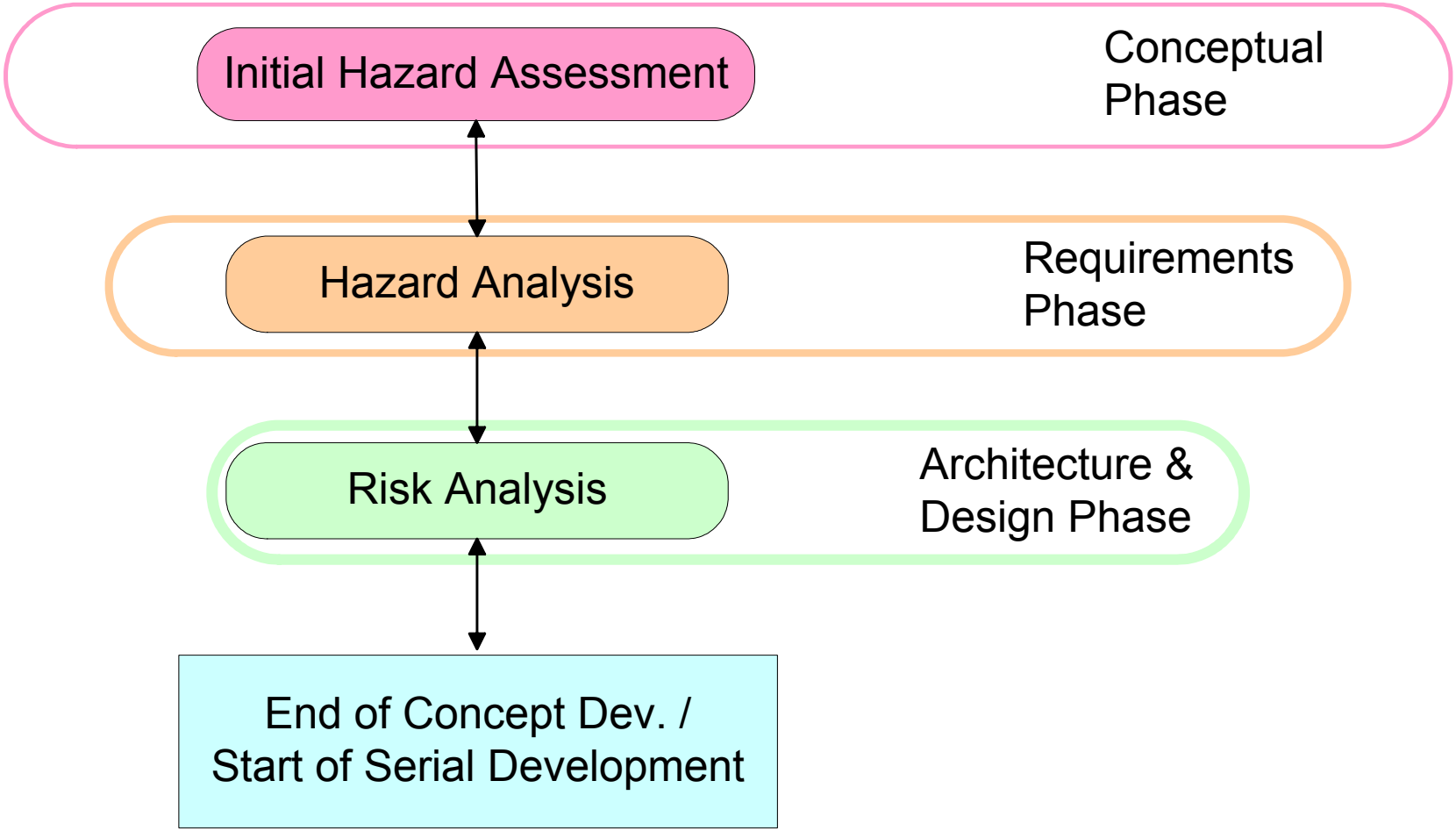
Introduction of Safety Process Elements in the (Automotive) Front Loading Phase

Dipl.-Ing. Ralf Westerkamp
Dipl.-Inf. Mirko Mrowczynski
eta_max space GmbH

Safety Process Elements in the Front Loading Phase



Content

- Introduction
- Safety Process Elements in Front Loading Phase
  - Motivation
  - Overview
- Methods and Tooling
  - **Initial Hazard Assessment**
  - **Hazard Analysis**
- Safety Process as Part of the Development Process
  - Interfaces
  - Safety Case

- Hands-on Presentation: Hazard Analysis
  - Method and Tool

The Safety Case in Automotive Systems

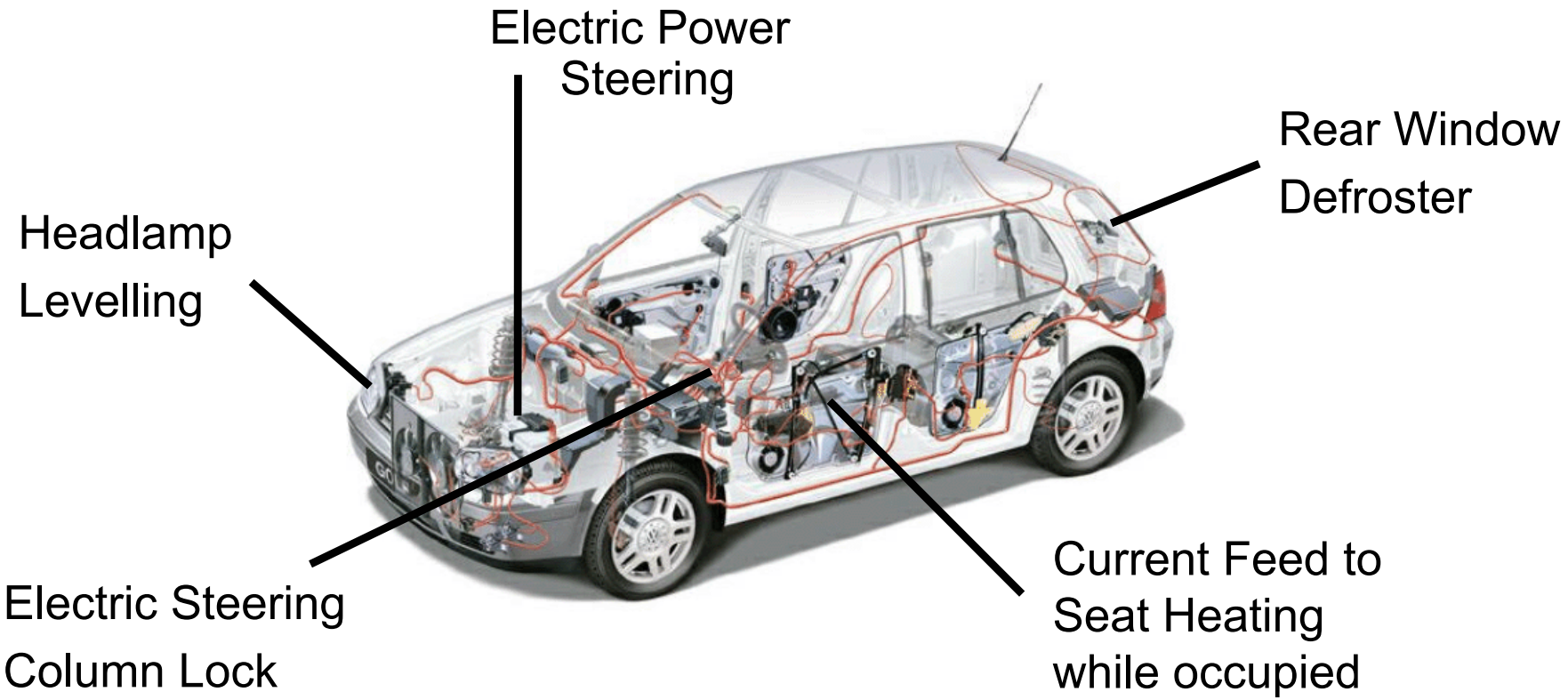
- Differentiated consideration of quite different E/E systems
  - differences w.r.t. criticality to be identified
  - adequate, adaptable treatment of more or less safety-relevant functions
- Large variety of existing functions motivates an initial filter
  → binary gate

- Normative guidelines are to be considered for safety-relevant functions
- "Global" standards need to be tailored
  → Synthesis of an "Automotive Standard"

- Life Cycle Requirements
  - safety requirements to be considered in the development process
  - systematic process monitoring of safety-relevant functions → Safety Plan

- Systematic and comprehensible definition of safety goals
  → classification into safety integrity levels (SIL)
  → derivation of safety requirements

Introduction



Initial / Preliminary Hazard Assessment

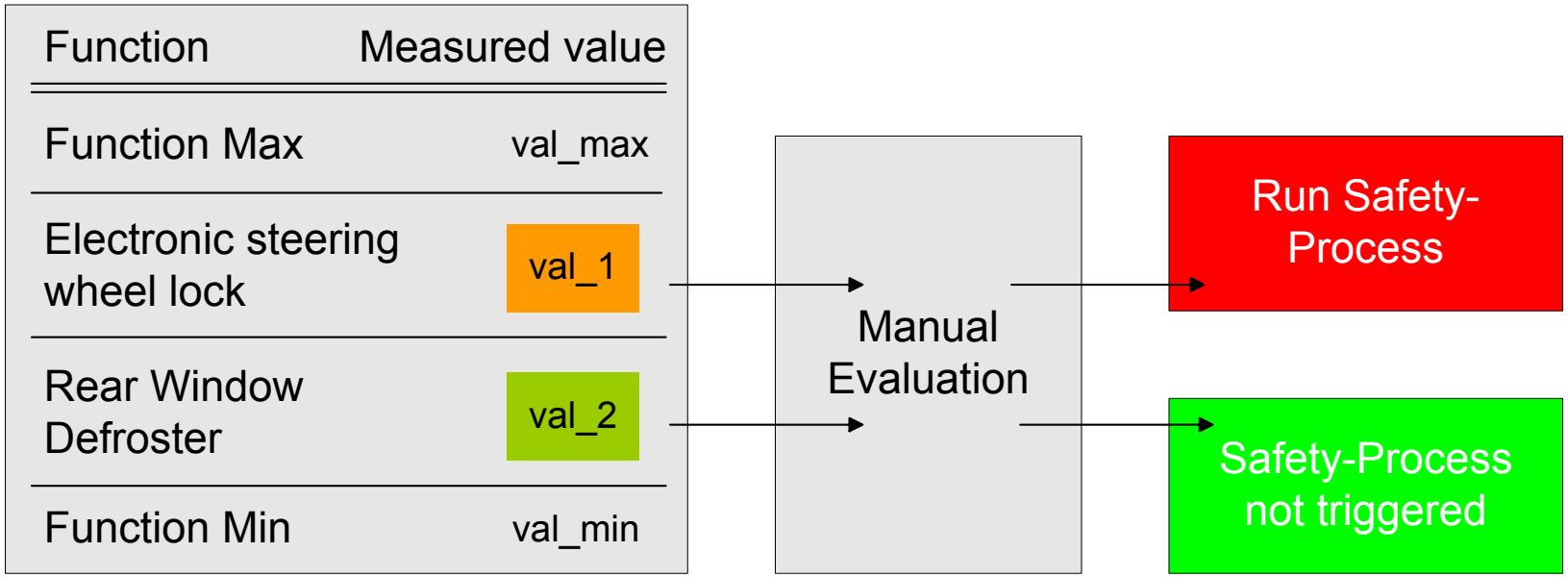
- Motivation
  - Large number of functions, more or less obvious w.r.t. safety relevance
  - Partially assessed, different level of detail
  - Goal: Unified assessment, simple application
- Relative assessment vs. absolute scale
- Basic Requirements / Input for the implementation
  - Functional Description
  - Tooling
  - Set of references in the same group of function (in the long-term)
- Individual Competence
  - Participants: Experts (of the considered function/functional context)
  - Moderator: methodological knowledge, cross-project consistency

Quality Function Deployment used for Hazard Assessment (excerpt)

Preliminary Hazard Assessment	Safety-related characteristics									
Category	**Increased risk of accident ..**		**Increased consequence of accident ..**		**Straight risk of injury**	**. .**	**Not field-proven**		**Evaluation**	
Criteria	.. durch Einfluss auf Belastung (Workload) für Fahrer	Einfluss auf Beschleuni-gungsverhalten des Fahrzeugs	.. durch Reduzierung der aktiven Sicherheit	.. durch Reduzierung der passiven Sicherheit			.. weil die Funktion neu ist	...		
Example for criteria	Belastung der Sinnesorgane, Notwendigkeit erhöhter Auf-merksamkeit oder anzuwen-dender Kräfte/ Momente	Bremsen, Gas, Liegenbleibe r	Ausfall der aktiven Sicherheits-systeme	Werkstoffe: Korrosion, Splittern, Brennen; Nichtauslösung Airbag	Radarstrahlung, Fensterheber, Airbag				**QFD**	**Manual Decision**
Electric Steering Column Lock								1...9	val_1	Yes
Rear Window Defroster								1...9	val_2	No
Function Max	9	9	9	9	9		9	9	val_max	Yes
Function Min	1	1	1	1	1		1	1	val_min	No

Triggering the Safety Process

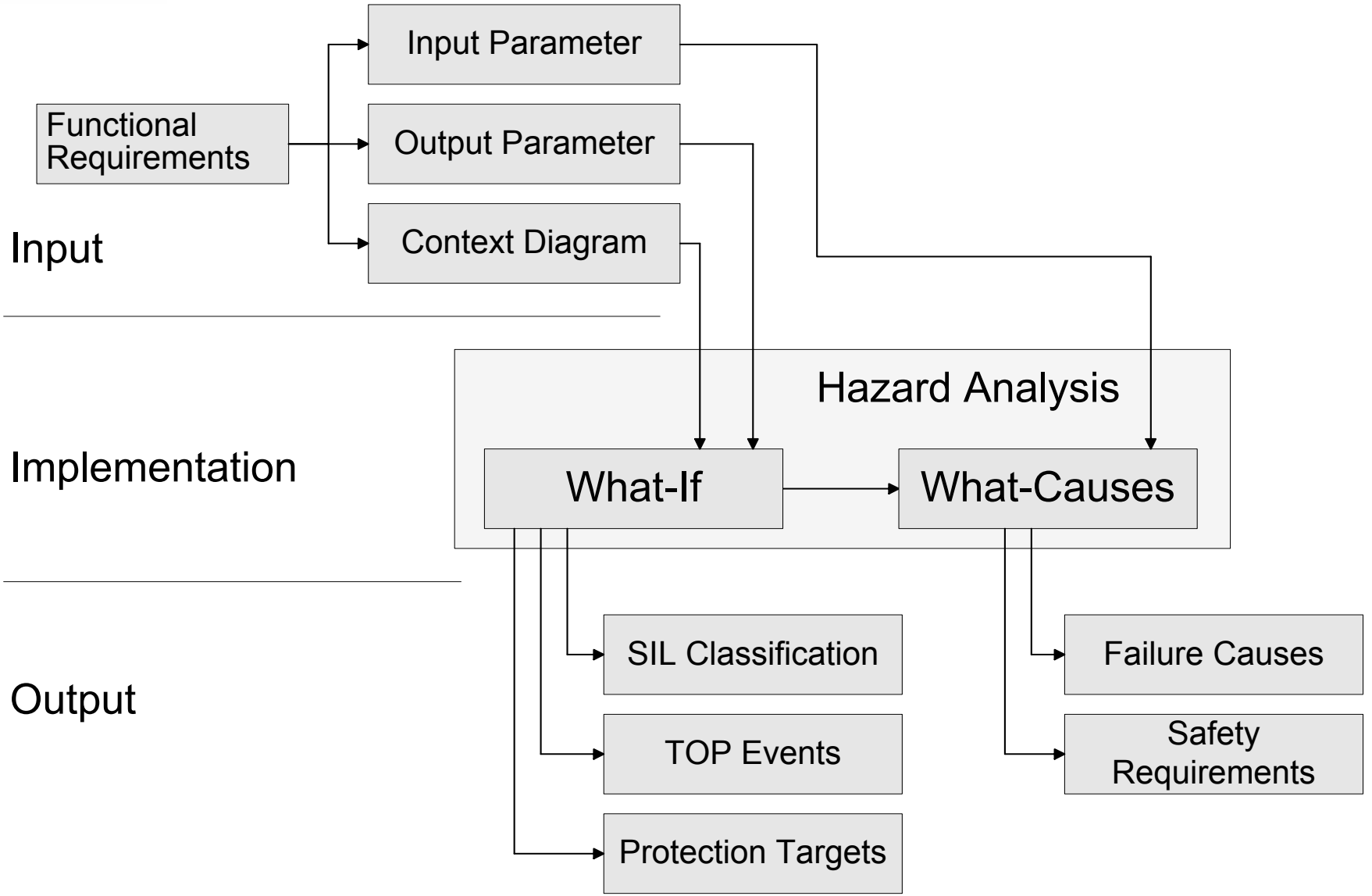
- Quantification of "gut feeling"
- Relative results, ranking, comparison between functions
- Deviation from average becomes visible
- Numerical result of QFD proposes relevance for safety process (limits defined)
- Final decision always manually by evaluation board (for each function)
- Reconsideration and triggering at later stage possible



Hazard Analysis

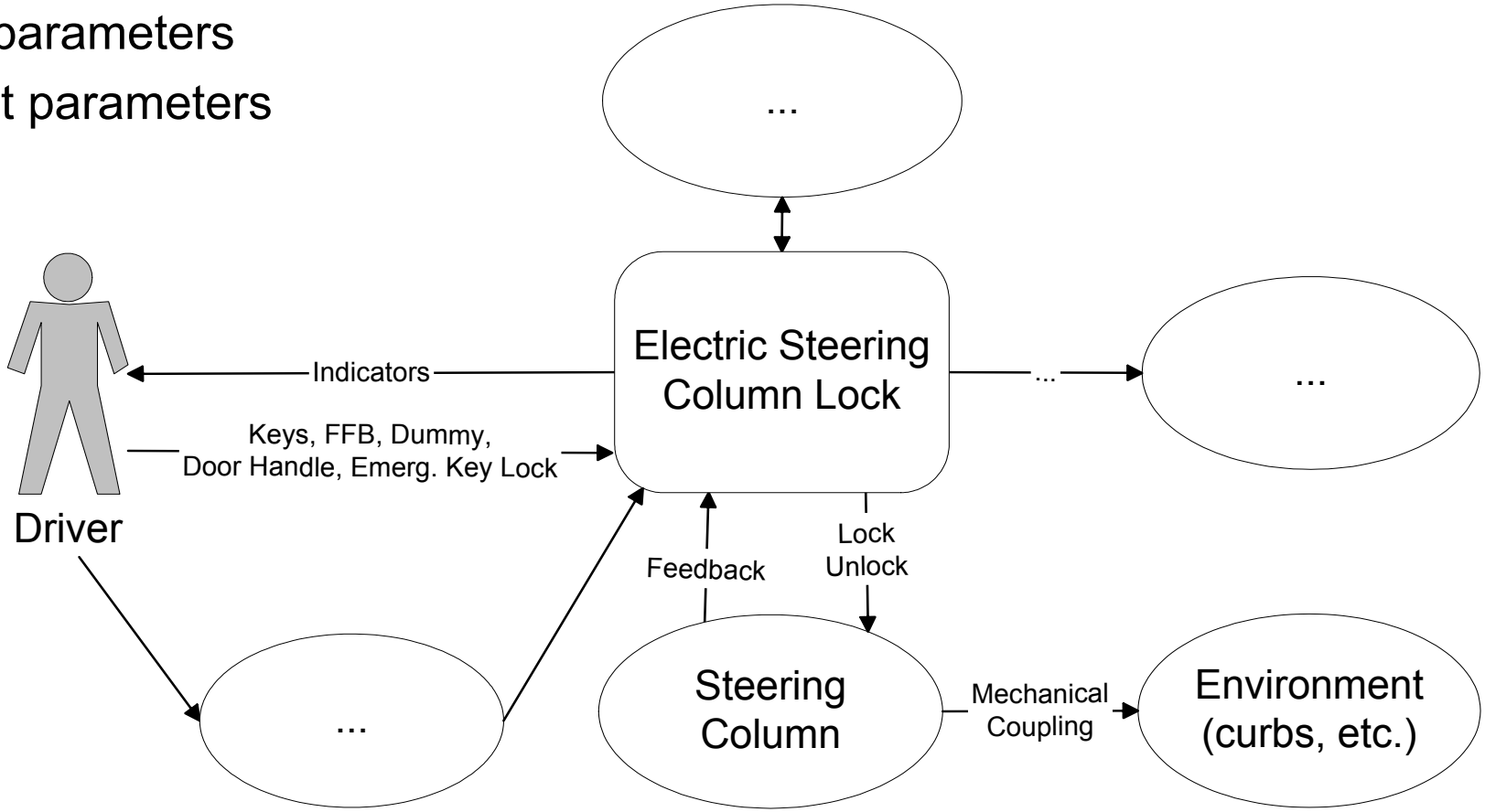
- Executed in the „Safety Process“, i.e. for safety-relevant functions
- Variety of possible methods, e.g.
  - HAZOP
  - WHAT-IF Checklist
  - FMEA, FTA
- Initial selection and lessons learned from first assessments lead to adaptation
  - Method "What-If / What-Causes“
  - Guide Words from HAZOP deemed helpful
  - Adaptation of COTS tool and template development
- Realisation in a workshop with function and safety experts
- Review
  - Integrity
  - Coherency with reference projects

Workflow in the Hazard Analysis



Hazard Analysis - Input

- Functional context (diagram)
- Input parameters
- Output parameters



Example: Excerpt of a context diagram for the electric steering column lock

Hazard Analysis – Following the What-If Checklist

Guide-Words (Template):

- More, Less,
- Unexpected,
- Reverse, ..

Situation within which a failure could occure

Risk Matrix and Criteria

What if

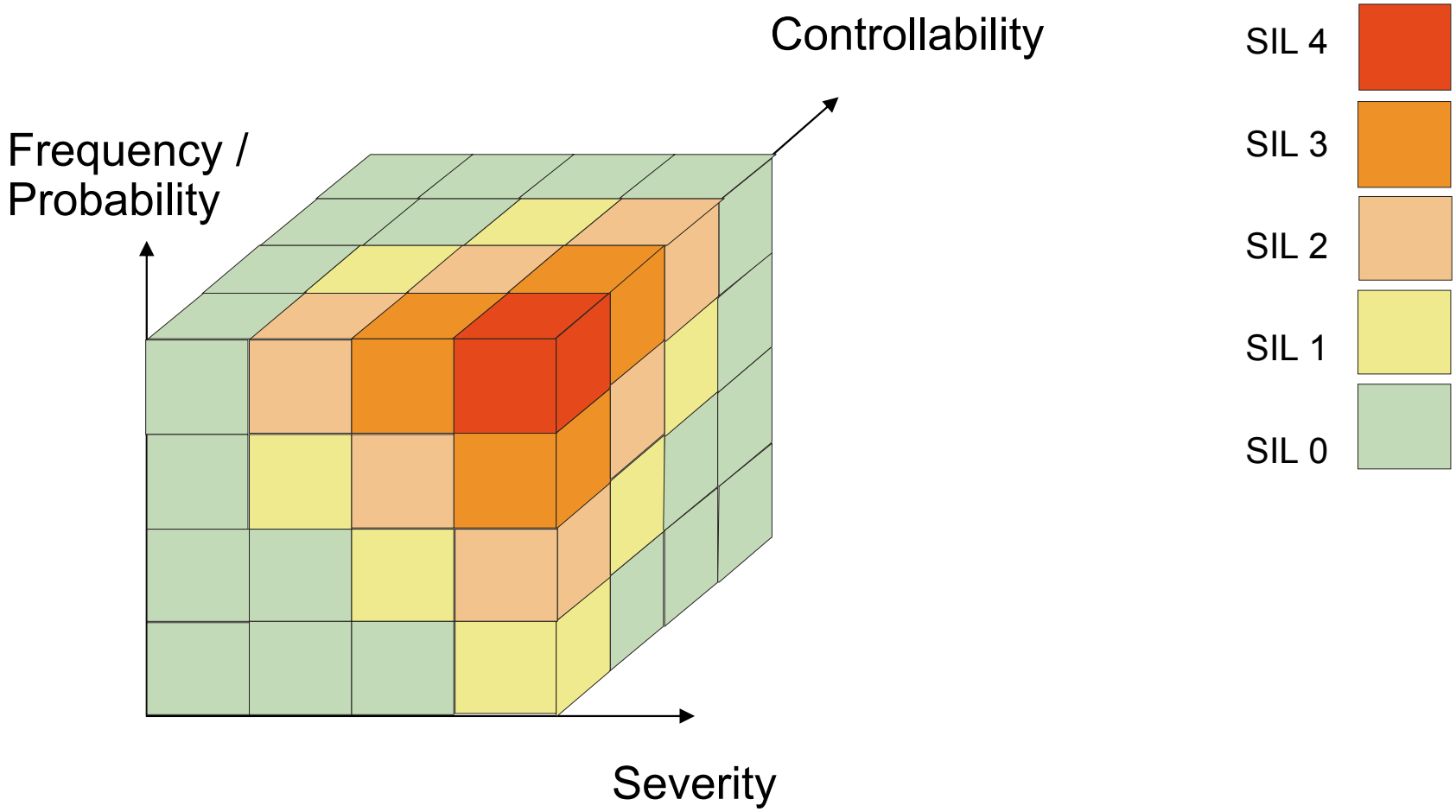
Funktion: 1. ELV

Parameter: 1. Verriegeln

Maximum:

Guide Word	Environment	Situation	Risk	Occurence	Frequency and exposure time risk parameter	Probability of the unwanted occurrence	Possibility of avoiding hazard risk parameter	Severity of consequence risk parameter	SIL
unerwartet	Fahren auf Landstrasse mit Gegenverkehr	beliebig	Lenksäule verriegelt unerwartet	Fahrzeug nicht mehr lenkbar		Häufig	Nicht beherrschbar	Hoch	SIL 4
	Fahrzeug angehalten vor Haltepunkt	beliebig	Lenksäule verriegelt unerwartet	Fahrzeug nicht mehr lenkbar, wird zum Verkehrshindernis		Häufig	einfach beherrschbar	Niedrig	SIL 0
immer aktiv	Fahrzeug abgestellt	beliebig	Lenksäule bleibt verriegelt	Fahrzeug nicht mehr lenkbar, wird zum Verkehrshindernis					

Hazard Analysis – Risk Matrix



Hazard Analysis – Top Events

- Identification of "Top (Critical) Events"
- Drives the definition of
  → Protection Targets
- Backward traceability to What-If
- Starting point for FTA, i.e. What-Causes

Top Events

Top Events			
Shortcut	Top Event	Protection Target	Place(s) Used
1. Verriegeln	1. ELV verriegelt während der Fahrt	Verriegeln während der Fahrt muß sicher verhindert werden.	Vorbedingungen: 1.1.1.1

Hazard Analysis – „What-Causes“

- Identification of causes for each event
- Safeguards
- Synthesis of safety requirements

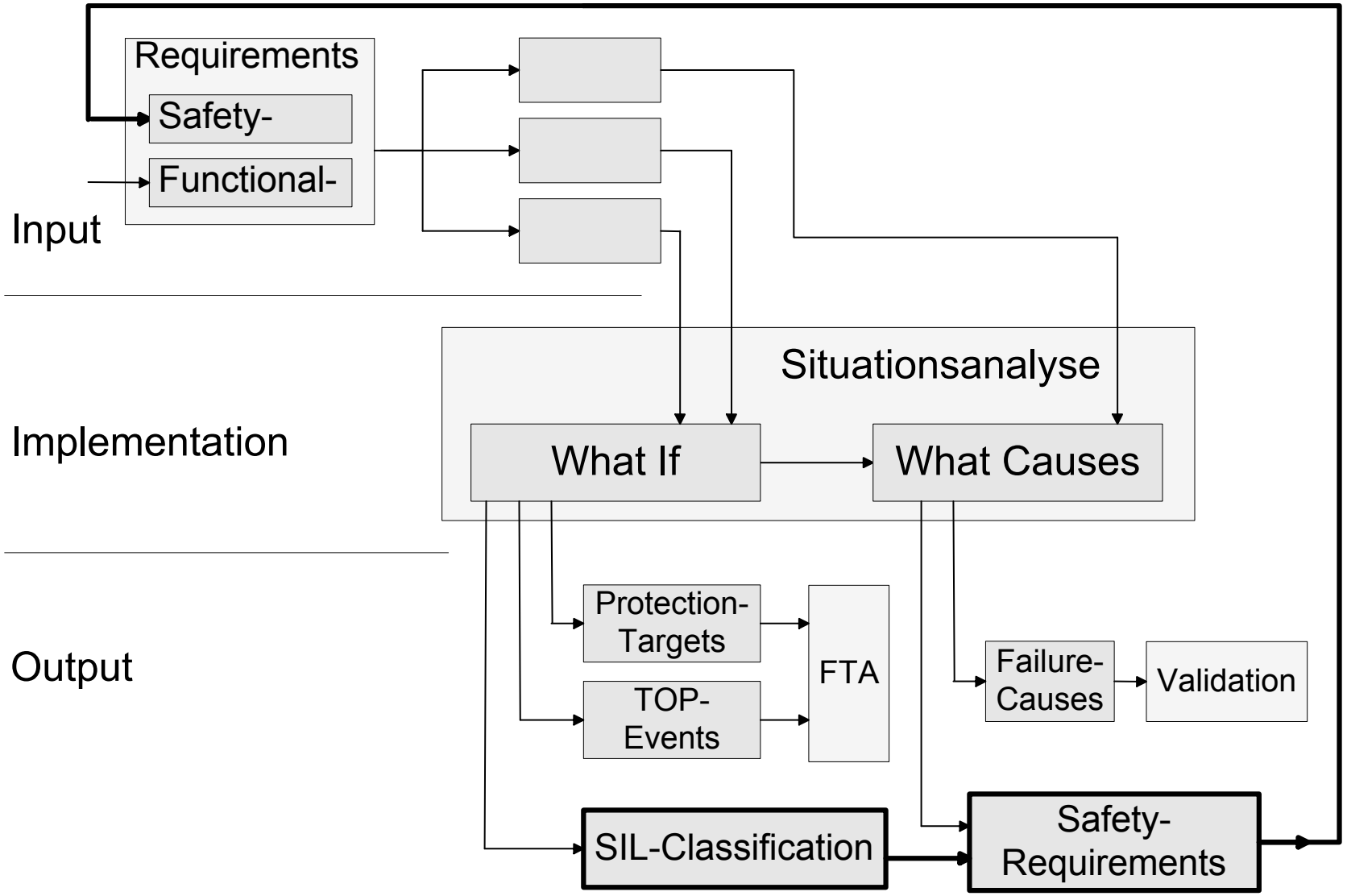
What Causes

Funktion: 1. ELV

Parameter: 1. Verriegeln; 2. Entriegeln; 3. Gelbe Warnlampe; 4. Rote Warnlampe

Parameter	Guide Word	Vorbedingung	Situation	Fehler	Fehlerkonsequenz	Risikoklasse	Ursache	Sicherheitsanforderungen	Top Events / Schutzziel
1. Verriegeln	unerwartet	Fahren auf Landstrasse mit Gegenverkehr	beliebig	Lenksäule verriegelt unerwartet	Fahrzeug nicht mehr lenkbar	SIL 4	Spannungsausfall ELV	1. Bei einem Spannungsausfall darf die ELV nicht verriegeln.	Verriegeln während der Fahrt muß sicher verhindert werden.

Iterative Development Process



Continuation of the Safety Process

- Governed by the safety plan
- Subsequent to the hazard analysis
  - Risk analysis
  - Transfer from requirements to architectural phase
  - Derivation of safety requirements from architectural elements
  - different methods
  - bridging the gap to the product's risk evaluation
- Transfer of process elements between OEM and supplier
  - definition of interfaces
  - transparency
- Verification and validation through the whole development process
- Acceptance and homologation

Summary

- Process Improvements
  - systematic
  - documentation
  - use of synergy
- Facilitates Repercussion Analysis
  - change management
  - identification of cost drivers
  - line of reasoning
- Proven in Project Application