A result from the German project “VV-Methods”

The “Risk Management Core”

How to align system risk with social expectations?

PROJECT of the PEGASUS FAMILY

VERIFICATION VALIDATION METHODS

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

Thomas Kirschbaum, Robert Bosch GmbH

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**

=

absence of unreasonable risk

provide (requirements for) **acceptance criteria**

represented by

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

Risks from Hazardous events

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

The Risk Management Core Overview

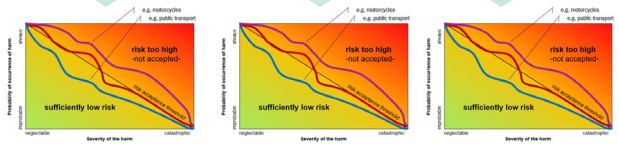
VERIFICATION VALIDATION METHODS

Stakeholders
Society, authority, ethical commission, manufacturer

Precise terms definitions and term relations

hazard > harm > severity > probability > risk

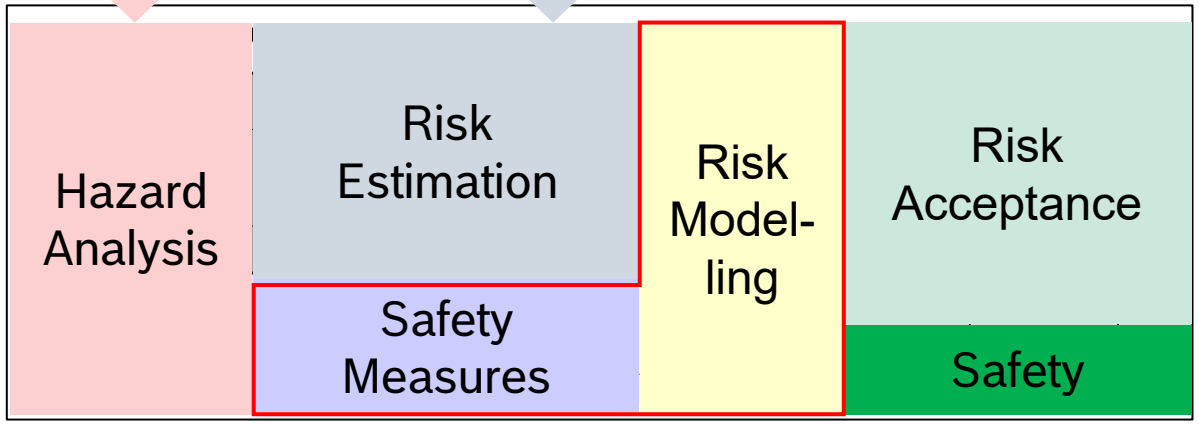
Stakeholder expectation
Safety, absence of unreasonable risk



Risk Acceptance Criteria

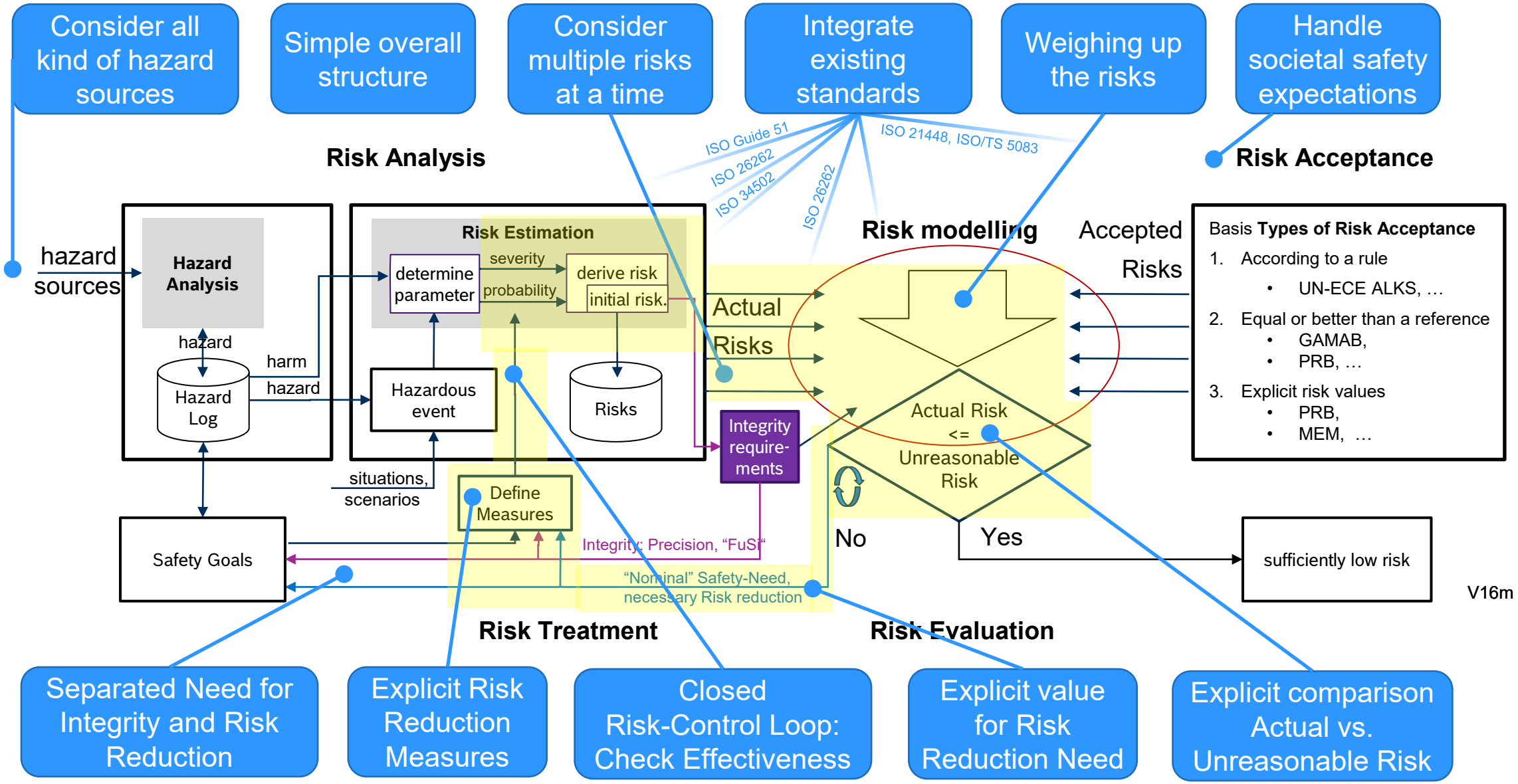
Hazard

Risk

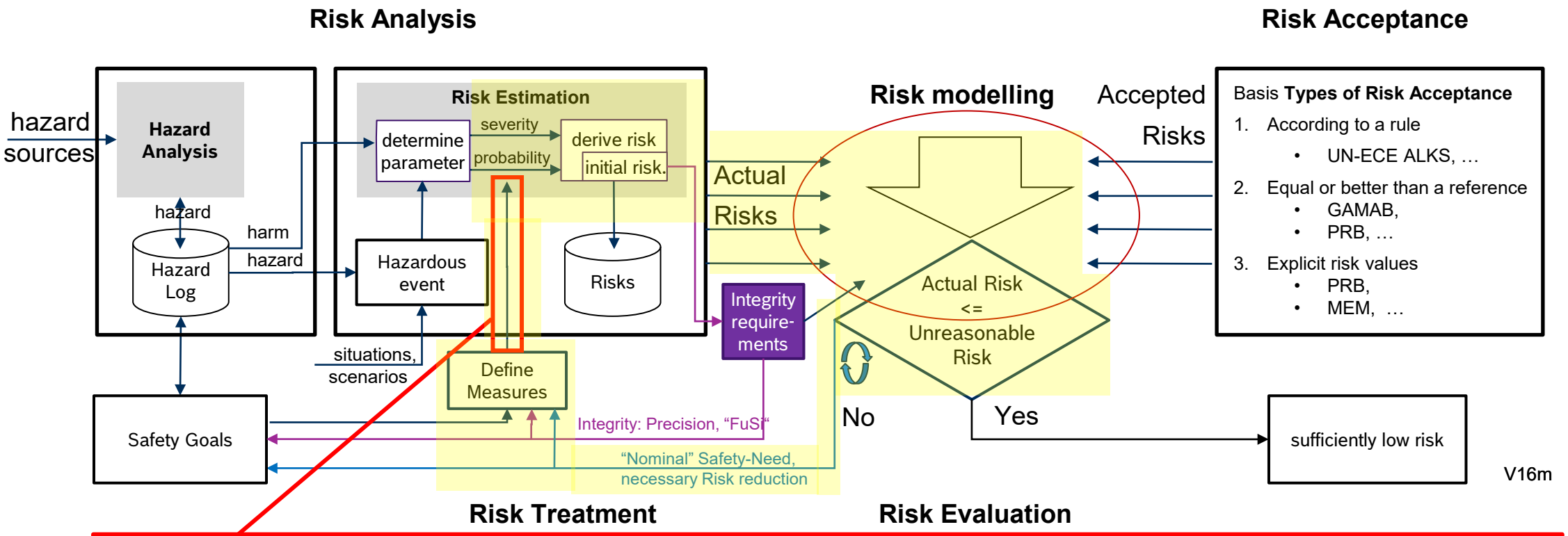


Risk Management Core

V03


Consider all kind of hazard sources
Simple overall structure
Consider multiple risks at a time
Integrate existing standards
Weighing up the risks
Handle societal safety expectations
ISO Guide 51
ISO 26262
ISO 34502
ISO 26262
ISO 21448, ISO/TS 5083
Risk Analysis
Risk Acceptance
Risk modelling
hazard sources
Hazard Analysis
hazard
Hazard Log
harm
hazard
Risk Estimation
determine parameter
severity
probability
derive risk
initial risk.
Hazardous event
Risks
Actual Risks
Accepted Risks
Basis Types of Risk Acceptance
1. According to a rule
• UN-ECE ALKS, …
2. Equal or better than a reference
• GAMAB,
• PRB, …
3. Explicit risk values
• PRB,
• MEM, …
Integrity require-ments
Actual Risk <= Unreasonable Risk
situations, scenarios
Define Measures
Safety Goals
Integrity: Precision, "FuSi"
"Nominal" Safety-Need, necessary Risk reduction
No
Yes
sufficiently low risk
V16m
Risk Treatment
Risk Evaluation
Separated Need for Integrity and Risk Reduction
Explicit Risk Reduction Measures
Closed Risk-Control Loop: Check Effectiveness
Explicit value for Risk Reduction Need
Explicit comparison Actual vs. Unreasonable Risk

Safety Driven V&V



Effectiveness Check: V&V needs to show, that **the measures in fact reduce the risk** as planned

- V&V is part of the Risk Management Core – it makes risk modelling possible at all
- V&V part in the Risk Management Core can check and demonstrate the social expectations

➔ **V&V targets** & success criteria need to be **derived from societal acceptance** criteria

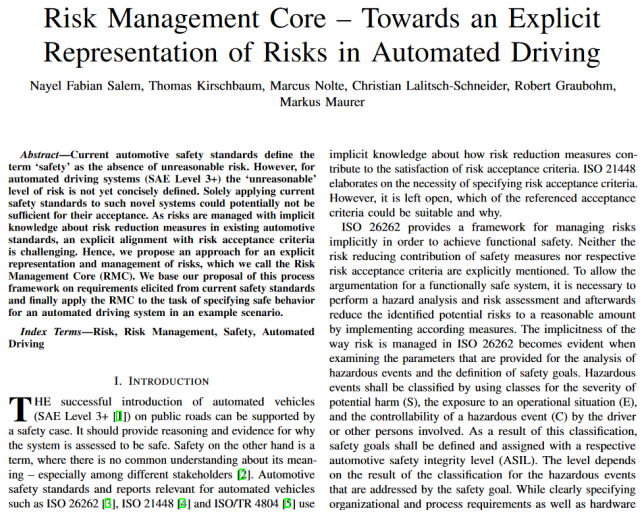
Risk Management Core: Interested?

Upcoming publication with further details

VERIFICATION VALIDATION METHODS

Publication from VVM Subproject TP3 AP3.2 - Local Safety Assessment

- **Titel:**
  - 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
- **Intended publication platform :**
  - IEEE Access
- **Submission period :**
  - Planned Q3/2023
  - Preprint available on ARxIV



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

The "Risk Management Core"
A result from the German project "VV-Methods"

PROJECT of the PEGASUS FAMILY

VERIFICATION VALIDATION METHODS

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

Thank you!

Thomas Kirschbaum, Robert Bosch GmbH