Security Risk Analysis

for

Automotive Systems

GENIVI All Member Meeting
Munich 16.5.2019
Dirk Leopold

Agenda

Overview itemis AG

Terms and Concepts

- Risk and Risk Management
- Privacy, Safety and Security

Methodology for Security Risk Analysis

Risk Analysis in the Automotive Domain

itemis AG
Short Facts

- founded 2003
- privately held – organic growth
- offices in Germany, France, Switzerland, Tunesia
- 225 employees + freelancers
- 22 Mio. Euros revenue
- 30% Automotive – 70% other (Insurance, Telecom, Logistics, Railway, Retail, …)

itemis AG
Methods and Tools

- Model Based Software Development
- Domain Specific Languages & Language Engineering
- Requirements Engineering & Traceability
- Productline Engineering & Variant Management
- Security & Safety

- GENIVI Associate Member
- Franca Project Lead

Security@itemis
Background Security Analyst

Security Analyst is a software tool supporting modular risk assessment of automotive systems

- based on various norms and best practice approaches (ISO 31000, ISO 27005, Common Criteria, STRIDE, TARA, ISO 21434...)
- result of cooperation between Fraunhofer AISEC (methods) itemis AG (tooling) and one German OEM since Q1 2016

Main functions supported within automotive security engineering

- system analysis and identification of security risks
- system design and definition of appropriate protective measures

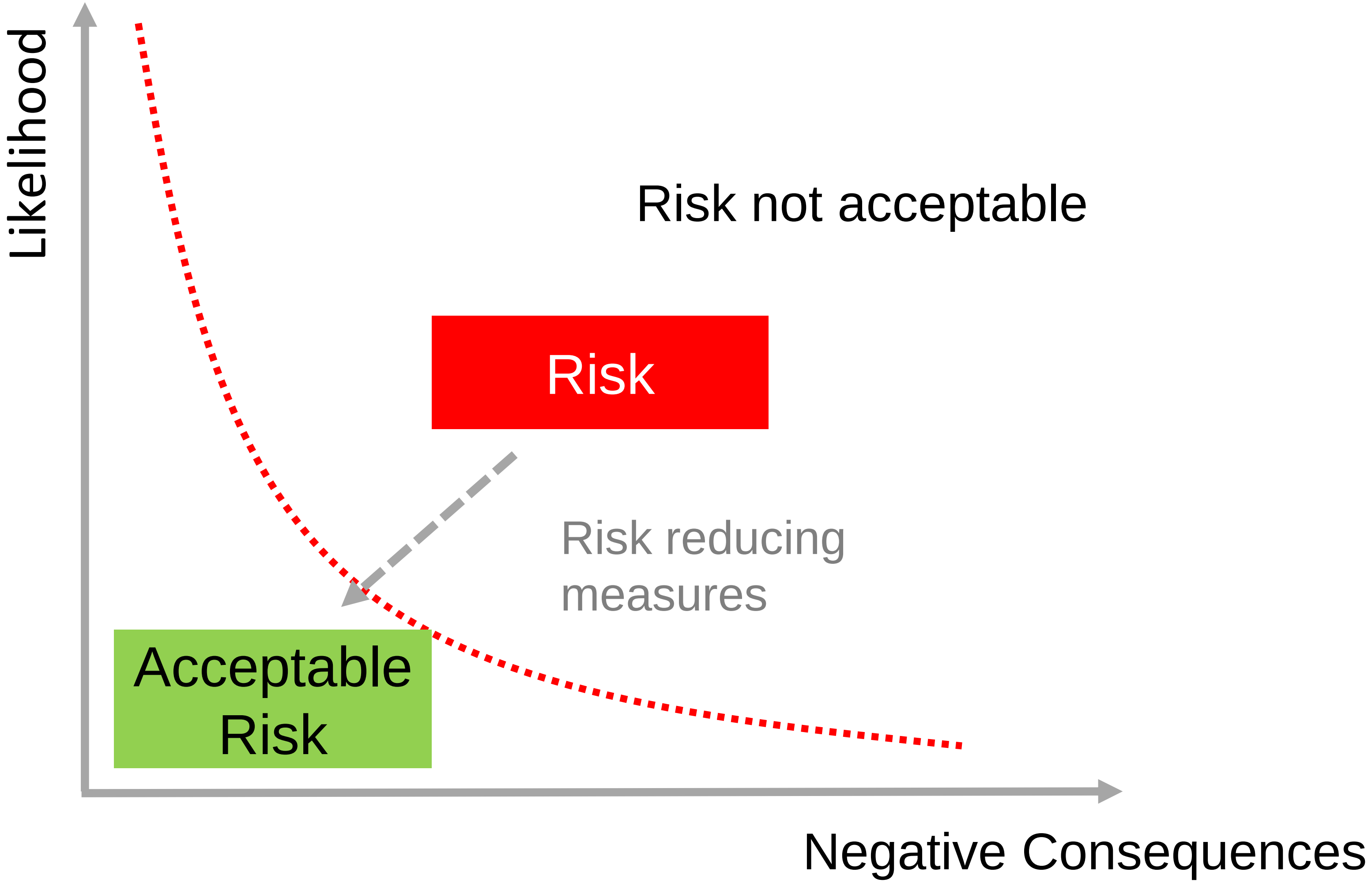
R&D Project „SecForCARs“
Security For Connected, Automated Cars

Bundesministerium
für Bildung
und Forschung

- „Bundesministerium für Bildung und Forschung“ R&D project
- duration: 1st April 2018 – 31st March 2021
- allocated funding of 7.2 million Euros
- kick-off: 12th-13th April in Munich
- partners include industry, SME, research and academia
  - Infineon, Robert Bosch GmbH, ESCRYPT
  - Itemis, Mixed Mode, Schutzwerk
  - Fraunhofer AISEC, Fraunhofer IEM
  - Universität Ulm, TU Braunschweig, TU München, Hochschule Karlsruhe

https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/sicherheit-fuer-vernetzte-autonome-fahrzeuge

Terms and Concepts
Risk Management



ISO 26262
Hazard Analysis and Risk Assessment

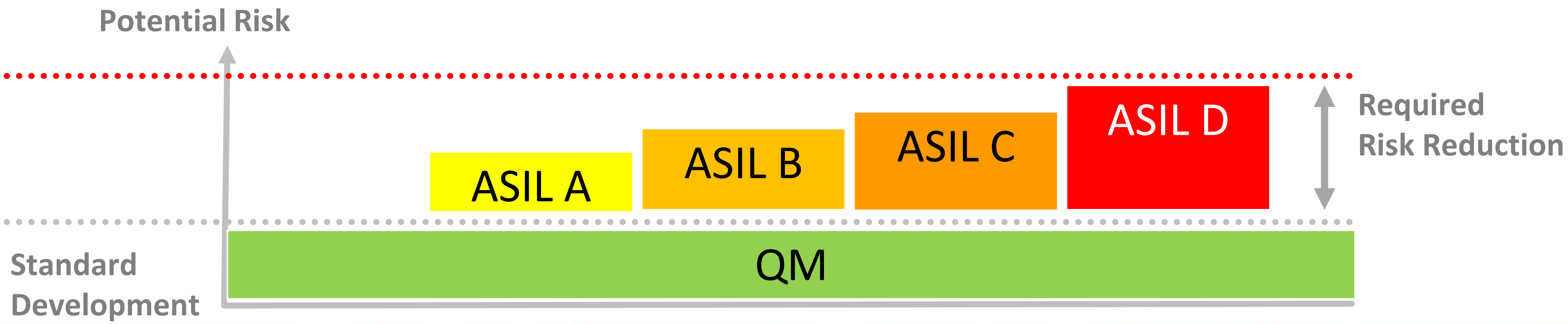
Risk = (expected loss in case of accident) x (probability of accident occurring)

or

Risk = Severity x (Exposure x Controllability)

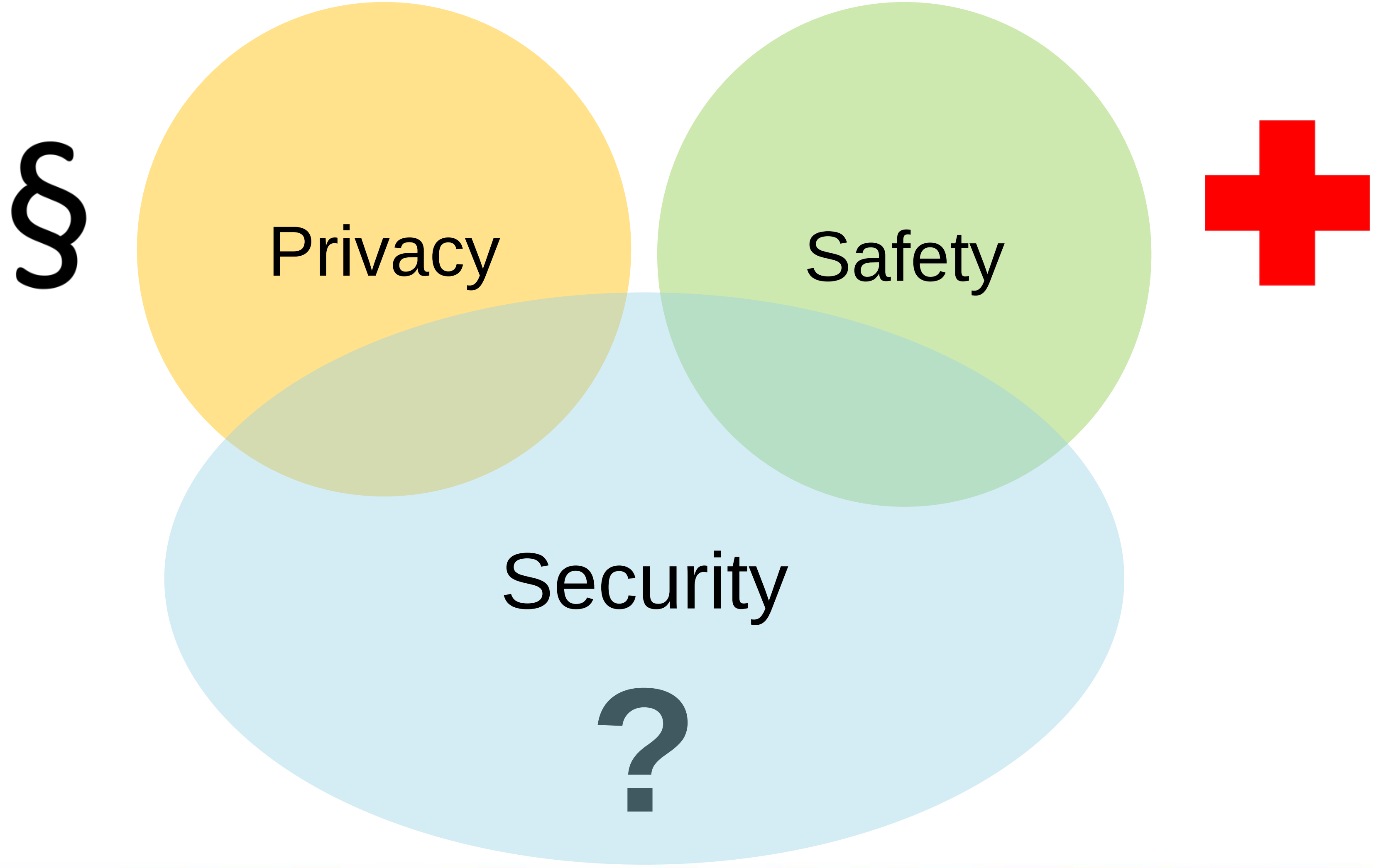
Automotive Safety Integrity Levels (ASIL)

- define the degree of rigor applied in the assurance of the safety requirements
- levels A – D
- QM level (quality management without specific safety aspect)

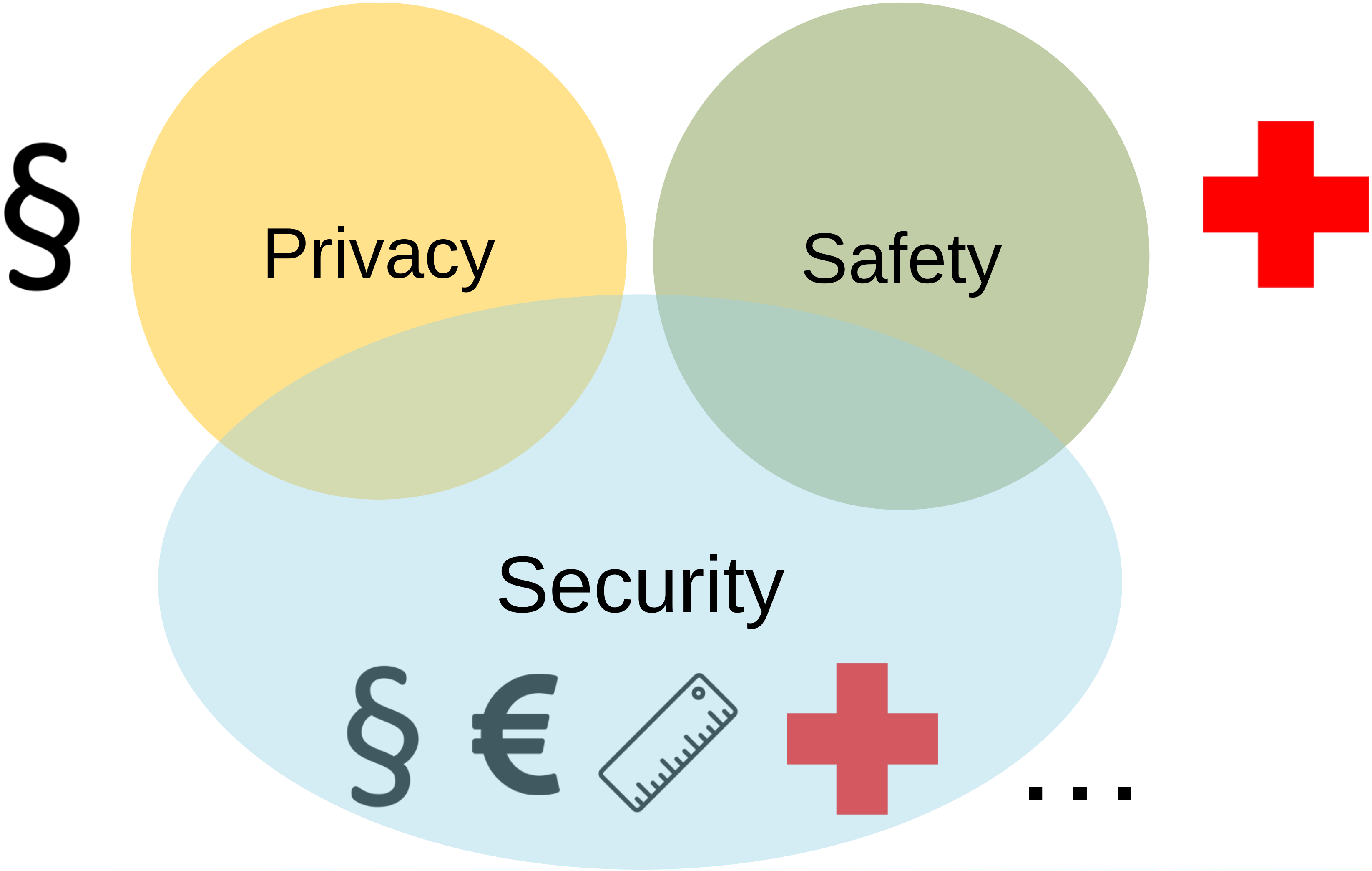


Terms and Concepts

Privacy, Security and Safety



Terms and Concepts
Privacy, Security and Safety



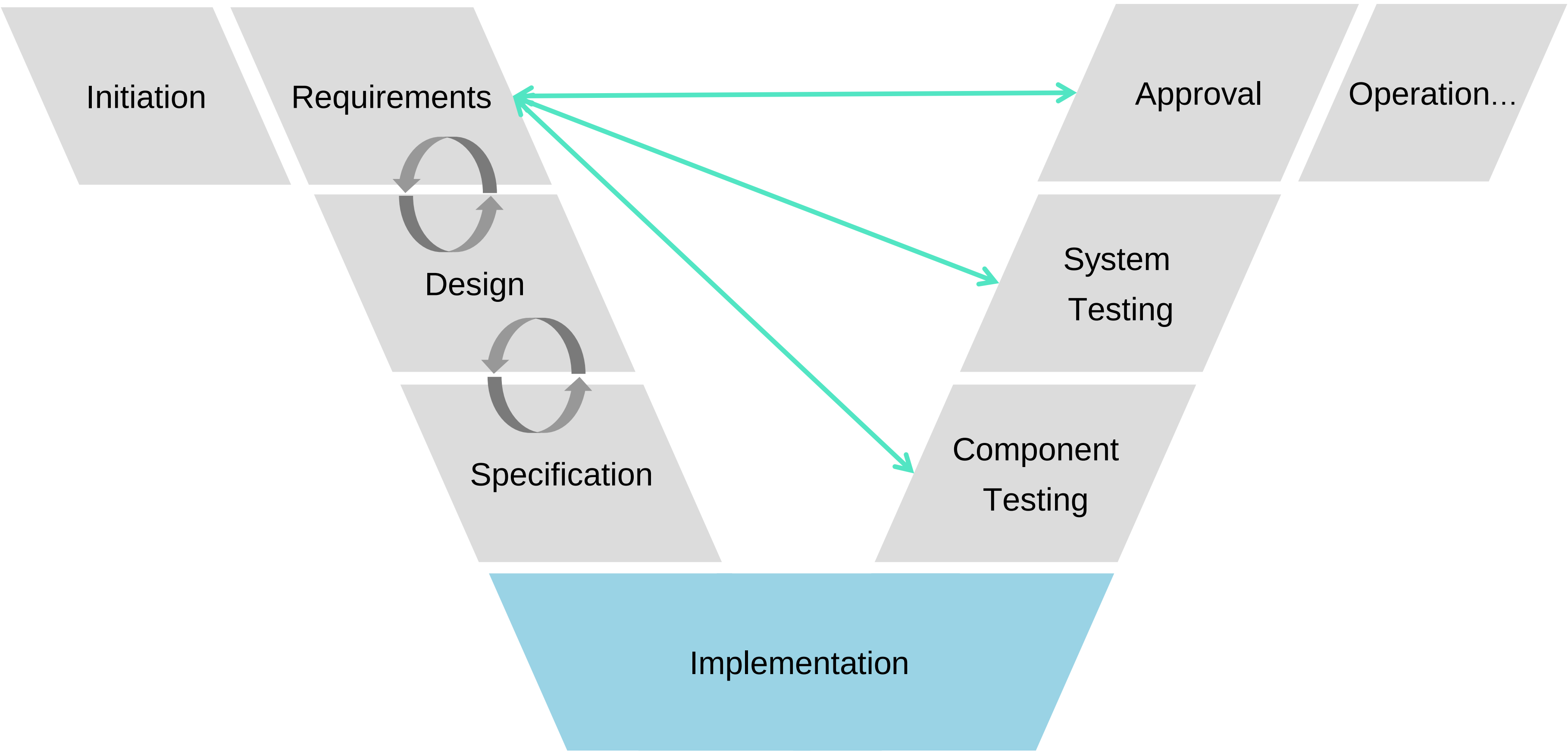
§ Privacy

Safety

Security

§ € ...

„Security by Design“
Security Risk Analysis in the Development Life Cycle



Initiation

Requirements

Design

Specification

Implementation

Component Testing

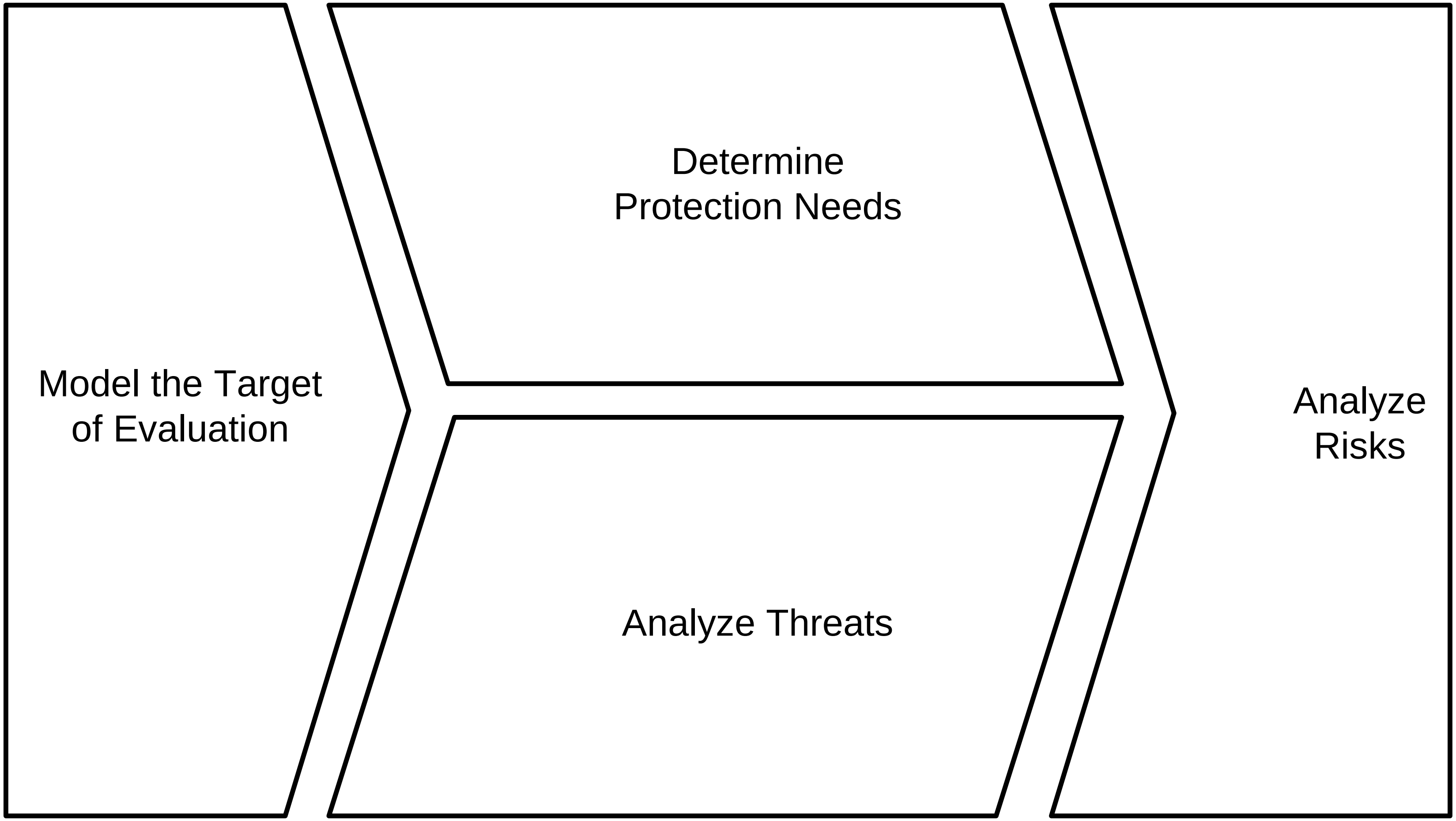
System Testing

Approval

Operation…

Modular Risk Assessment (MoRA)

Methodology



Model the Target of Evaluation

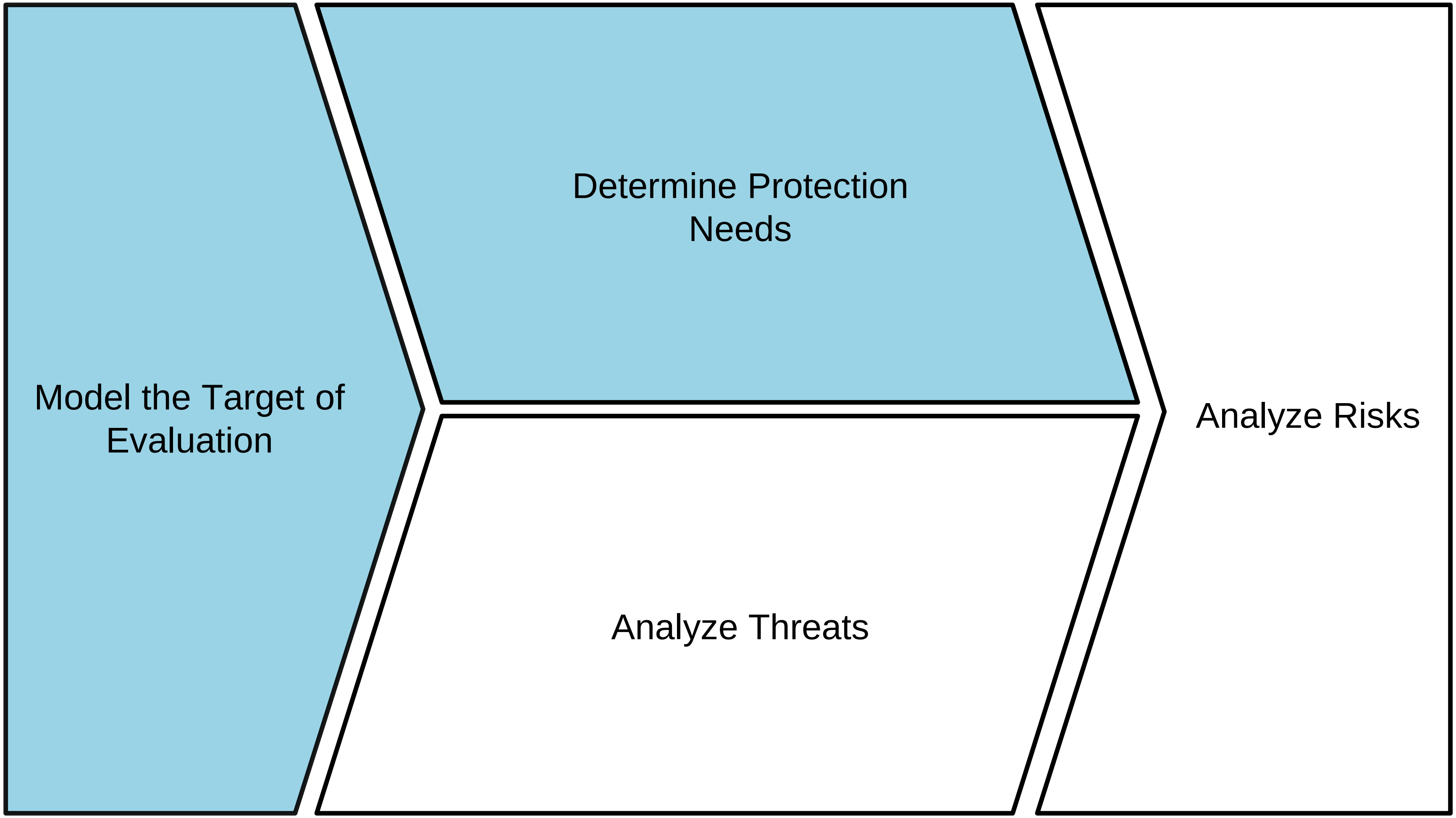
Determine Protection Needs

Analyze Threats

Analyze Risks

J. Eichler and D. Angermeier. "Modular risk assessment for the development of secure automotive systems". 31. VDI/VW-Gemeinschaftstagung Automotive Security, VDI, 2015

Security Risk Analysis
Domain Experts…



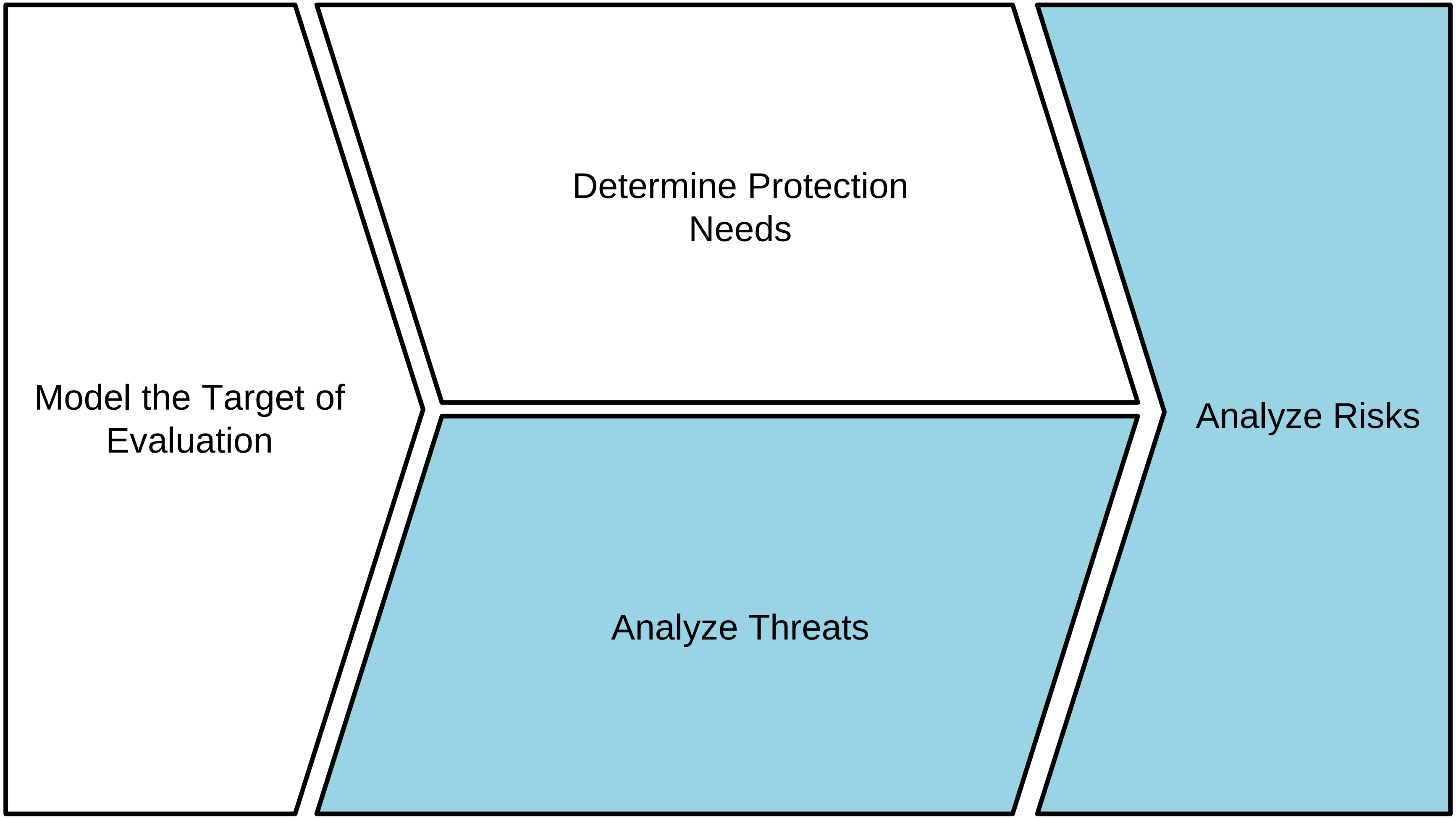
Model the Target of Evaluation

Determine Protection Needs

Analyze Threats

Analyze Risks

Security Risk Analysis
… and Security Experts have to work together!



Model the Target of Evaluation

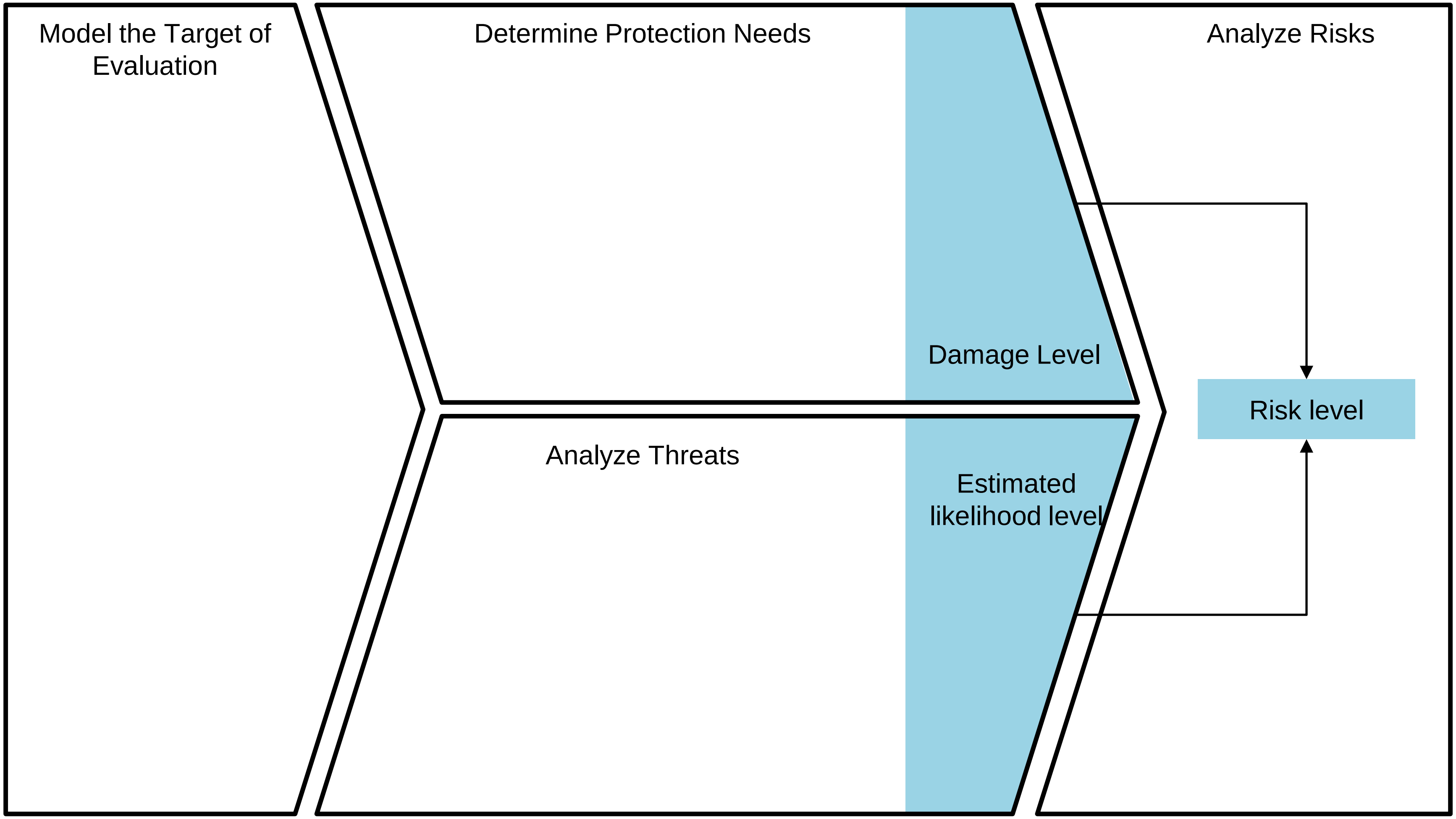
Determine Protection Needs

Analyze Threats

Analyze Risks

Modular Risk Assessment (MoRA)

Core Activities


Model the Target of Evaluation

Determine Protection Needs

Damage Level

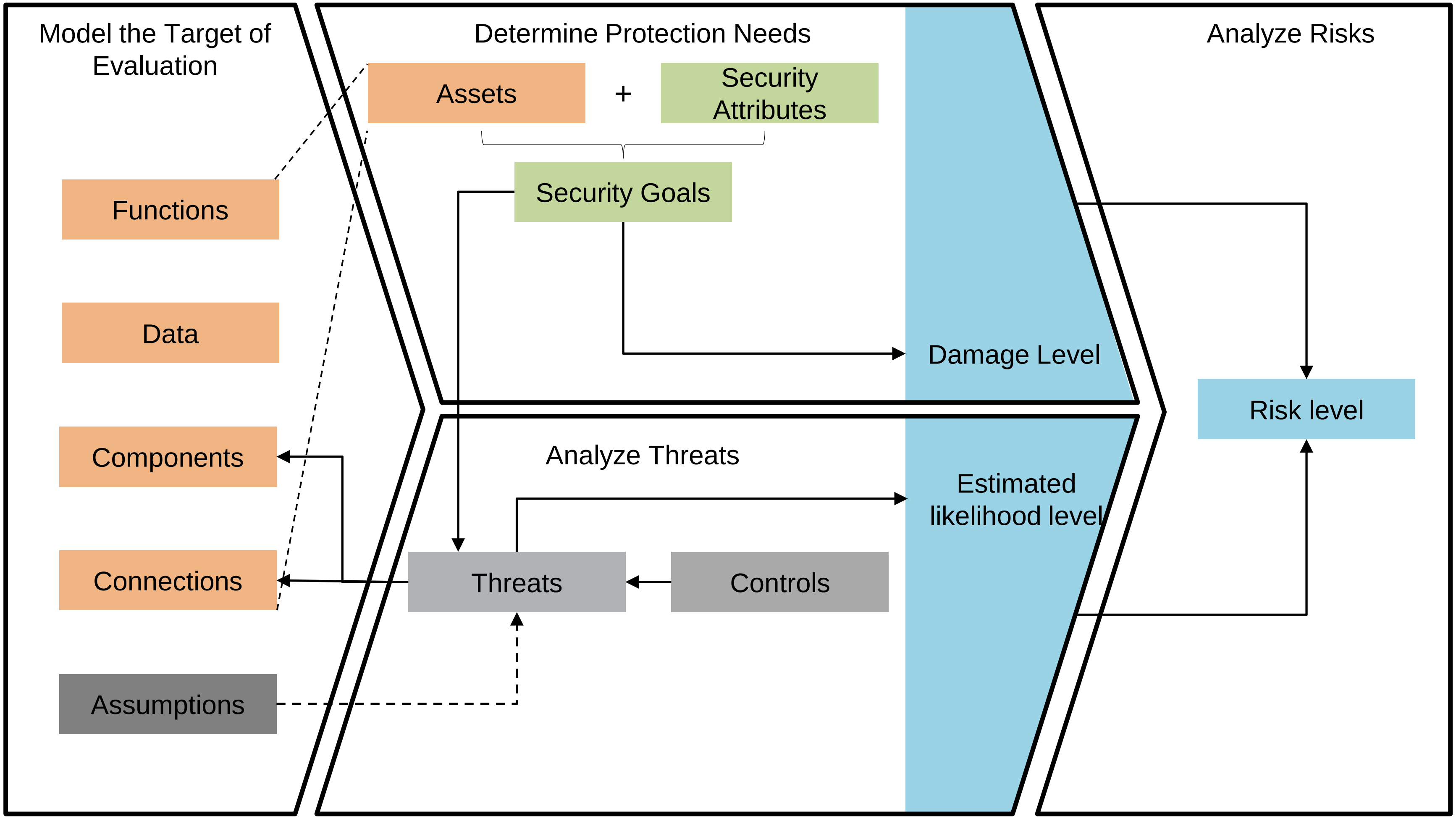
Analyze Threats

Estimated likelihood level

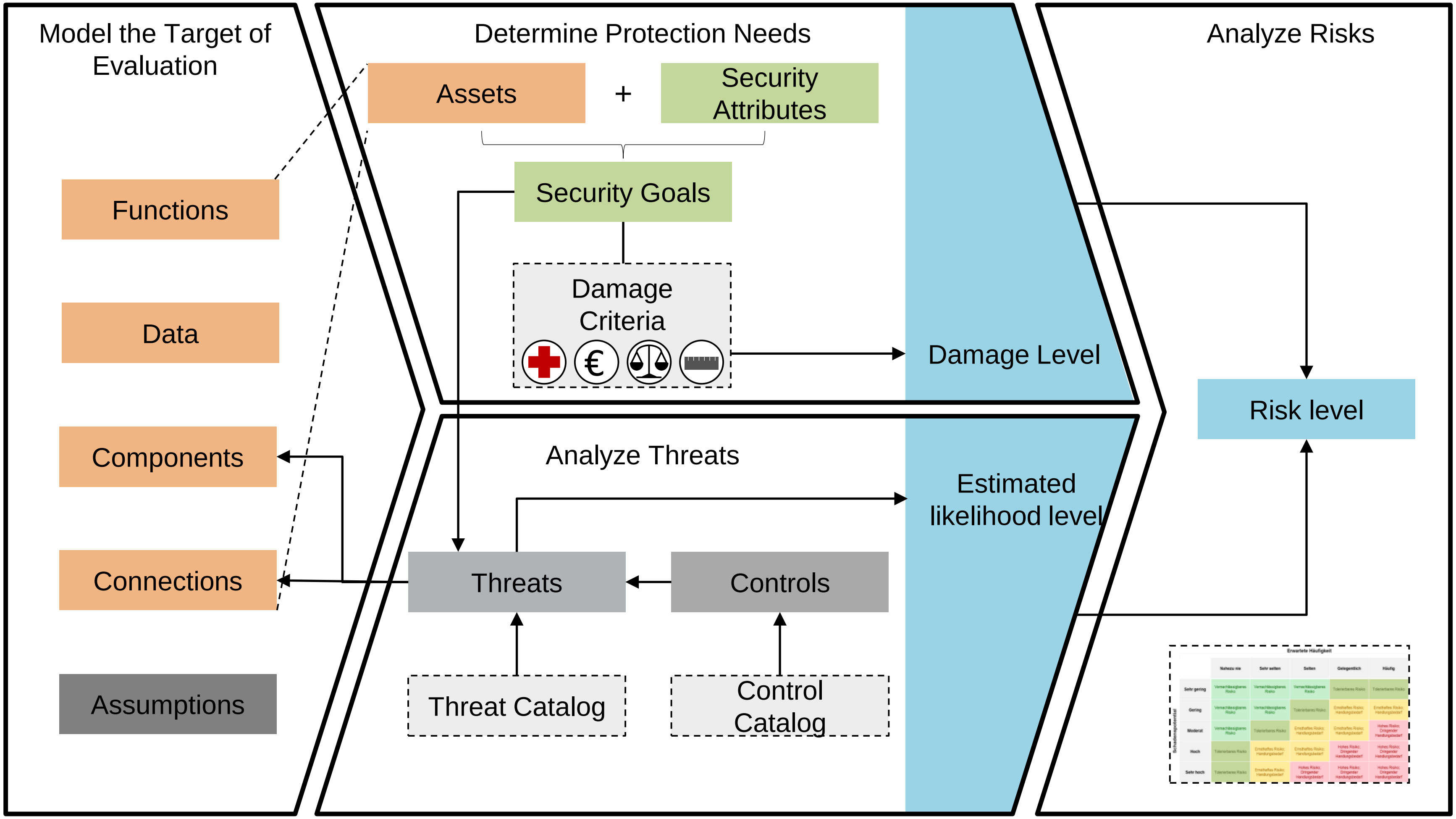
Analyze Risks

Risk level

Modular Risk Assessment (MoRA)
Results



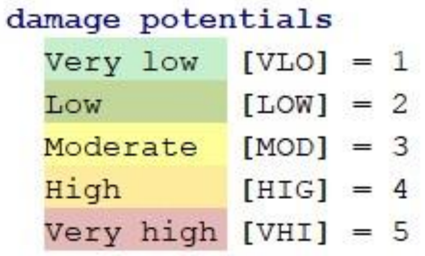
Modular Risk Assessment (MoRA)
Example Configuration



	Erwartete Häufigkeit				
	Nahezu nie	Sehr selten	Selten	Gelegentlich	Häufig
Sehr gering	Vernachlässigbares Risiko	Vernachlässigbares Risiko	Vernachlässigbares Risiko	Tolerierbares Risiko	Tolerierbares Risiko
Gering	Vernachlässigbares Risiko	Vernachlässigbares Risiko	Tolerierbares Risiko	Ernsthaftes Risiko; Handlungsbedarf	Ernsthaftes Risiko; Handlungsbedarf
Moderat	Vernachlässigbares Risiko	Tolerierbares Risiko	Ernsthaftes Risiko; Handlungsbedarf	Ernsthaftes Risiko; Handlungsbedarf	Hohes Risiko; Dringender Handlungsbedarf
Hoch	Tolerierbares Risiko	Ernsthaftes Risiko; Handlungsbedarf	Ernsthaftes Risiko; Handlungsbedarf	Hohes Risiko; Dringender Handlungsbedarf	Hohes Risiko; Dringender Handlungsbedarf
Sehr hoch	Tolerierbares Risiko	Ernsthaftes Risiko; Handlungsbedarf	Hohes Risiko; Dringender Handlungsbedarf	Hohes Risiko; Dringender Handlungsbedarf	Hohes Risiko; Dringender Handlungsbedarf

Negative Consequences
Damage Potential (DP)

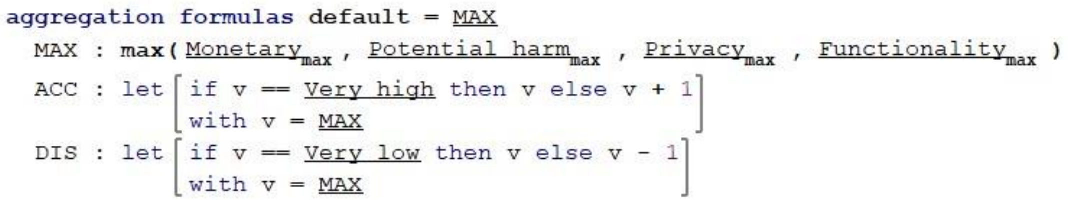
- the damage potential (DP) describes the potential damage resulting from the loss of a defined security goal
- severity levels of damages have to be defined and documented for each damage class (e.g. very high, high, moderate, low, very low)



damage potentials

Very low	[VLO]	=	1
Low	[LOW]	=	2
Moderate	[MOD]	=	3
High	[HIG]	=	4
Very high	[VHI]	=	5

- qualitative and quantitative damage properties have associated with severity levels (e.g. financial loss exceeding 1 million Euros -> very high)
- the rules for the aggregation of damage potentials across damage classes have to be defined and documented (e.g. mathematical weighted model)



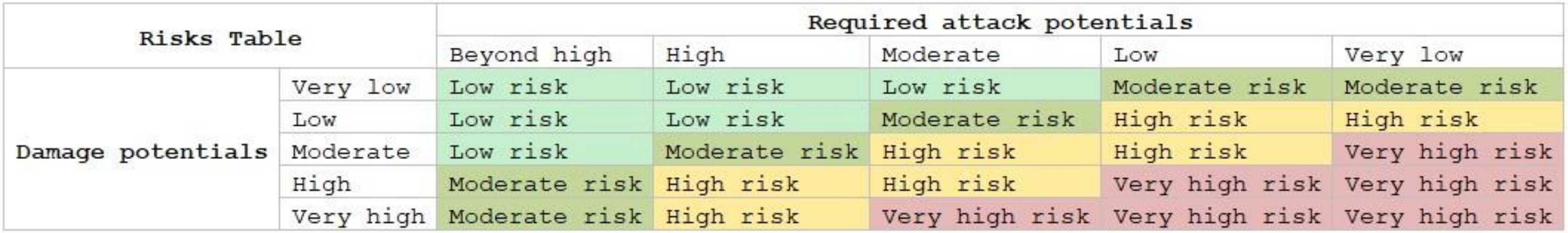
```
aggregation formulas default = MAX
  MAX : max( Monetary_max , Potential harm_max , Privacy_max , Functionality_max )
  ACC : let [ if v == Very high then v else v + 1
              with v = MAX                          ]
  DIS : let [ if v == Very low then v else v - 1
              with v = MAX                          ]
```

Likelihood Determination
Attack Potential

- no statistical data (e.g. MTBF) applicable in the realm of security!!
- risk factors required for the calculation of RAP
  - expertise (e.g. layman, proficient, expert, multiple experts)
  - knowledge about SUD (e.g. public, restricted, sensitive, critical)
  - equipment (e.g. standard, specialized, bespoke, multiple bespoke)
  - required time (e.g. minutes, hours, days, years)
- likelihood determined by the required capabilities of the attacker to perform a successful attack = required attack potential (RAP)

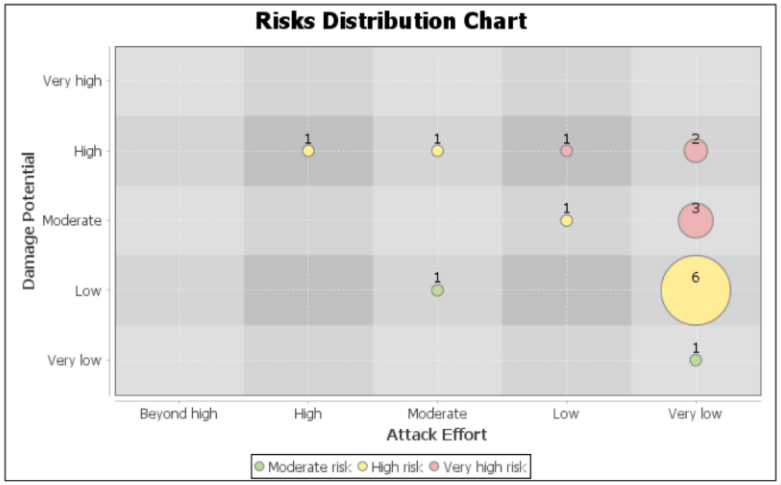
Risk Analysis
Determining the Security Risk

- combining damage potentials (severity) & attack potentials (likelihood)



Risks Table		Required attack potentials				
		Beyond high	High	Moderate	Low	Very low
Damage potentials	Very low	Low risk	Low risk	Low risk	Moderate risk	Moderate risk
	Low	Low risk	Low risk	Moderate risk	High risk	High risk
	Moderate	Low risk	Moderate risk	High risk	High risk	Very high risk
	High	Moderate risk	High risk	High risk	Very high risk	Very high risk
	Very high	Moderate risk	High risk	Very high risk	Very high risk	Very high risk

- calculation of resulting risk for each Security Goal / asset in matrix
- creation of risk analysis reports



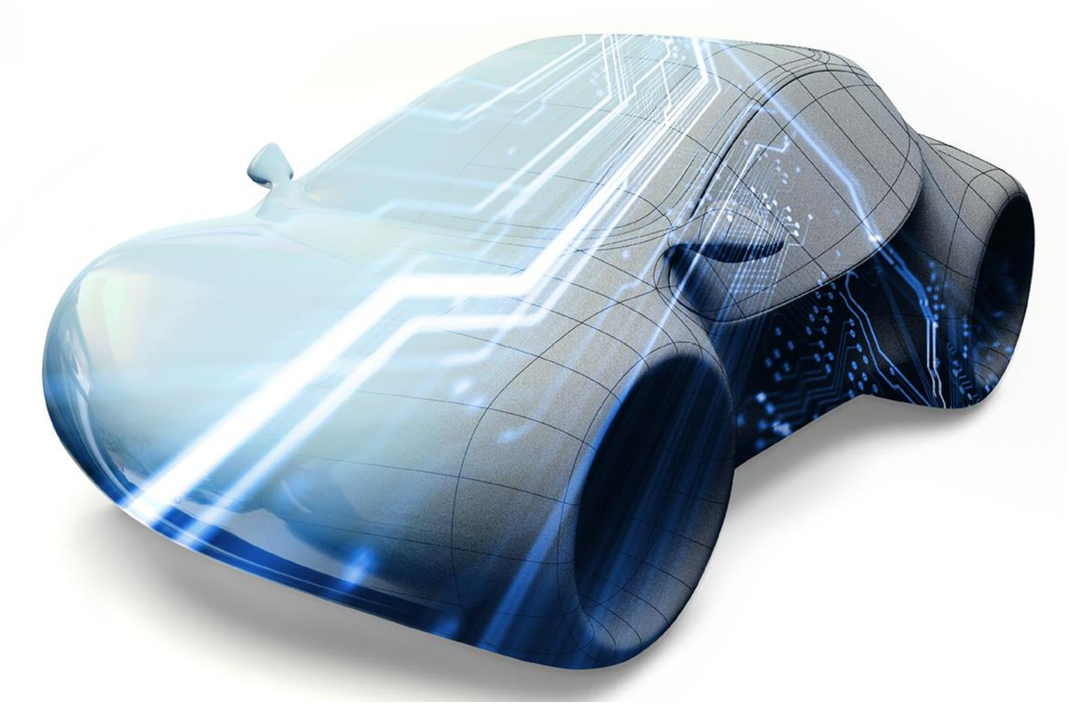
Risk Analysis in the Automotive Domain
Special Challenges

- Highly distributed system development (OEM, Tier 1, Tier 2, …)
- Impact of (semi-)autonomous vehicles
- Influence of changes during the life cycle
  - Periodical reevaluation of risk levels
  - Continuous update and tracking of system dependencies
  - Influence of system updates on security and safety
    - Remote software updates?
    - Status of certifications?
    - Selective deactivation of functions ?
- Automotive Responsible Disclosure (ARD)
- …

THANK YOU

FOR YOUR

ATTENTION !



Contact:

Dirk Leopold

leopold@itemis.de