Technische Universität Braunschweig

Institut für Regelungstechnik

www.ifr.ing.tu-bs.de/MOBILE, photo by Marcus Nolte

Evaluating High Voltage Safety Measures for an Experimental Full-by-Wire Vehicle Utilizing STPA

Torben Stolte, **Marcus Nolte**, Bernd Amlang, Markus Maurer
Technische Universität Braunschweig | Institute of Control Engineering
March 28, 2017

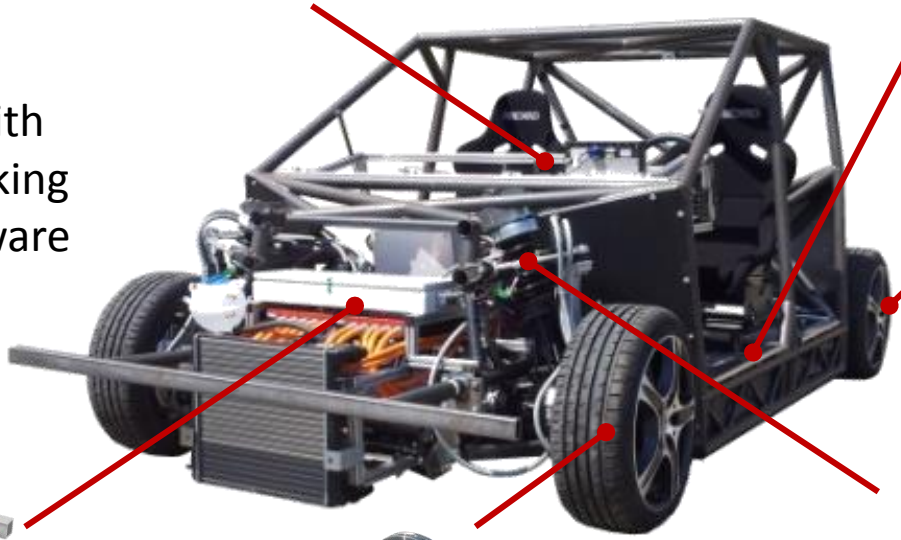
The Experimental Vehicle MOBILE

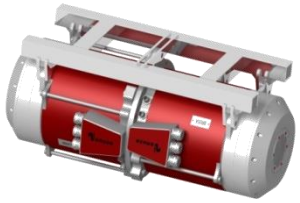
modular energy storage, voltage levels 360V, 48V and 12V

flexible human machine interface

double wishbone axle

development ECUs with time-triggered networking & fully accessible software





modular drive units at the front and the rear(~100kW per wheel)

electromechanic brake system

4x independent steering

Challenge High Voltage Safety

- maiden voyage summer 2013
- out-of-service in summer 2014 due to high voltage safety

Questions:

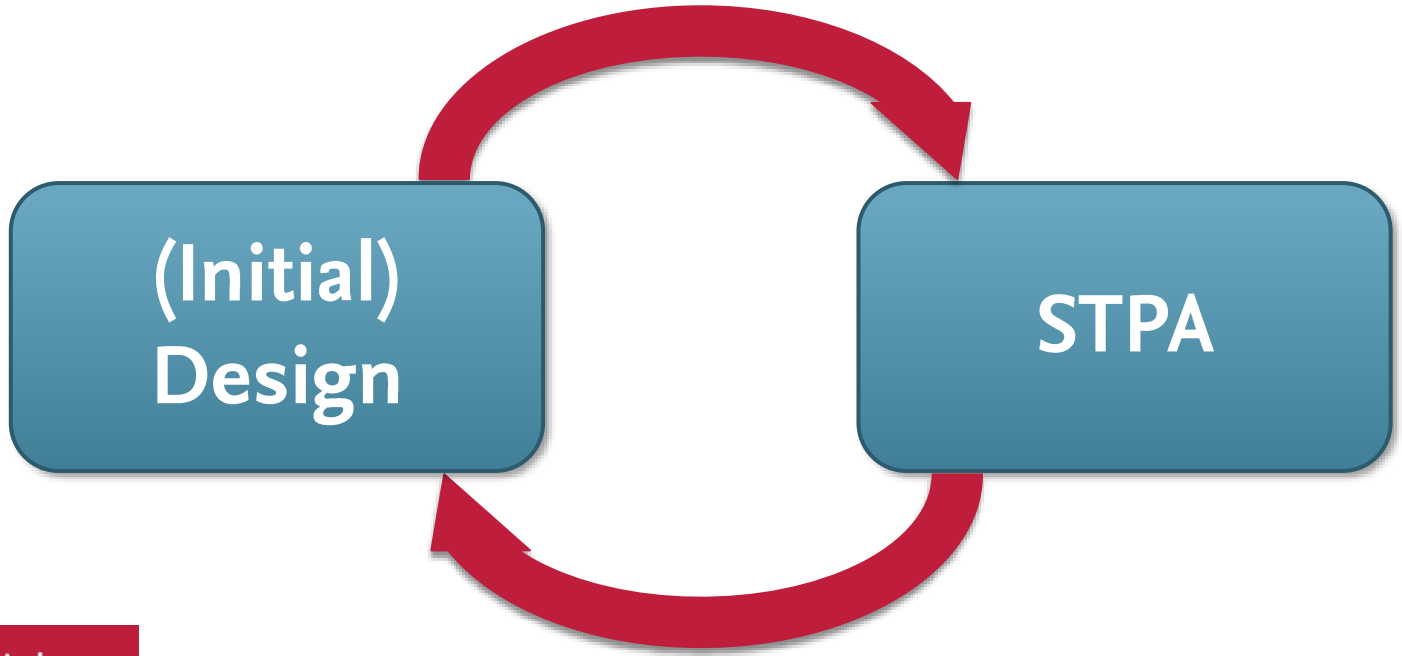
1. What must be done to ensure high voltage safety?
   ➔ several measures implemented
2. How can we evaluate implemented measures?
   ➔ STPA

Challenge High Voltage Safety

Why utilize STPA?

- little experience with high voltage safety
- systematic approach
- rethink high voltage safety from a different perspective

(as control problem)



What did we do?
Implemented Measures vs. STPA Safety Contraints

16	Monitoring	Feedback line of HV+ contactor not connected/not available	Not connected HV+ contactor feedback line must trigger open command to contactor	yes		
17	Monitoring	State of HV- contactor is wrongly read	Forcibly actuated feedback path for HV- contactor must be implemented	yes		
18	Monitoring	State of HV- contactor is unknown	HV- contactor feedback line must be conn	no	Check not included in work instructions	Plausibility check in software of co triggers failure as a not connected feedback equals open contactor
19			Unknown HV- contactor stat ger open command to contactor	no	not explicity implemented	Plausibility check in software of co triggers failure as a not connected feedback equals open contactor
20	Monitoring	Feedback line of HV- contactor not connected/not available	Not connected HV- cont edback line must trigger open command to contactor	yes		
21	Monitoring	State of precharge wrongly read	arge contactor must be activated		t prepared on ECU	
22	Monitoring	State of precha unknown	be connected		k instructions	
23			igger open command to contactor			
24	Monitoring	Feedback line not connected	k line must trigger open command to contactor			
25	Monitoring	Feedback of HV is wrong	t disable HV system		disconnect plug	not plugged in HV disconnect plug 12V supply for contactors
26			able HV system			
27	Tools	Tool's insulation			nted yet	Inspection before tool usage requi work instruction
28			Exchange of defect tool an ls that do have an unknown status	no	Scheduled, not implemented yet	Inspection before tool usage requi work instruction
29			Inspection of HV tools be	yes		
30	Tools	Tool not HV approved	Work instruction must pro n-HV-eligible tools	yes		
31			Training of users regarding safe ial consequences of using non-HV-eligible too	yes		
32	Tools	Covers not HV approved	Covers must be HV approved	yes		
33	Tools	Covers defect	All covers must be able to carry a grown-	yes		
34			Regular inspections of covers regarding defects	no		
35	Tools	HV gear not HV approved	Work instruction must enforce use of HV gear (glasses, gloves)	yes		
36			Training of users regarding safety and potential consequences of using non-HV-eligible tools	yes		
37			Work instruction must require dual control of HV gear completeness before start of works on HV system	no		
38	Tools	HV gear defect	Regular inspection of HV gear	no	scheduled, not implemented yet	Inspection before each usage requ work instruction
39			Exchange of defect gear and gear that do have an unknown status	no	not implemented	
40			Inspection of HV gear before usage	yes		

STEP1 | STEP2 | Contexts

BEREIT

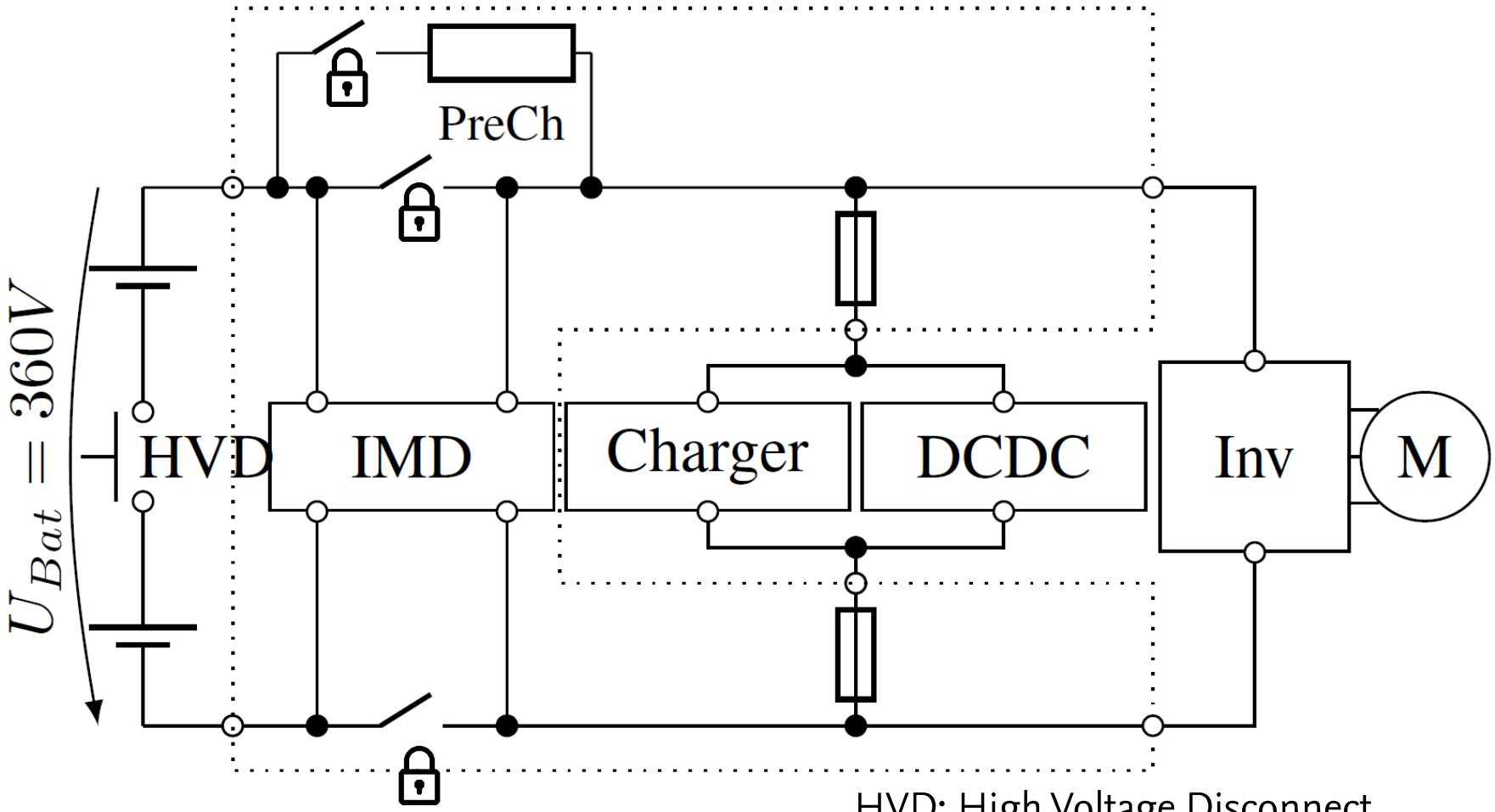
(Initial) Design

STPA

Outline

- Motivation and Project Context
- High Voltage System and High Voltage Measures
- Applying STPA
  - Step 0: Process Model and Control Structure
  - Step 1: Identification of (Unsafe) Control Actions
  - Step 2: Causal Analysis
- Conclusion

MOBILE‘s High Voltage System



HVD: High Voltage Disconnect
IMD: Insulation Measurement Device

Established High Voltage Safety Measures
Hazard Analysis

Hazard	Risk*	Safety Goal
Electrical perfusion of a human body	+++	Protection against electric shock
Electrical arc	+++	Protection against arc eye and burn
Electromagnetic radiation	+	Avoidance of exposure of implants (e.g. cardiac pacemaker) to electromagnetic radiation
Fire	+	Avoidance of fire destructing the vehicle, other appliances, and buildings

* +++ high, ++ medium, + low

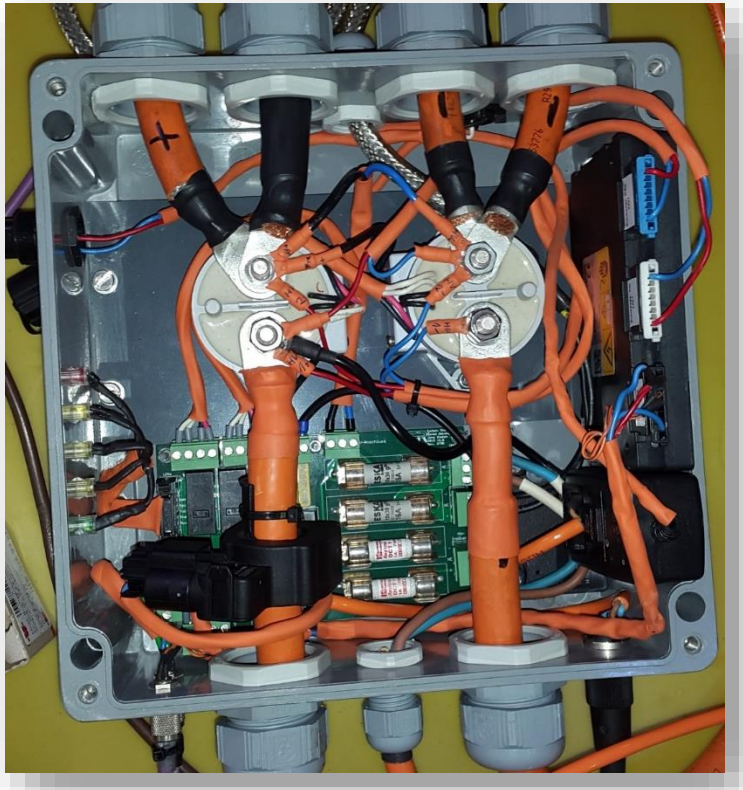
Hazards:

- **Low insulation resistance** between HV-carrying parts
- **HV-carrying** parts are **touchable**
- Different **HV levels** can be **shorted**
- Exposure of implants to electromagnetic radiation
- Undesired vehicle dynamics

Established High Voltage Safety Measures

Technical Measures (selection)

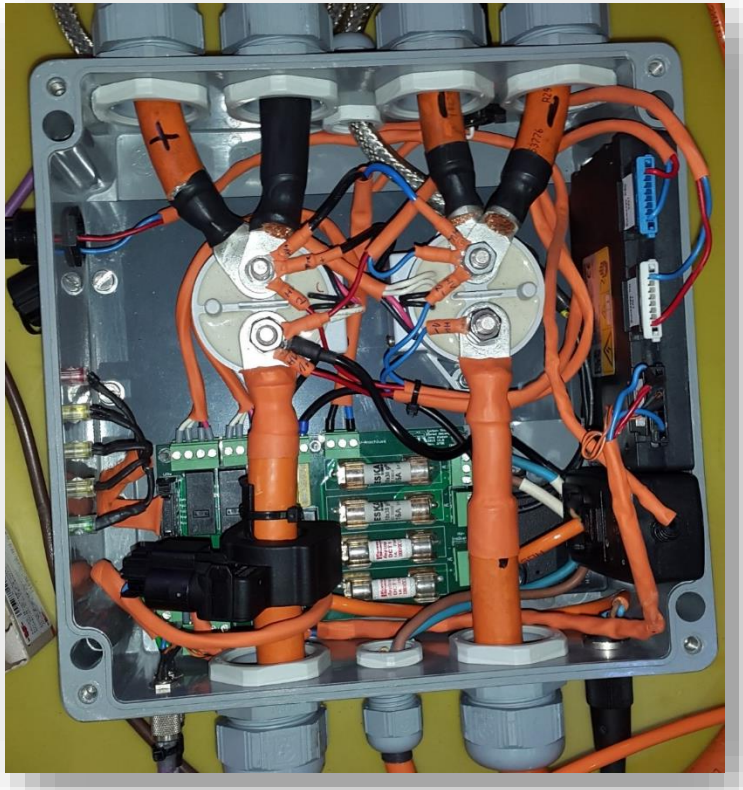
- redesign of contactor box
- pilot line
- continuous measurement of insulation resistance
- warning in MOBILE‘s HMI
- …



Established High Voltage Safety Measures

Organizational Measures

- purchase of **HV equipment**
- **HV-Trainings** of co-workers
- detailed **work instructions**
  - non-HV works
  - work on the HV system
  - work on non-HV battery

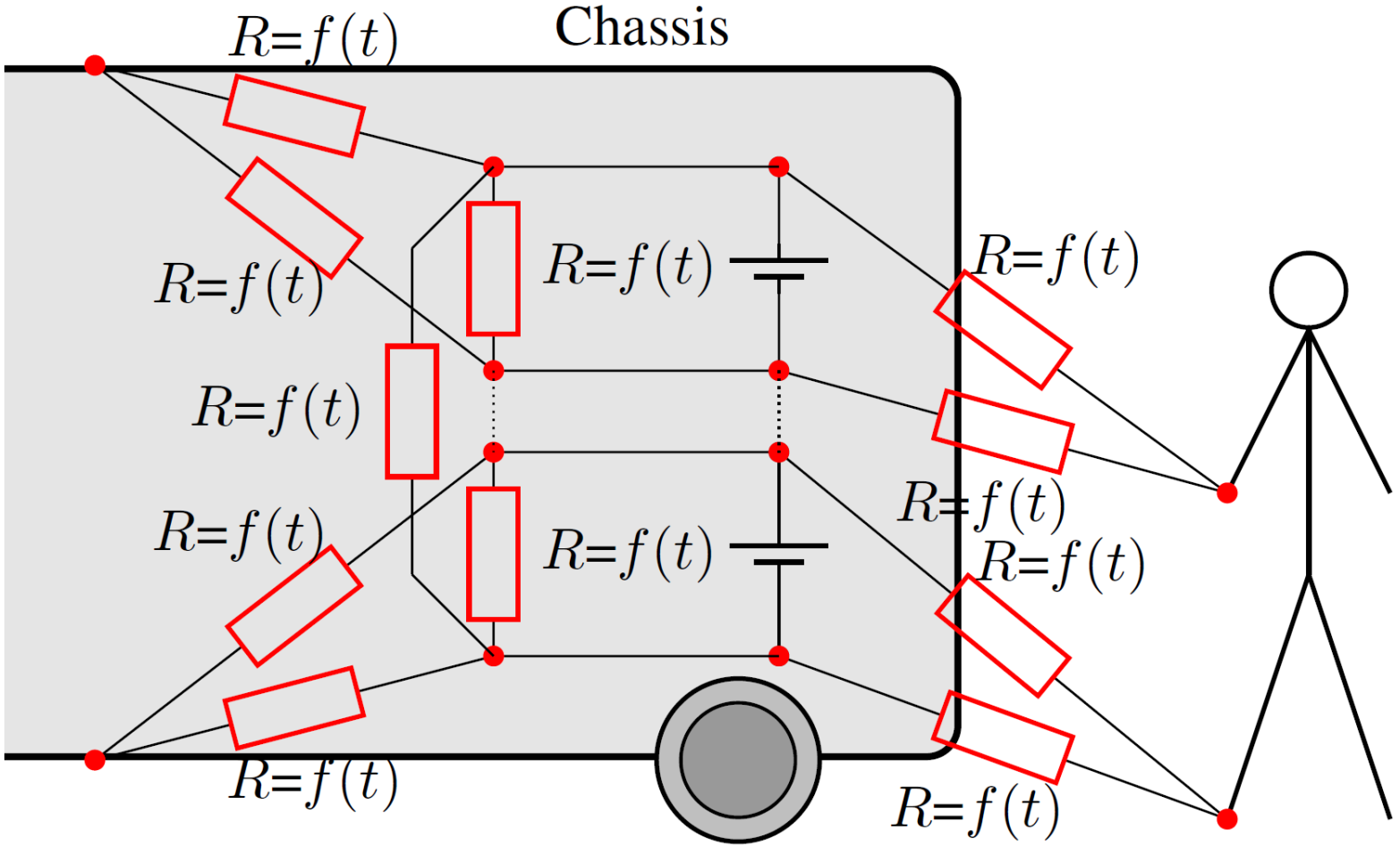


Outline

- Motivation and Project Context
- High Voltage System and High Voltage Measures
- Applying STPA
  - Step 0: Process Model and Control Structure
  - Step 1: Identification of (Unsafe) Control Actions
  - Step 2: Causal Analysis
- Conclusion

Applying STPA

Process Model: What is the actual controlled process?

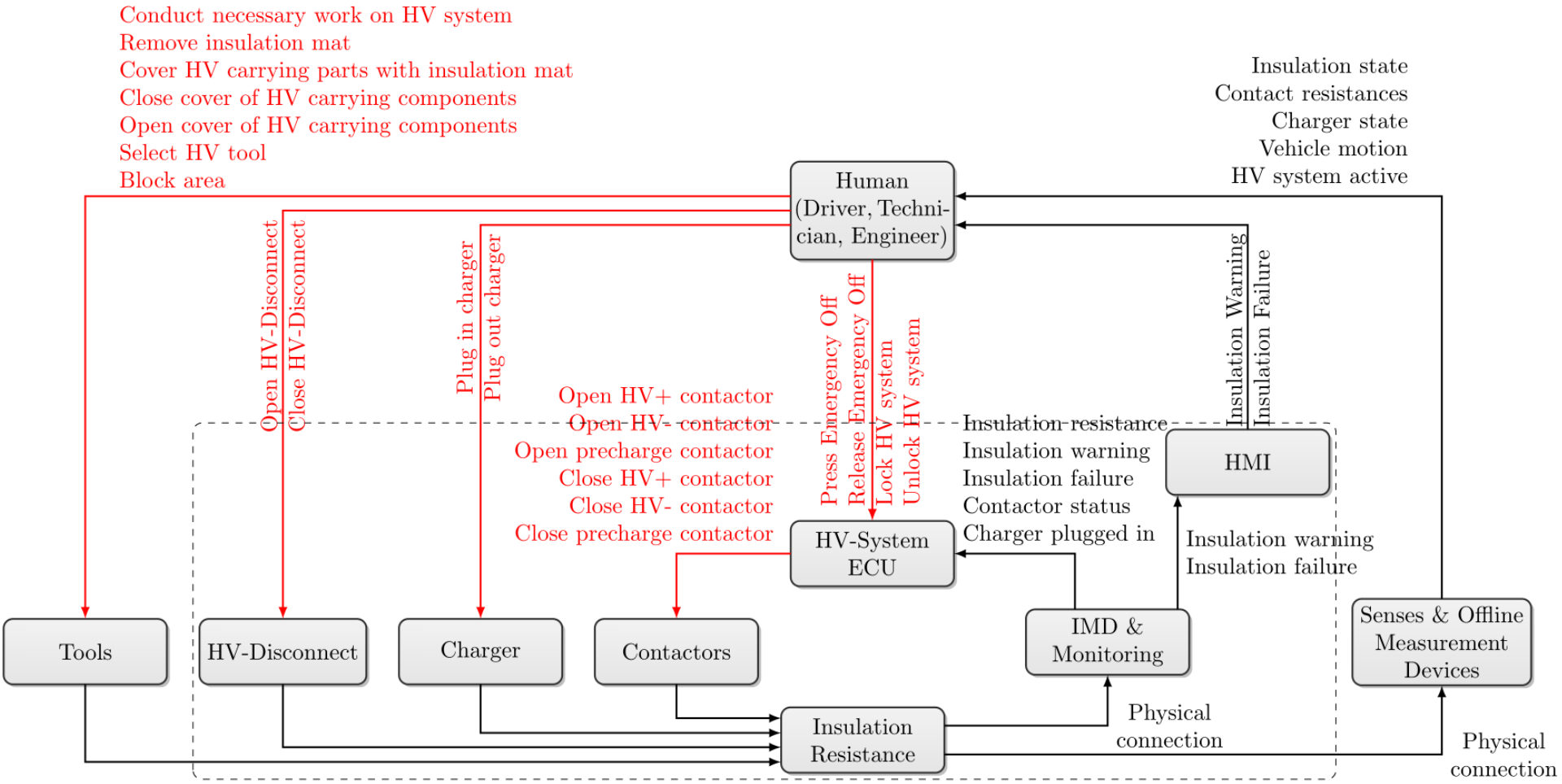


Applying STPA
Identification of Control Structure

Questions

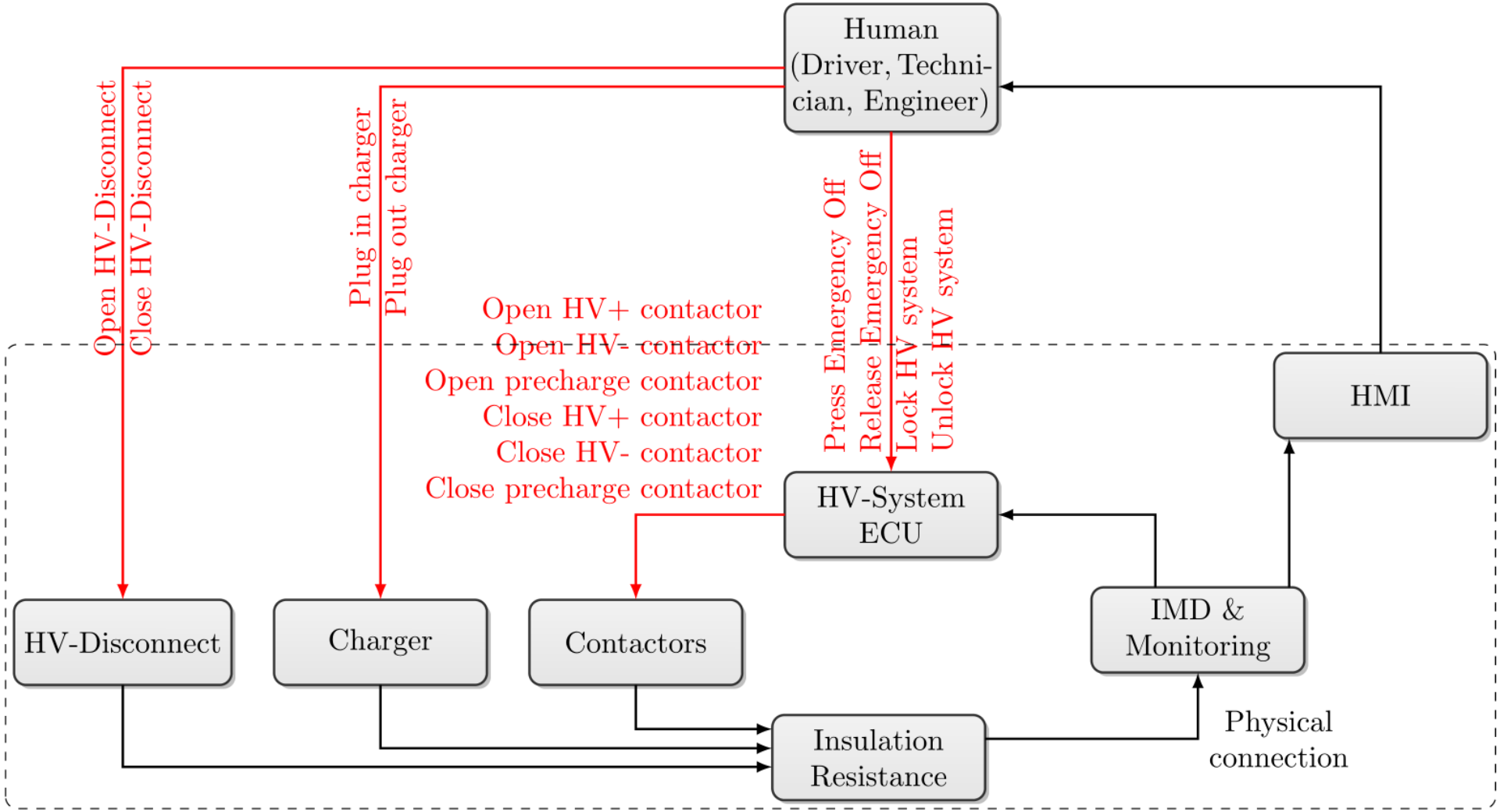
- **How do we model tool usage?**
  ➔ actuator
- **What is a suitable level of granularity?**
  ➔ as high level as possible, as detailed as necessary
- **Can work instructions be considered as superimposed controllers themselves or control algorithms of the human (e.g. technician)?**
  ➔ control algorithm

Applying STPA
Overall Control Structure



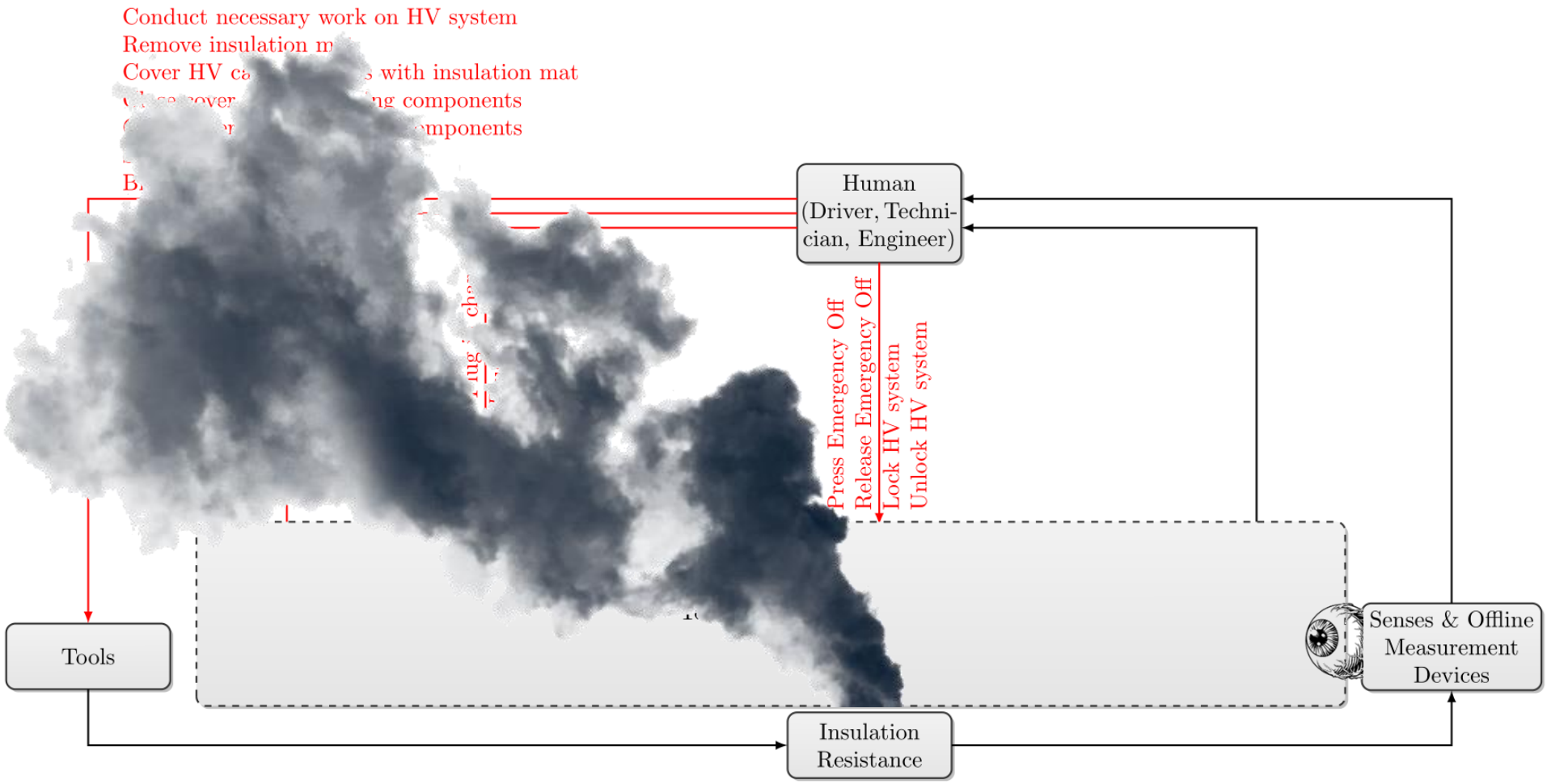
IMD: Insulation Measurement Device

Applying STPA
Control Structure of Technical System

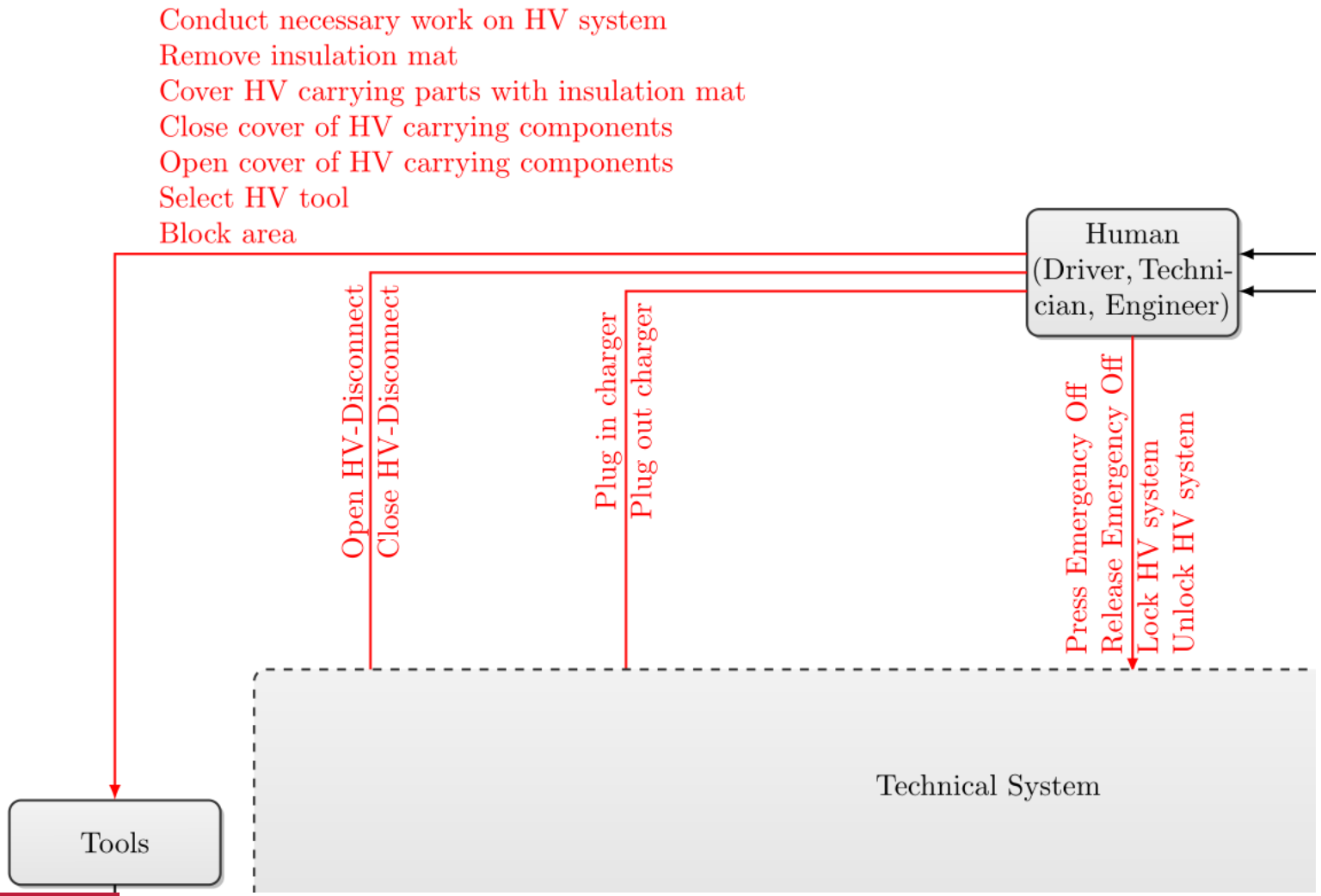


IMD: Insulation Measurement Device

Applying STPA
Control Structures of „Human“ System



Applying STPA
Control Structures of „Human“ System



Applying STPA
Contexts

Human

- **HV system**
  - Power sinks active
  - Power sinks not active
  - Unknown
- **Insulation**
  - No insulation failures present
  - Insulation failure present
  - Unknown
- **Vehicle velocity**
  - Moving
  - Standstill
- **Charger**
  - Connected
  - Not connected

HV System ECU

- **HV system**
  - Power sinks active
  - Power sinks not active
  - Unknown
- **Insulation**
  - No insulation failures present
  - Insulation failure present
  - Unknown
- **Vehicle velocity**
  - Moving
  - Standstill
  - Unknown
- **Charger**
  - Connected
  - Not connected
  - Unknown

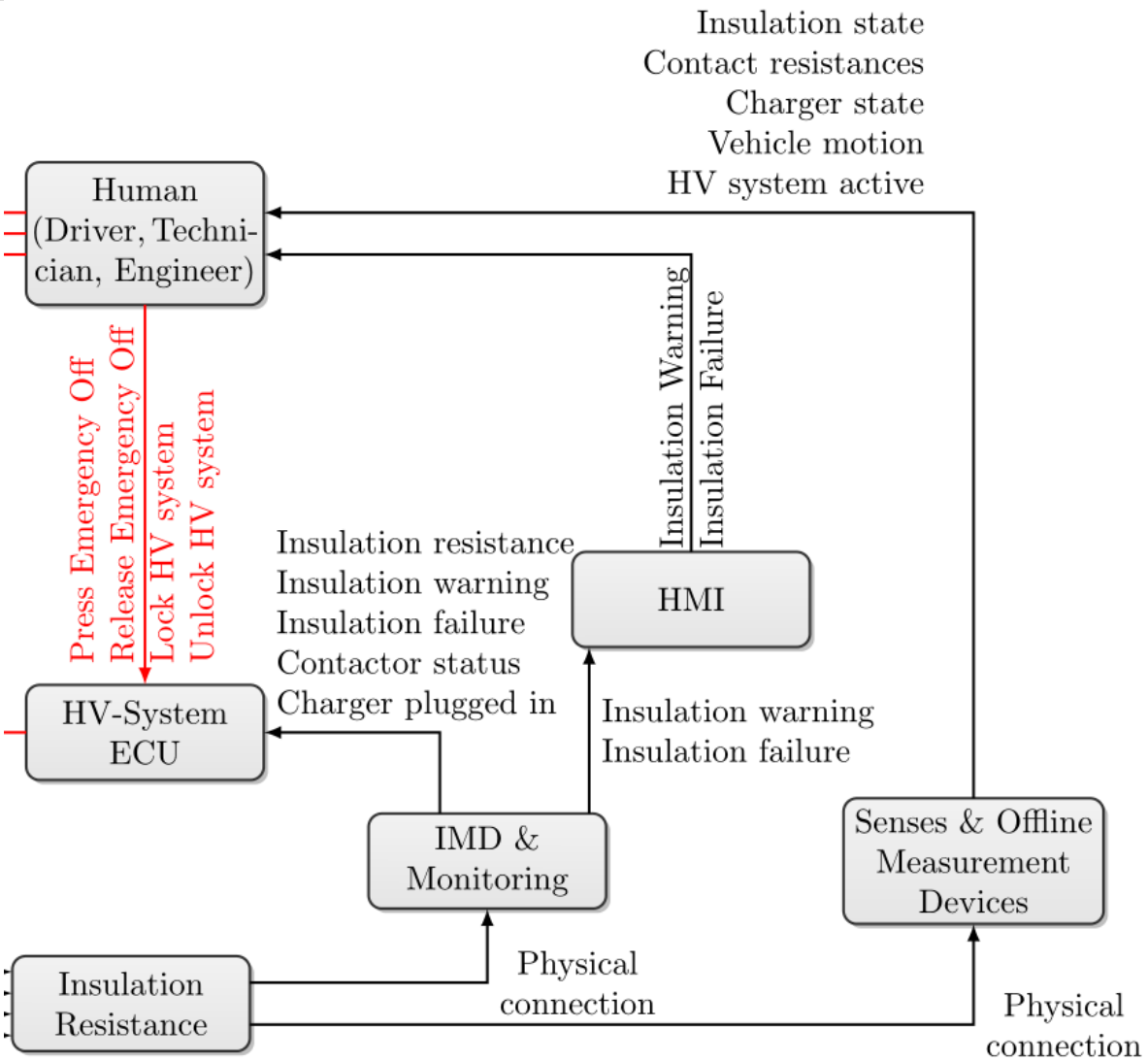
Applying STPA
STEP 1

- **44** Unsafe Control Actions and Safety Constraints
- **38** Safety constraints already implemented
- **6 Safety constraints not implemented!**

Examples

- **HV disconnect must kept closed** when vehicle is driving
- Only **HV approved tools** in blocked area allowed
- **Lock (key switch) of the HV system** has an important role (originally implemented to prevent misuse)

Applying STPA
Step 2: Control Structure - Feedback



IMD: Insulation Measurement Device

Applying STPA
STEP 2

- **46** causal factors
- **74** additional safety constraints
- **51** implemented

- **9 not implemented**, e.g.

  ➔ no **monitoring of precharge contactor**

- **14** not implemented but **reasoned safe**, e.g.
  - **unknown HV+ contactor state** must trigger open command to contactor
    - not explicitly implemented
    - **BUT: Plausibility check in software** of controller triggers failure as a not connected contactor feedback equals open contactor

Outline

- Motivation and Project Context
- High Voltage System and High Voltage Measures
- Applying STPA
  - Step 0: Process Model and Control Structure
  - Step 1: Identification of (Unsafe) Control Actions
  - Step 2: Causal Analysis
- Conclusion

Conclusion

Thorough thinking about HV safety from a totally different perspective

- general insights
  - STPA proven helpful
    - **important role of intensive training** is emphasized (before: necessary evil)
    - **reflection** on importance of scheduled measures (Do it!)

Conclusion

Thorough thinking about HV safety from a totally different perspective

- technical insights
  - **HV lock** is not only a feature for operational safety but also HV safety
  - HV safety and operational safety are **interconnected**
    (e.g. driver can lock HV system during drive (undesired vehicle dynamics)

- TODOs
  - so far **only high level analysis**
    - beyond STPA:
      particularization of **technical implementation** needed

Thank you for your attention! Questions?

Marcus Nolte
nolte@ifr.ing.tu-bs.de
+49 531 391 3827

Torben Stolte
stolte@ifr.ing.tu-bs.de
+49 531 391 3862