgastzelle durch herabfallende Steine Hz2A: Spurverlust & Verlassen der Fahrbahn durch Steine auf der Fahrbahn
Gefährliches Ereignis (hazardous event): combination of a hazard and an operational situation [ISO 26262]	He1Hz1A: Stein mit 100kg Masse trifft die Frontscheibe eines Kfz während der Fahrt im Bereich des Fahrers He2Hz1A: Stein mit 1 kg Masse trifft Masse trifft die Frontscheibe eines Kfz im Stillstand im Bereich des Beifahrers
Schaden (harm): physische Verletzung oder Schädigung der Gesundheit von Personen oder der Beschädigung von Sachen [ISO/IEC Guide 51] <i>modified</i>	Verletzung der FZ-Insassen durch 1. beschädigte Fahrgastzelle 2. Verlassen der Fahrbahn
Risiko (risk): Schadensausmaß kombiniert mit Eintrittswahrscheinlichkeit [ISO/IEC Guide 51]	120 x Steinschläge /Jahr 10 % große Steine mit Verletzungspotential Verkehrsdichte 1:10 Scheibengröße 1:10 => 0,12 Verletzungsfälle/Jahr
Unfall (accident): Eintritt eines Schadens durch ein ungeplantes Ereignis [ISO 24765]	Tatsächlich verletzte Personen durch herabfallende Steine, welche die Windschutzscheibe eines Fz durchschlagen haben.



```

graph TD
    B[BEDROHUNG threat] -- "+" --> C[GEFÄHRDUNG hazard]
    UC[Bezug zu einem bestimmten Use Case] -- "+" --> C
    C -- "+" --> E[GEFÄHRLICHES EREIGNIS hazardous event]
    G[Bezug zu einem bestimmten „Geschädigten“] -- "+" --> E
    E --> H[SCHADEN harm]
    H -- "+" --> R[RISIKO risk]
    S[SCHADENSCHWERE Severity] -- "+" --> R
    R -- "+" --> A[UNFALL accident]
    RB[Eintritt der Randbedingungen] -- "+" --> A
    S[SITUATION, SZENARIO situation, scenario] --> E
    S --> P[WAHRSCHEINLICHKEIT des Eintretens Probability of occurrence Exposure, Controllability, )]
    S --> P
    H --> P
    R --> P
    
```

V05

What is the Mechanism to achieve Safety?

Safety expectation and fulfillment: The Mechanism to achieve Safety

ADS Products are Safe

because they meet

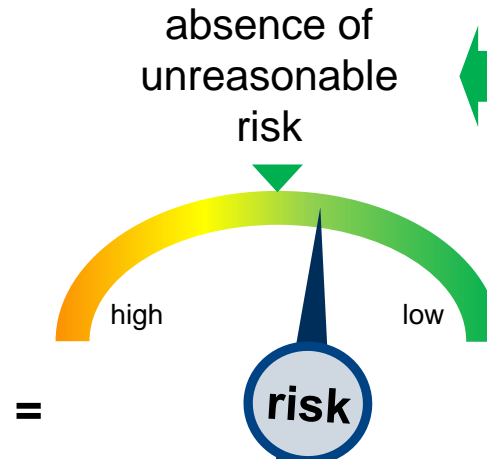
Societal Safety Expectations

despite

- Specification insufficiencies
- Process insufficiencies
- Knowledge insufficiencies
- Behavior uncertainties (others, emergent)
- Measurement uncertainties
- Implementation uncertainties

Expose people to hazards that can lead to harm

Risks from Hazardous events

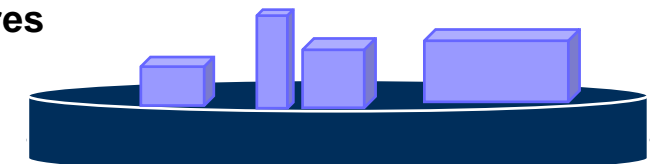


represented by

- RDW, KBA
- NHTSA, FMCSA
- EU Commission, UN-ECE
- Courts, Manufacturer

Safety measures

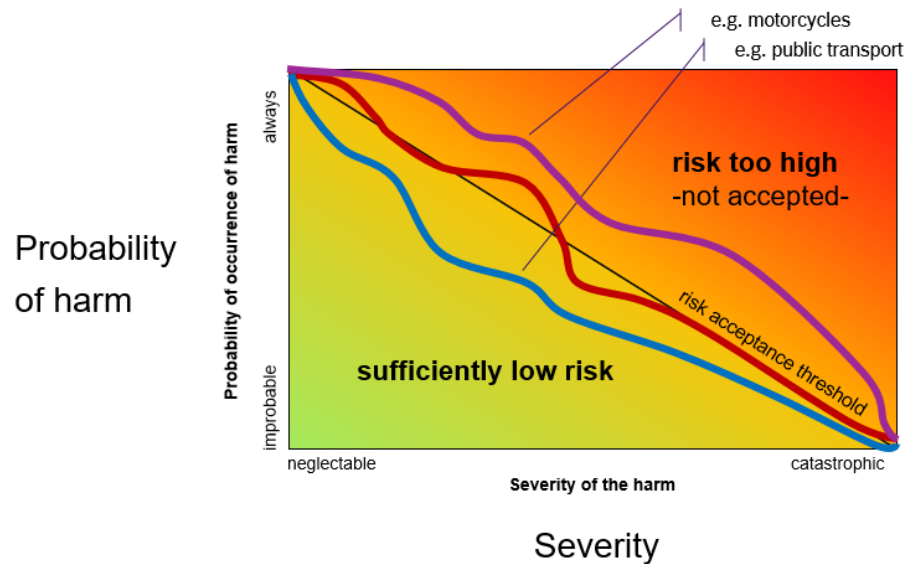
- Rules
- Safety mechanisms, processes
- ODD restrictions, ...



ADS – Automated Driving System
ODD – Operational Design Domain
RDW, KBA – national EU state authorities
NHTSA, FMCSA - US authorities

What is „reasonable risk“?

- ▶ „reasonable“ becomes explicit through
 - ▶ **Legislation** (laws, directives)
 - ▶ **Jurisprudence** (court rulings)
 - ▶ **State of the art** (industrial facts)



Types of Risk Acceptance Criteria (RAC)

1. Generic RAC **with reference**
example: MEM, GAMAB, PRB
2. Generic RAC **without reference**
example: ALARP
3. **Explicit RAC with/without reference**
example: EU L4 implementing act:
fatalities < 10^{-7} /h (indicative target)

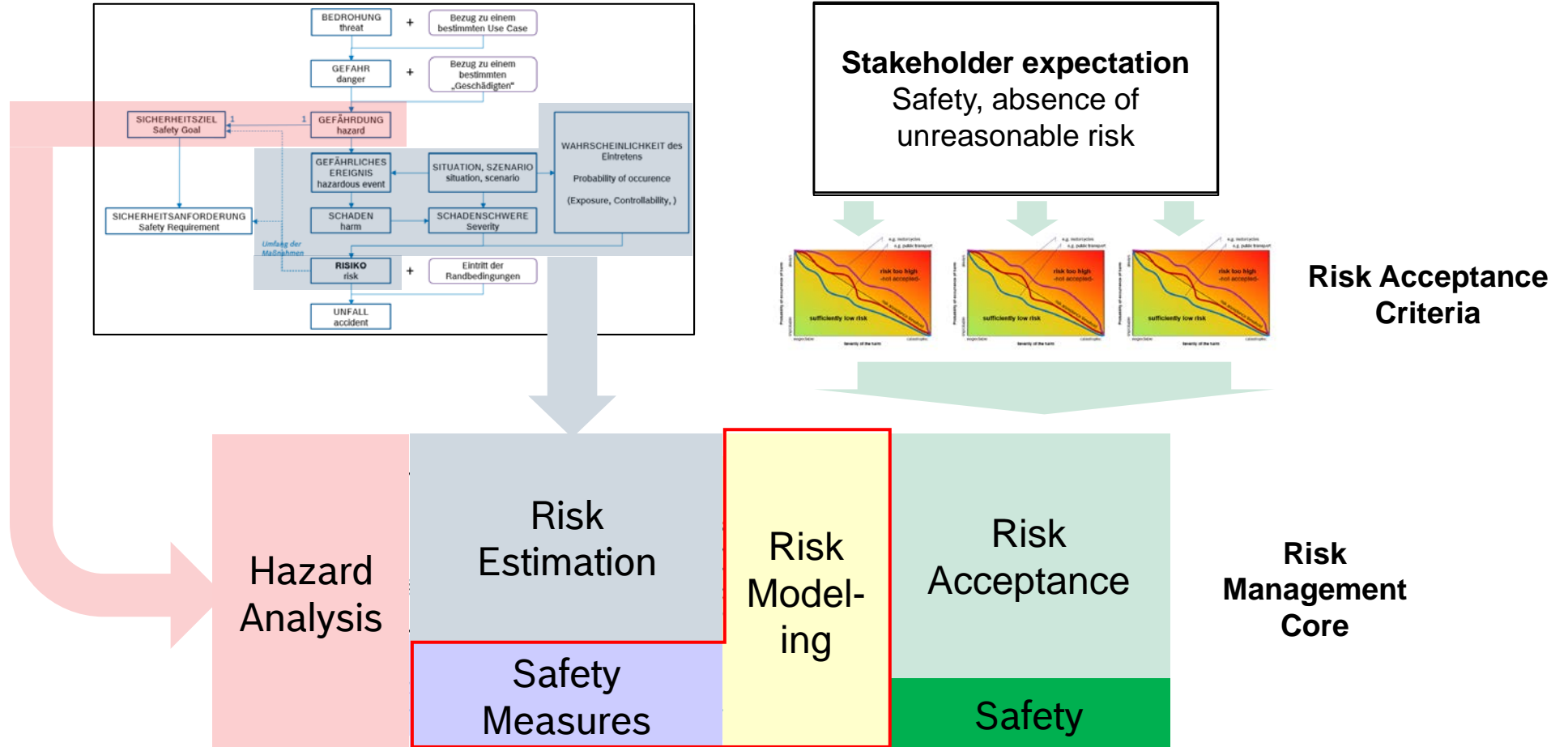
MEM	Minimal Endogenous Mortality, EU youth mortality rate
GAMAB	Globalement Au Moins Aussi Bon, Principle of equal safety
PRB	Positive Risk Balance, Statistic or Capability as reference
ALARP	As Low As Reasonable Practicable, State of the art + x

Risk Acceptance is not only ONE number | There are multiple RACs at the same time

How did VVM assemble the Method 'Risk Management Core'?

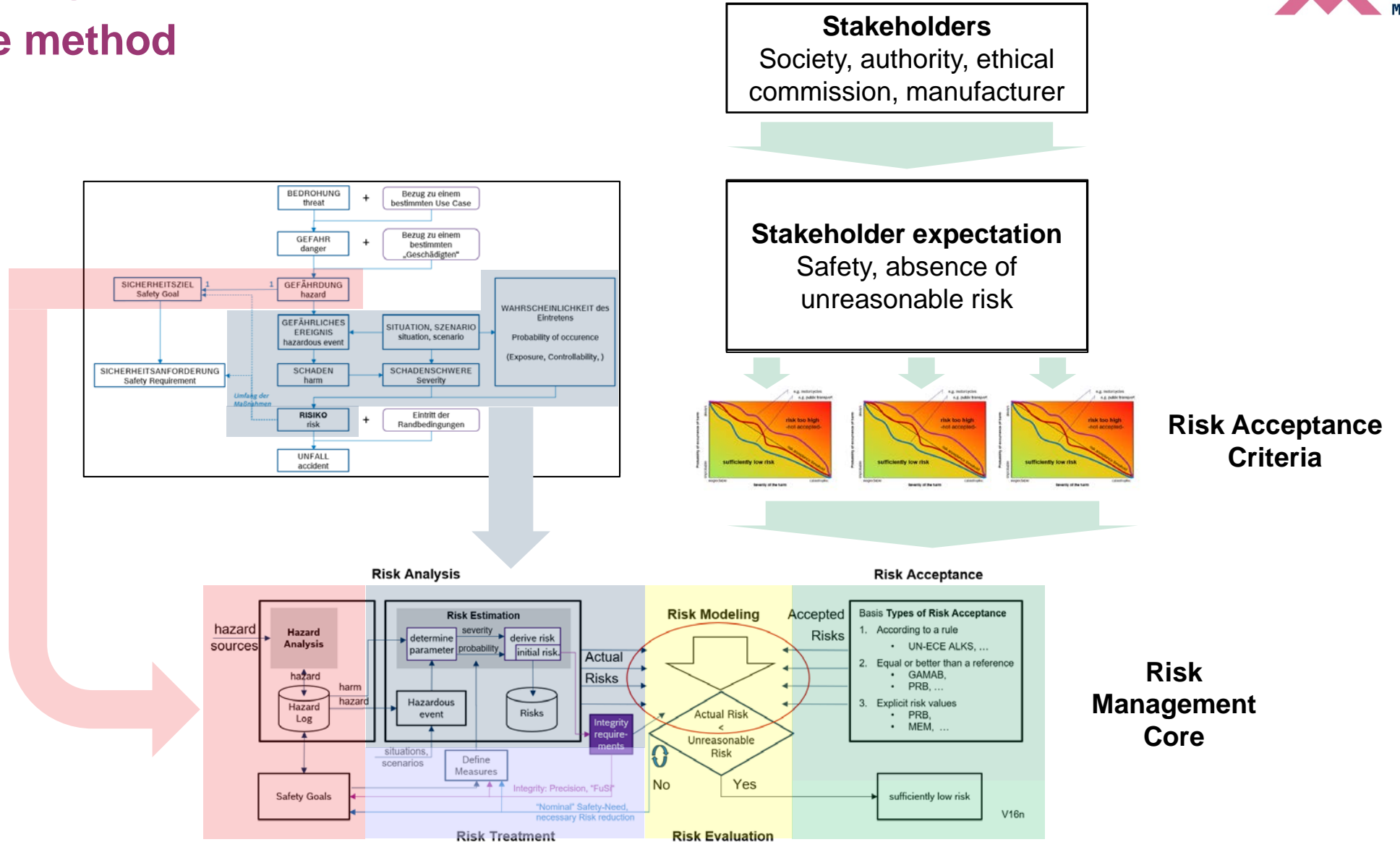
The Risk Management Core

Creating the method



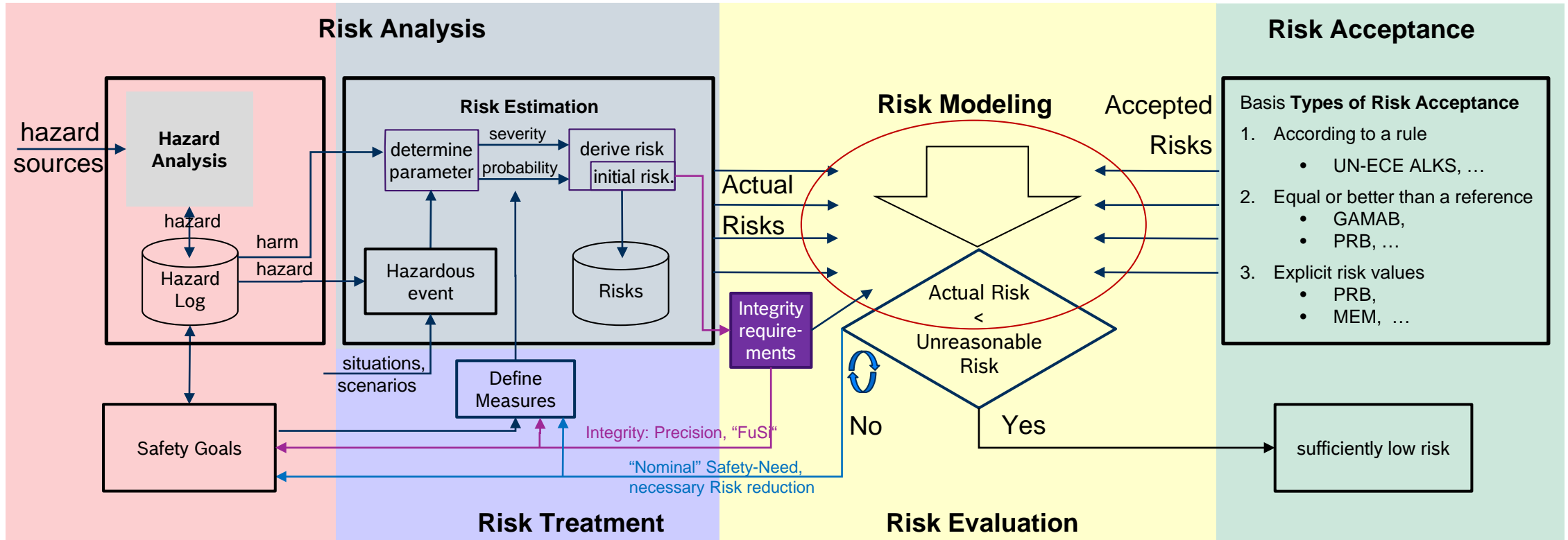
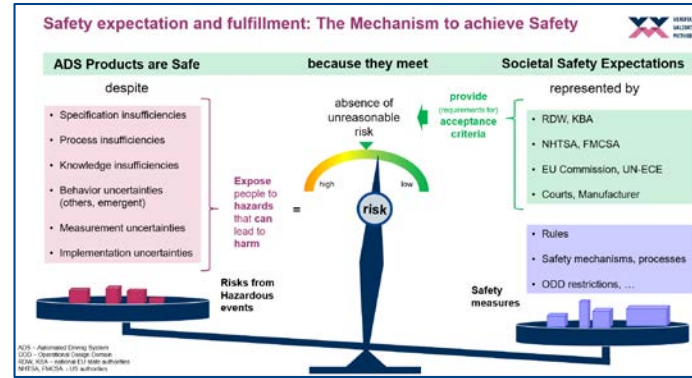
The Risk Management Core

Creating the method

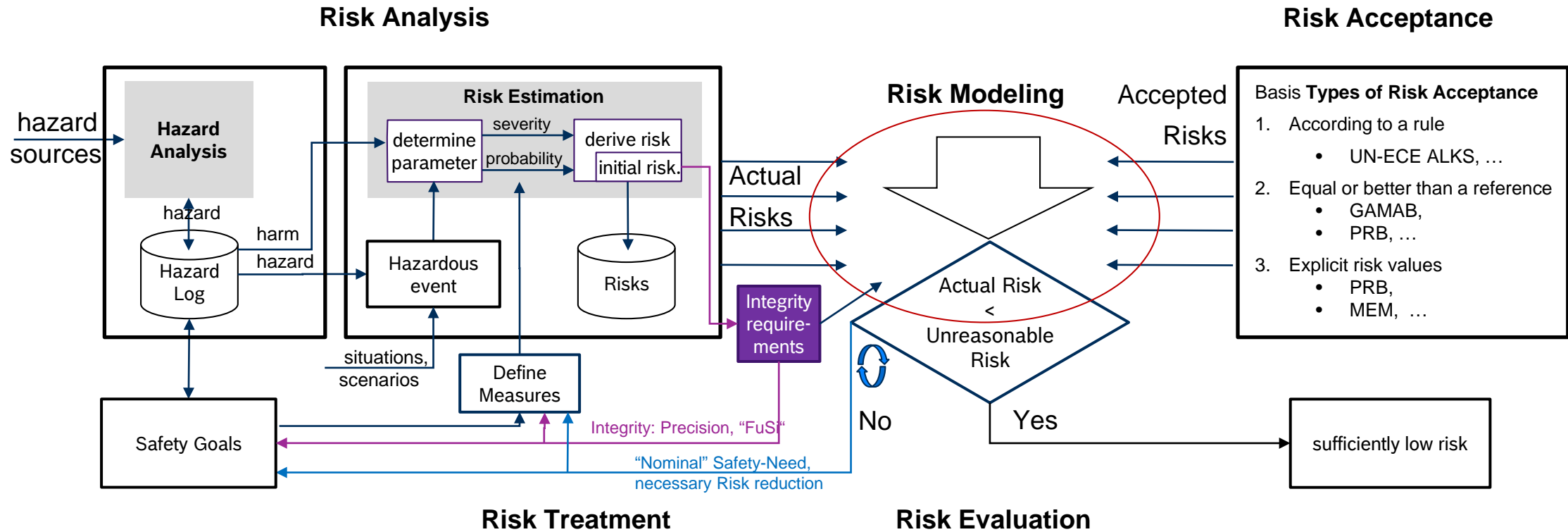


The Risk Management Core

The implemented Mechanism

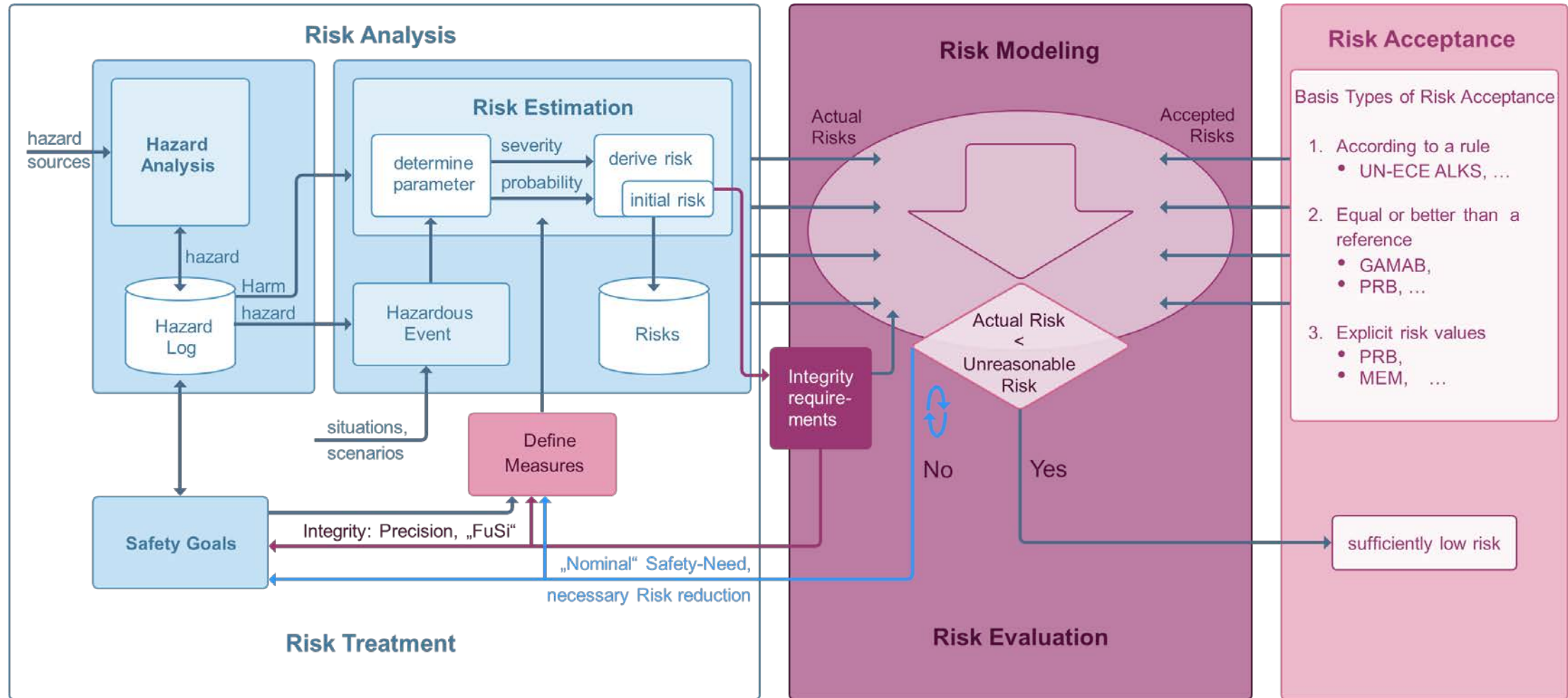


One VVM Method: The Risk Management Core



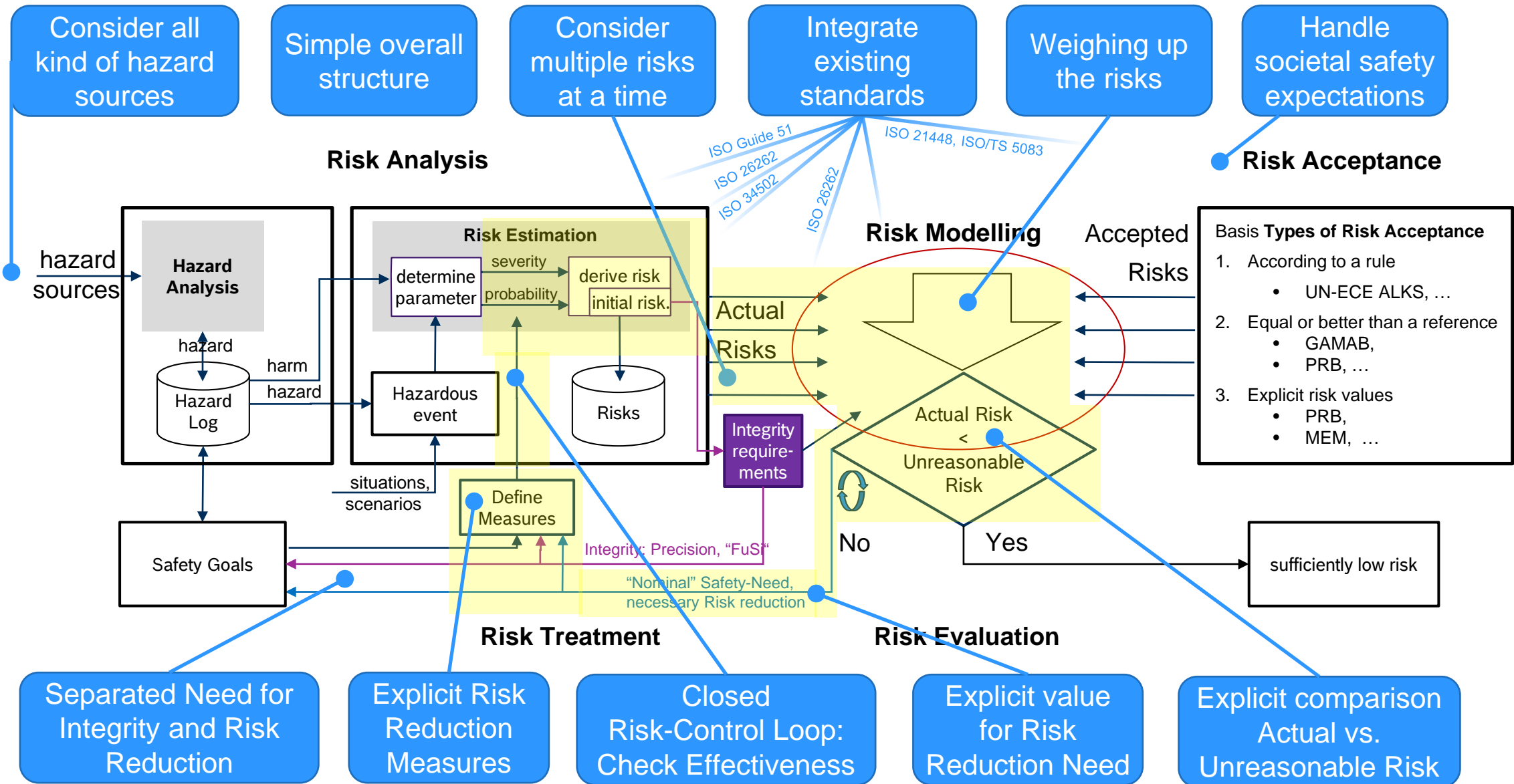
One VVM Method:

The Risk Management Core - Communication Color Design



See the Advantages of the Method 'Risk Management Core'



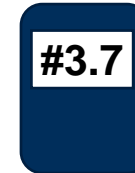


Transition

Interested in the topic?

➤ Details on Poster

- Poster #3.7 - The Risk Management Core



➤ More about the application of the Risk Management Core

- Presentation: “How VVM handles risk and links to the development process”

➤ Read the Pre-Print

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

➤ Authors:

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

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 “reasonable” level of risk is not yet explicitly defined. Simply 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 derived 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+) on public roads can be supported by a safety case. It should provide convincing 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 [1]. Automotive safety standards and reports relevant for automated vehicles such as ISO 26262 [2], ISO 21448 [3] and ISO/TR 4804 [4] 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



Thank you!

Thomas Kirschbaum, Robert Bosch GmbH
Thomas.Kirschbaum@de.bosch.com



A project developed by the VDA Leitinitiative
autonomous and connected driving

Supported by:



on the basis of a decision
by the German Bundestag