Functional Safety/ SOTIF & Safety for Automated Driving

NAVIGATING THROUGH STANDARDS COMPLEXITY: A SIDE BY SIDE STANDARDS COMPARISON AND OVERVIEW OF REQUIREMENTS OF ISO 26262 AND SOTIF

November 30th, 2021

SGS TÜV SAAR

SGS

SGS at a glance

Nº1
WORLD LEADER in Testing, Inspection, Certification

94,000
EMPLOYEES

2,600
OFFICES AND LABORATORIES

Headquarters in Geneva, Switzerland

SGS-TÜV SAAR GMBH – “SGS-TÜV”

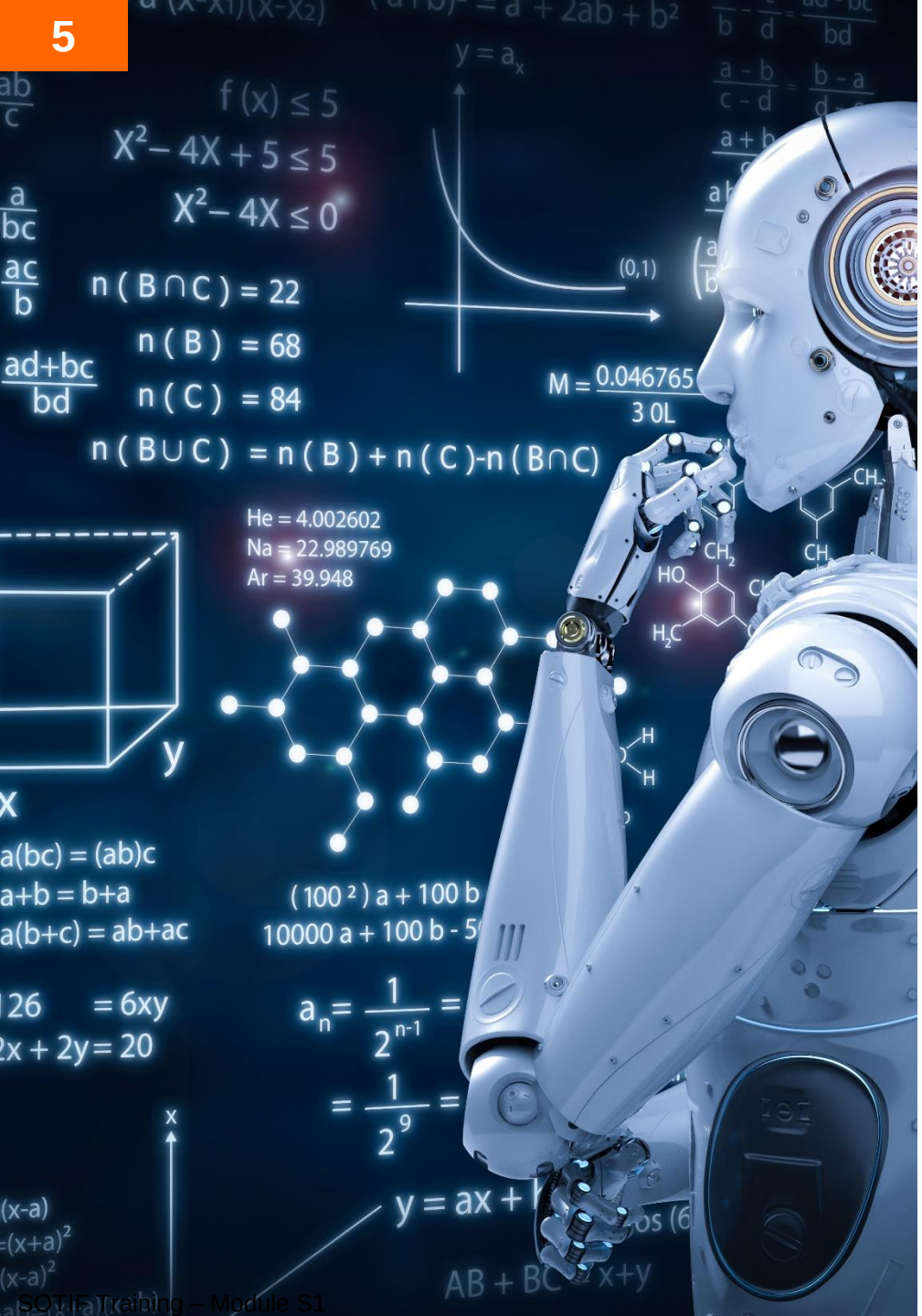
- Joint-venture between SGS Group and TÜV Saarland e.V., Germany
- Global Competence Center Functional Safety within SGS Group
- TIC world market leader in Functional Safety Automotive & Semiconductor
- Leading Personal certification supplier Automotive & Semiconductor (> 5,000 graduates, > 25,000 persons trained)
- Accredited laboratory & inspection body for Functional Safety & Cyber Security in acc. with ISO/IEC 17020/ 17025
- Member of relevant standardization committees like for ISO 26262, ISO/SAE 21434, IEEE P2851, ISO TS 5083 & ISO PAS 8800

For more info, please go to www.sgs-tuev-saar.com/fs

GLOBAL NETWORK FUNCTIONAL SAFETY

- Global Competence Center
  - Headquarters in Munich / Germany
  - Branch offices in Dortmund and Stuttgart
- International branches
  - China
  - Finland
  - Japan
  - Korea
  - Taiwan
- Cooperation partner in the USA
- Global network with 90+ experts

For more info, please go to
www.sgs-tuev-saar.com/fs



AGENDA

1. **Motivation**
2. Introduction into SOTIF and Functional Safety
3. Overview and organization of SOTIF activities – Management of SOTIF wrt. Functional Safety
4. SOTIF and AI

[**source:** https://www.theverge.com/2020/9/16/21439354/uber-backup-driver-charged-autonomous-self-driving-car-crash-negligent-homicide]

SAFETY OF AUTOMATED DRIVING FUNCTIONS – INCIDENTS (1)

- **Uber crash – March 2018:**
  - It is believed to be the first fatal collision of an automated driven vehicle
  - Investigators have analyzed that the vehicle recognized the person with the bicycle but did not react properly by braking the car → **“false negative”**
  - The “safety-driver” also did not react because she was distracted (head downwards) – She has been charged with negligent homicide in 2019

driver of the Tesla Model S said she was using Autopilot

[**source:** https://www.consumerreports.org/autonomous-driving/nhtsa-safety-defect-investigation-tesla-autopilot-crashes-a6996819019/]

SAFETY OF AUTOMATED DRIVING FUNCTIONS – INCIDENTS (2)

- **Tesla crash – March 2018:**
  - Autopilot was activated – Driver shall always be ready to drive the car by observing the “Automated Driving System”
  - Driver was using his phone while driving and did not focusing on the traffic Crash data showed that the driver failed to react in the moments before the crash, and the phone was playing a video game at the time of impact
  - The NTSB [1)] concluded that the car steered itself toward a barrier where a left-hand exit led off the highway → **“foreseeable misuse / misleading product definition”**

[1)] NTSB = **N**ational **T**ransportation **S**afety **B**oard

SOTIF INTENTIONS

- Automated driving is not a matter of “if” furthermore it is a matter of “when”
- With automated driving, there will be an impact on nowadays vehicle architectures – This includes for example:
  - new technologies with new or changing risks which are currently not known completely
  - increase of complexity

Functional **Sa**fety and **S**afety **O**f **T**he **I**ntended **F**unctionality, based on the standards ISO 26262 and ISO 21448 provide methods and tools to cope with coming requirements.

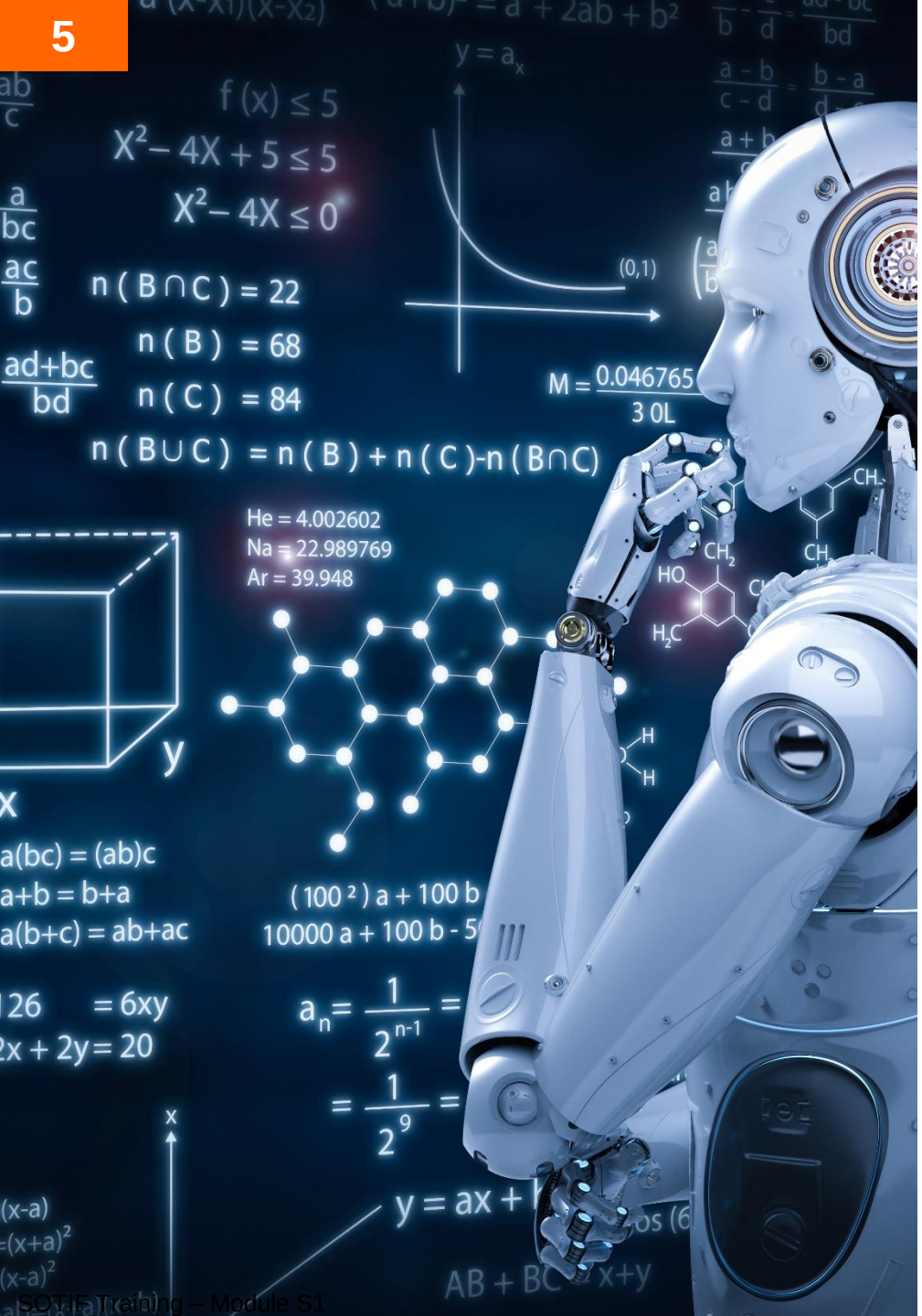
[picture - Detroit: Become Human – video game – Quantic Dream]

LEVELS OF DRIVING AUTOMATION

[ISO DIS 21448; table 2 + SGS-TÜV additions]

Dynamic Driving Task (DDT)					
SAE Level	**Name**	**Lateral & longitudinal vehicle motion control** performed by	**"Object and Event Detection Response" (OEDR)** performed by	**DDT Fallback** (in case of a loss of the automated driving function)	Availability of **"Operational Design Domain" (ODD)**
0	No driving automation	Driver	Driver	Driver	Not available/ applicable
1	Driver assistance	Driver & Vehicle system/ function	Driver	Driver	Limited[1] available
2	Partial driving automation	Vehicle system/ function	Driver	Driver	Limited[1] available
3	Conditional driving automation	Vehicle system/ function	Vehicle system/ function	Handover of control to "prepared" drivers	Limited[1] available
4	High driving automation	Vehicle system/ function	Vehicle system/ function	Vehicle system/ function	Limited[1] available
5	Full driving automation	Vehicle system/ function	Vehicle system/ function	Vehicle system/ function	Unlimited available

[1]Limited, based on the necessary ODDs for the respective automated driving function/ DDT



AGENDA

1. Motivation
2. **Introduction into SOTIF and Functional Safety**
3. Overview and organization of SOTIF activities – Management of SOTIF wrt. Functional Safety
4. SOTIF and AI

DEFINITIONS – SOTIF VERSUS FUNCTIONAL SAFETY ?

- **Safety Of The Intended Functionality [ISO DIS 21448, clause 3]**

*"Absence of unreasonable risk due to **hazards** resulting from **functional insufficiencies** of the **intended functionality** or its implementation."*

***Hazard** = potential source of harm caused by the hazardous behavior of the system*

***Functional insufficiencies** = insufficiency of specification (e.g., incompleteness) or performance limitation (e.g., of technical capabilities) of the intended functionality*

***Intended functionality** = Specified function on vehicle level*

- **Functional Safety [ISO 26262-1]**

*"Absence of **unreasonable risk** due to **hazards** caused by **malfunctioning behavior** of **E/E systems**."*

***Unreasonable risk** = risk, judged to be unacceptable in a certain context according to valid societal moral concepts*

***Hazards** = potential source of harm caused by malfunctioning behavior of the item*

***Malfunctioning behavior** = failure or unintended behavior of an item with respect to its design intent*

***E/E systems** = system that consists of electrical or electronic elements, including programmable electronic elements (at least a set of sensors + controller + actuator)*

SOTIF is inherently a part of Functional Safety – Therefore SOTIF/ ISO DIS 21448 is the logical complement to functional safety as specified in ISO 26262.

DEFINITIONS – CAUSES OF UNREASONABLE RISK

- **Functional insufficiencies at vehicle level – ISO 21448**
  - **Insufficiency of specification e.g.,**
    - incompleteness of environmental specification (e.g., temperature areas)
    - incorrect specification of the maximum vehicle speed or vehicle weight
  - **Performance limitation e.g.,**
    - limited and not considered perception range of a sensor
    - overestimated and therefore limited braking assistance

- **Malfunctioning behavior of E/E systems at vehicle level – ISO 26262**

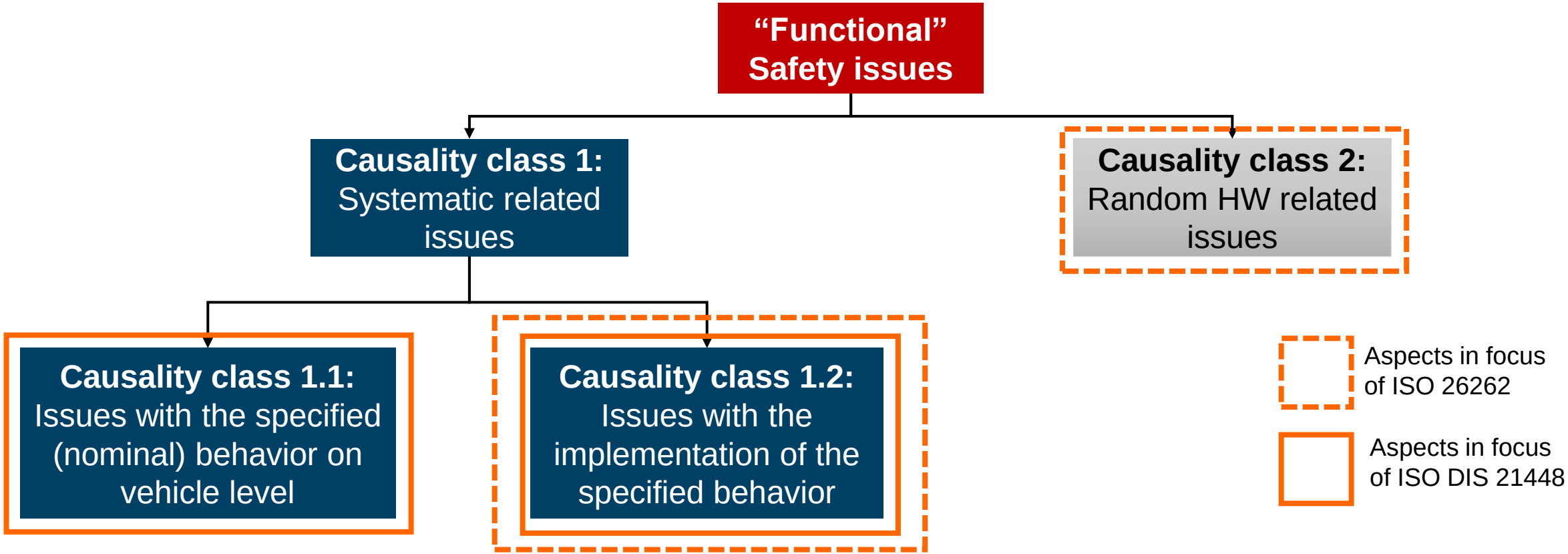
  - Unintended acceleration
  - Unintended deceleration
  - Unintended loss of acceleration
  - Unintended loss of deceleration
  - Unintended vehicle motion in general

Dangerous situations due to "functional insufficiencies (according to ISO 21448)" can lead to the same or more severe hazards as from "malfunctioning behavior (according to ISO 26262)" or cause new, previously unknown hazards.

Definitions – Safety issues causality classification scheme

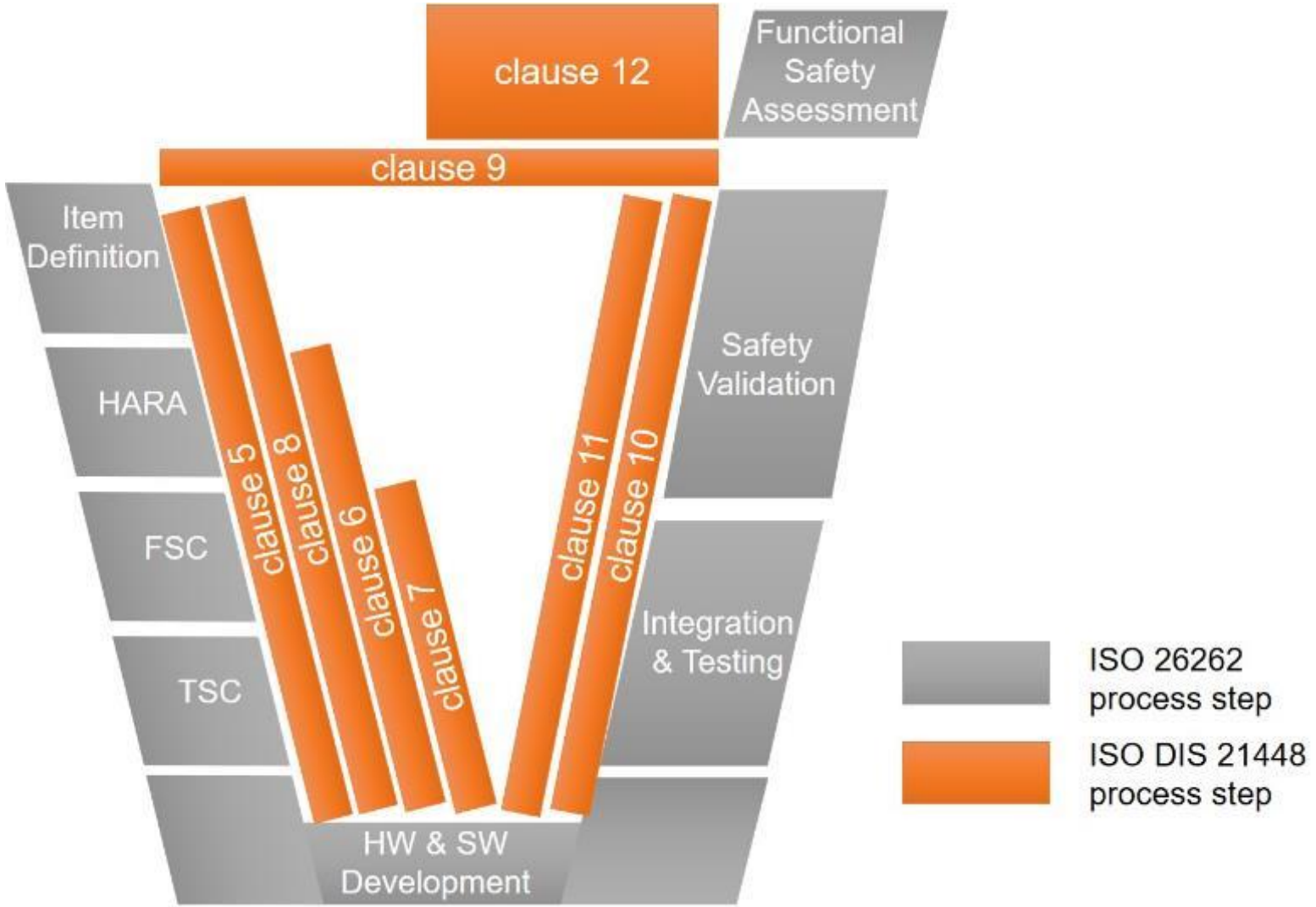
[ISO DIS 21448; annex A.2; figure A.14]

- The classification scheme focuses only on safety issues caused by E/E systems addressed by the ISO 26262 series and this document:



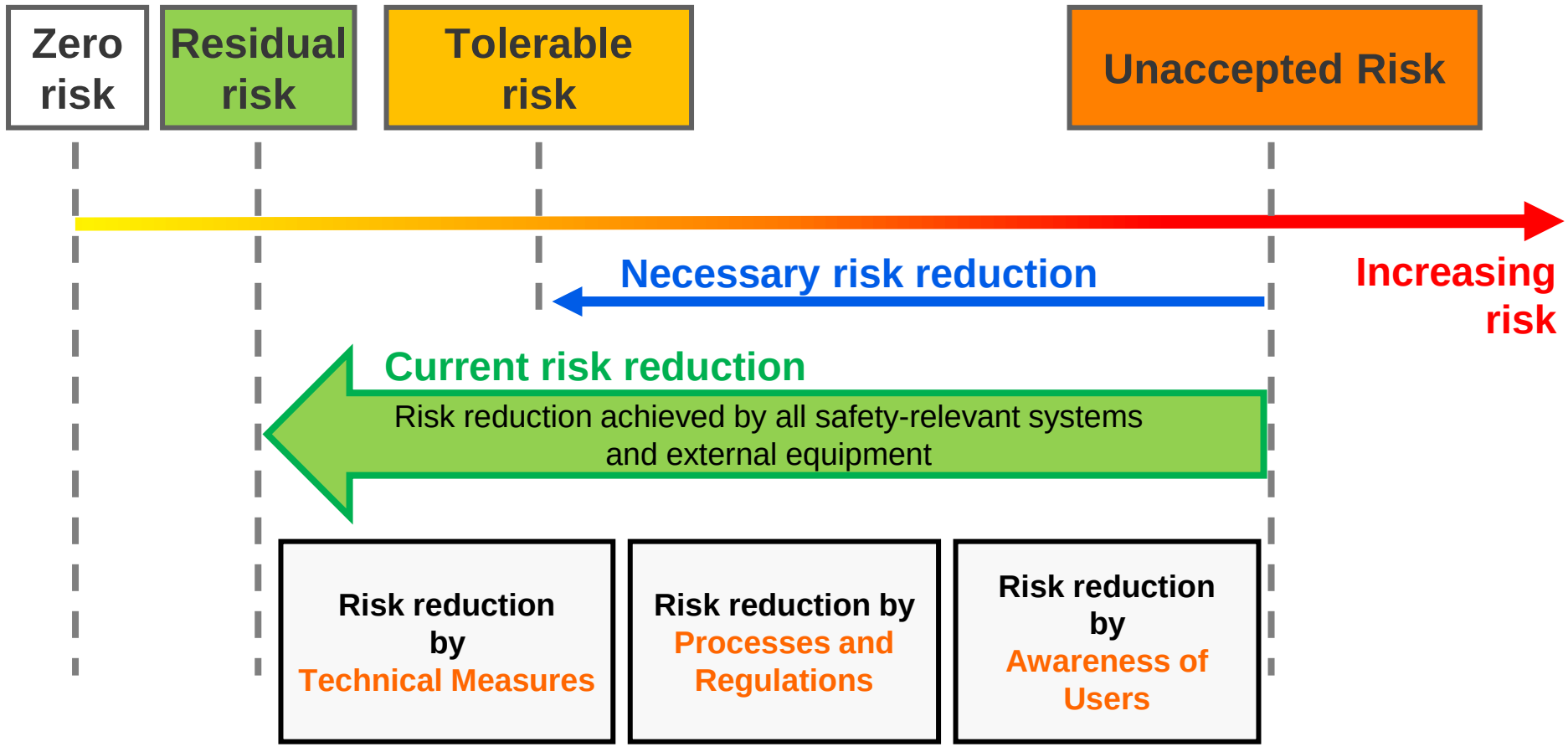
If a certain safety issue cannot clearly be classified as an issue for SOTIF or for functional safety, then both standards can be applied in combination to address the issue.

DEFINITIONS – INTERACTIONS OF DEVELOPMENT ACTIVITIES OF ISO 26262 WITH CLAUSES OF ISO DIS 21448 [ISO DIS 21448; annex A; figure A.15]



GENERAL CONCEPT FOR RISK REDUCTION

[IEC 61508]



Risk reduction is typically a combination of different measures

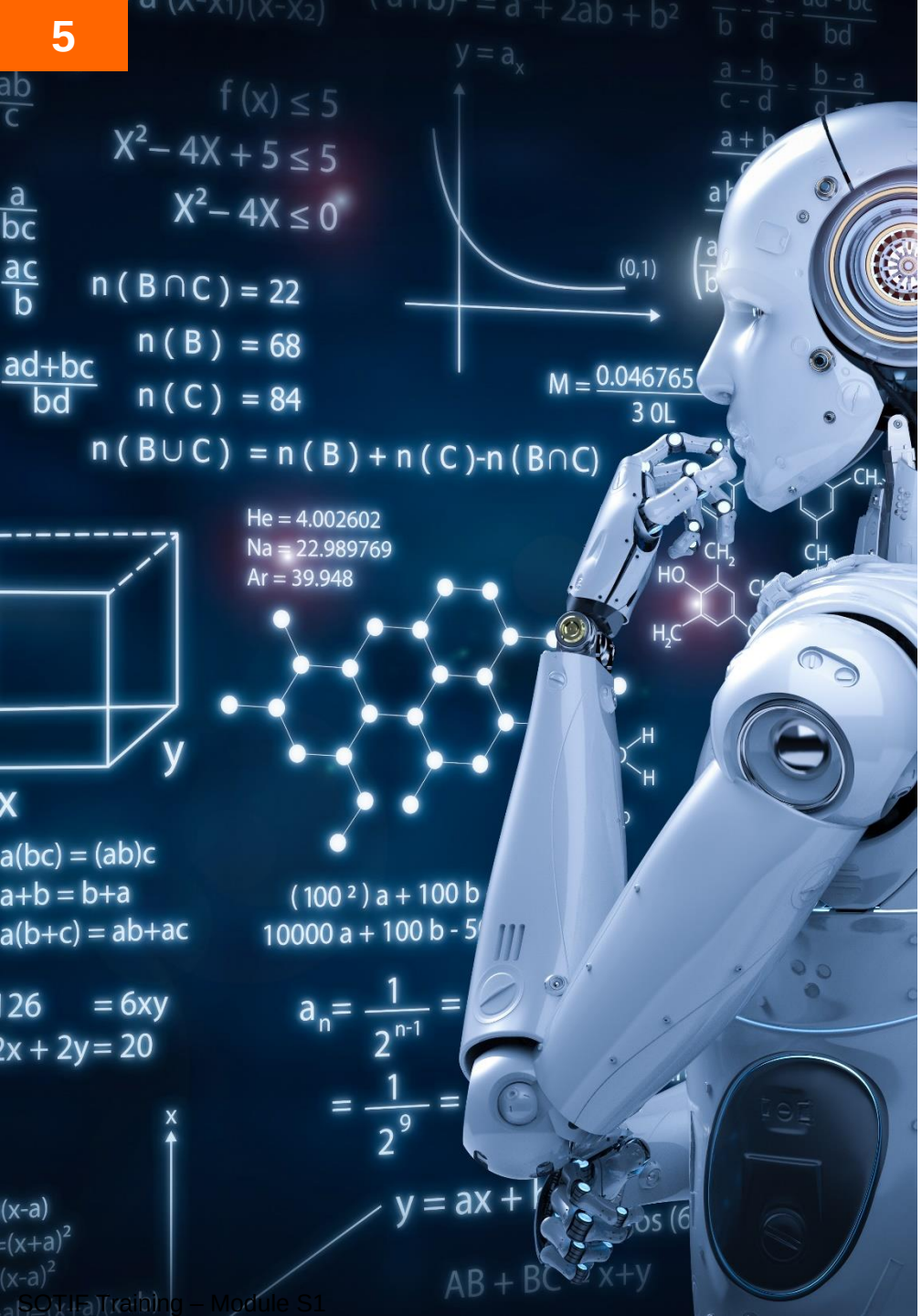
OVERVIEW OF SAFETY RELEVANT TOPICS ADRESSED BY DIFFERENT SAFETY STANDARDS

Source	Cause of hazardous events	Within scope of
System	E/E System failures – caused by random HW faults and systematic HW and SW faults	ISO 26262
	Insufficiencies of specification, performance limitations or insufficient situational awareness, with or without reasonably foreseeable misuse	ISO 21448
	Incorrect and inadequate design of Human-Machine-Interfaces (HMI) – inappropriate user situational awareness (e.g., HMI designs which lead to confusion of the user, user overload or user inattentiveness)	ISO 21448 & European Statement of Principles on HMI (2007/78/EC)
	System technologies – hazards caused by non-E/E-systems / system elements (e.g., electric shock, eye damage from a sensor laser)	specific standards (e.g., EN ISO 12100, EN ISO 13849, EN ISO 62061, ISO 6469)
External factor	Reasonably foreseeable misuse (direct and indirect)	ISO 21448
	Attack exploiting vehicle security vulnerabilities – Cybersecurity (e.g., hacking)	ISO SAE 21434 or SAE J3061
	Impact from active infrastructure and/ or vehicle to vehicle communication, and external systems	ISO 21448 & ISO 20077, ISO 26262
	Impact from vehicle surroundings (e.g., other users, passive infrastructure, climatic conditions/ weather, Electro-Magnetic Interference (EMI)	ISO 21448 & ISO 26262

[ISO DIS 21448:2020; table 1] + SGS-TÜV additions

CHAPTER 2 – SUMMARY

- SOTIF [ISO DIS 21448] and Functional Safety (FuSa) [ISO 26262] complement each other to realize the “Overall Functional Safety” from the E/E-perspective
- SOTIF in acc. with ISO DIS 21448 is applicable for the automation levels 1 to 5
- SOTIF covers “functional insufficiencies” on vehicle level (→ insufficiency of specification + performance limitations) and FuSa covers the “malfunctioning behavior” of E/E systems (random HW faults + systematic HW and SW faults)
- SOTIF and FuSa can be developed in parallel if a new function is realized – If FuSa already has been accomplished and SOTIF will be developed afterwards, an “impact analysis” shall be performed to identify issues where SOTIF activities may result in impacts on FuSa
- Only a small part of ISO DIS 21448 is normative
- **WORK PRODUCTS:**
  - **None**



AGENDA

1. Motivation
2. Introduction into SOTIF and Functional Safety
3. **Overview and organization of SOTIF activities – Management of SOTIF wrt. Functional Safety**
4. SOTIF and AI

MANAGEMENT OF SOTIF ACTIVITIES + SUPPORTING PROCESSES – OVERALL PRODUCT SAFETY – OVERVIEW

[ISO DIS 21448; clause 4.4.1 + SGS-TÜV additions]

Management of Safety and Security for Automated Driving Systems – new standards under development e.g., ISO TS 5083, ISO PAS 8800, ISO 34502,...

Functional Safety Management – based on ISO 26262	**SOTIF Management** – based on ISO DIS 21448	**Security Management** – based on ISO SAE 21434

General Safety Management– e.g., based on EN ISO 12100, EN ISO 13849, ISO 6469

Quality Management System – e.g., based on ISO 9001, IATF 16949, ISO 15288, ASPICE

- Developing a „safe“ product is not possible without a strong base – **Quality Management System/ Process**
- Safety topics, which are not part of Functional Safety and SOTIF e.g., mechanical safety or chemical safety are considered using other standards – **General Safety**
- The Safety of Functions/ Functionality is now considered within the topics of Functional Safety + SOTIF + Cybersecurity in parallel – **Management of the Safety Of Functions**
- Future safety topics e.g., Safety for Automated Driving Systems will be covered by new standards, which are currently under development – **The Management of these future topics is not defined yet**

MANAGEMENT OF SOTIF ACTIVITIES – GENERAL REQUIREMENTS

[based on ISO 26262-2]

The Management of SOTIF activities shall be based on the "Management of Functional Safety" as specified in ISO 26262-2, extended to the SOTIF related activities as specified in ISO DIS 21448.

- **OVERALL Safety Management – ISO 26262-2; clause 5**
  - Safety Culture
  - Management of safety anomalies
  - Competence management
  - Quality Management during the safety lifecycle
  - Project independent tailoring

- **PROJECT-SPECIFIC Safety Management – ISO 26262-2; clause 6**
  - Roles & Responsibilities
  - Planning and coordination of safety activities
  - Project-specific "tailoring" of the safety lifecycle
  - Confirmation measures
  - Release for production

- **Safety Management AFTER "START OF PRODUCTION" – ISO 26262-2; clause 7**
  - Roles & Responsibilities
  - Planning of safety activities
  - Field monitoring
  - Modification

MANAGEMENT OF SOTIF ACTIVITIES – DISTRIBUTED DEVELOPMENT

[ISO DIS 21448; clause 4.4.2]

- **Distributed development** activities concerning **SOTIF** shall be **organized by** using **ISO 26262:2018; clause 5** “Interfaces within distributed developments”, to:
  - define the interactions and dependencies between customer and suppliers' activities,
  - describe the allocation of responsibilities and
  - identify the work products to be exchanged for distributed development of a product and its comprising elements & components
- The **framework of** a “**Development Interface Agreement (DIA)**” as specified in ISO 26262 can be **used bu**t need to be **reworked** – The activities and work products of ISO 26262 needs to be substituted by the activities and work products of ISO DIS 21448; clauses 5 to 13.
- The **main tasks** of the “management of distributed SOTIF related developments are:
  - **supplier selection** criteria in acc. with ISO 26262; clause 5.4.2,
  - **initiation and planning** of distributed development in acc. with ISO 26262; clause 5.4.3 and
  - **execution** of distributed development in acc. with ISO 26262; clause 5.4.4

MANAGEMENT OF SOTIF ACTIVITIES – DISTRIBUTED DEVELOPMENT

[ISO DIS 21448; clause 4.4.2]

- SOTIF is heavily influenced by environmental factors (e.g., by the **O**perational **D**esign **D**omain or the scenario) → Therefore SOTIF is subdivided into three types which represent the different concerns depending oh hierarchical layers of a product:

  a) ***Vehicle level system*:** The complete system is developed using all SOTIF activities including clause 12 (Criteria for SOTIF release). Other distributed parties who develop subsystems and components receive the requirements and activities to fulfill associated to the relevant clauses of ISO DIS 21448 from the customer.

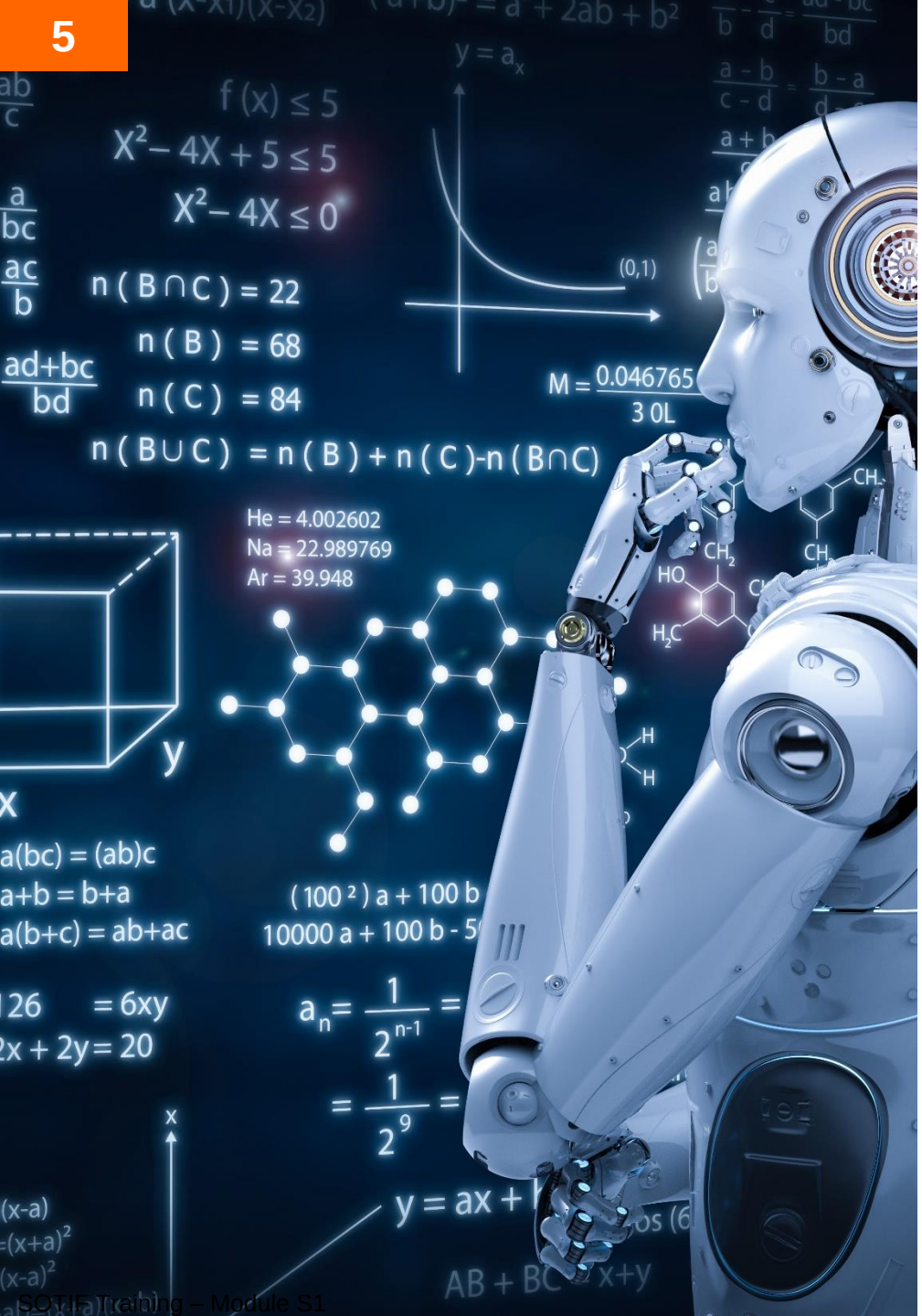
  b) ***Scenario related subsystems*:** Subsystems can be developed based on assumptions on the possible usage and hazardous scenarios on the vehicle system level. So, the work products related to specification & design (clause 5) and other activities (clauses 6, 7, 8, 9, 10, 11 and 13) are depending on the assigned role/ position of the supplier in the hierarchy of the development lifecycle.

  c) ***Other components*:** For subsystems and components not to be considered in a) or b) the SOTIF related work products cannot be completed independently because the dependency on the requirements from the higher level are mandatory as an input.

In general, the procedure for Safety Elements out of Context (SEooC) from ISO 26262; clause 9 is applicable. This can be performed by the substitution of the ISO 26262 related safety aspects with the safety aspects from ISO DIS 21448.

CHAPTER 3 – SUMMARY

- The Management of SOTIF is widely based on the Management of Functional Safety as specified in ISO 26262-2
- The supporting processes from ISO 26262-8 can be applied for SOTIF as well. These processes needs to be extended with and/ or be substituted by the SOTIF activities from ISO DIS 21448.
- Concerning the topic “Distributed Development” special attention for requirements cascading and traceability needs to be given.



AGENDA

1. Motivation
2. Introduction into SOTIF and Functional Safety
3. Overview and organization of SOTIF activities – Management of SOTIF wrt. Functional Safety
4. **SOTIF and AI**

Eduard Dojan
B. Eng., AFSE, CACSP

- 2021 **Senior Automotive Safety & Security Expert**
- 2017 – 2021 **Functional Safety EMEA**
- 2014 – 2016 **Project Development Engineer Functional Safety**
- 2010 – 2014 **Development Engineer**
- 2004 – 2010 **Laboratory Technician**

- Qualifications
  - **Degree in technical Computer science**
  - **State-certified technical computer scientist**
  - **Automotive Functional Safety Expert** (AFSE), ISO 26262
  - **Automotive Cyber Security Professional** (CACSP)

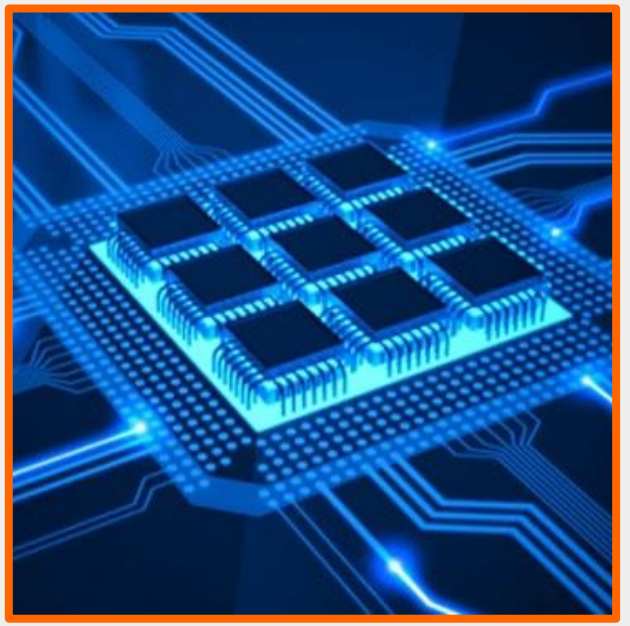
- Membership **German standardization group for ISO PAS 8800**
  (Road vehicles – Safety and Artificial Intelligence)

SGS TÜV SAAR

SGS

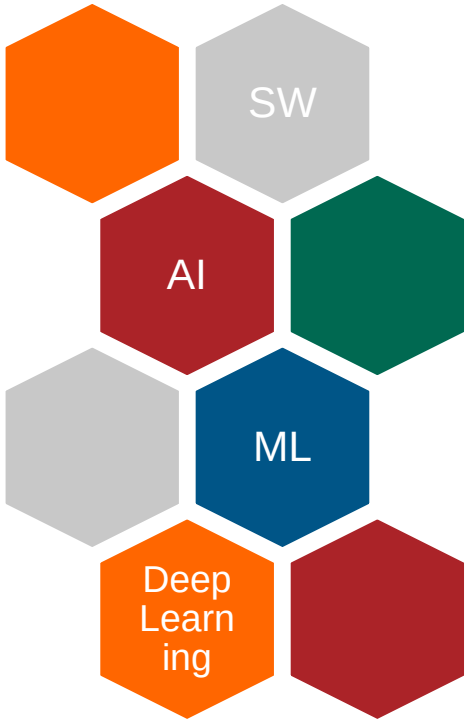
MOTIVATION

- mainly complex nonlinear transfer function machine learning and neural network provide superior solutions
- hardware accelerator on the other hand are from functional safety point of view follows a far more well-established functional safety approach.
- Machine Learning (ML) and Artificial Neural Networks (ANN) experience a lot of skepticism in safety applications



MACHINE LEARNING

- concurrent development showed, machine learning provides in general better functionality than classical programming for complex transfer functions



Relation

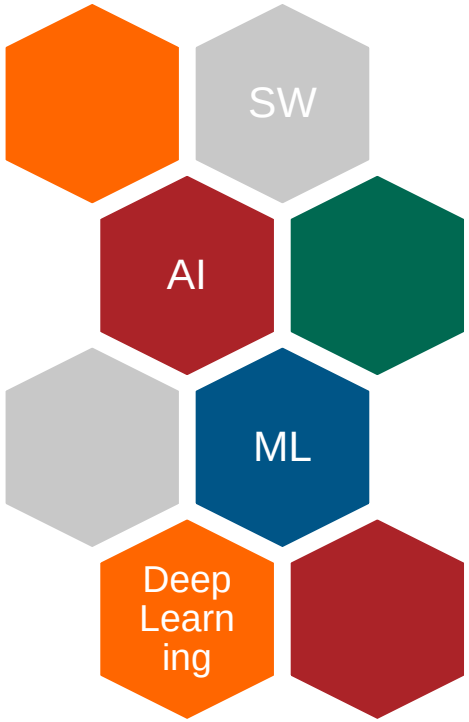
Annex D.2 of SOTIF:

- safety of ML involves a mixture of ISO 26262 and SOTIF
- Achieving safety when the intended functionality is implemented using ML (D.2.3)

D.2 Implications for machine learning

D.2.1 **General**

Autonomous vehicle technology often involves some type of machine learning (ML), especially for object detection and classification. Machine learning algorithms are mainly used when a full specification of the problem at hand is not possible (e.g. it is impossible to specify the data representation of a pedestrian in all varieties such that it could always be recognized by an algorithm). To overcome this, machine learning algorithms are used. ML algorithms learn to map inputs to outputs by extracting correlations existing in the data. Thus, differently from humans, ML algorithms do not learn about semantic context that could



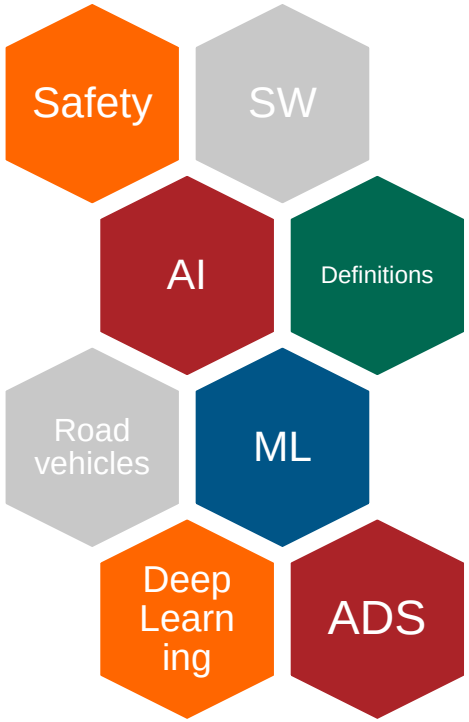
ML / ISO26262 & SOTIF

- Machine Learning ISO 26262 versus SOTIF Implications
- Achieving safety when the intended functionality is implemented using ML
- Implications for off-line training of machine learning algorithms
- An example off-line ML training process flow
- Analysis of the off-line training 3602 process of machine learning algorithms

D.2 Implications for machine learning

D.2.1 **General**

Autonomous vehicle technology often involves some type of machine learning (ML), especially for object detection and classification. Machine learning algorithms are mainly used when a full specification of the problem at hand is not possible (e.g. it is impossible to specify the data representation of a pedestrian in all varieties such that it could always be recognized by an algorithm). To overcome this, machine learning algorithms are used. ML algorithms learn to map inputs to outputs by extracting correlations existing in the data. Thus, differently from humans, ML algorithms do not learn about semantic context that could

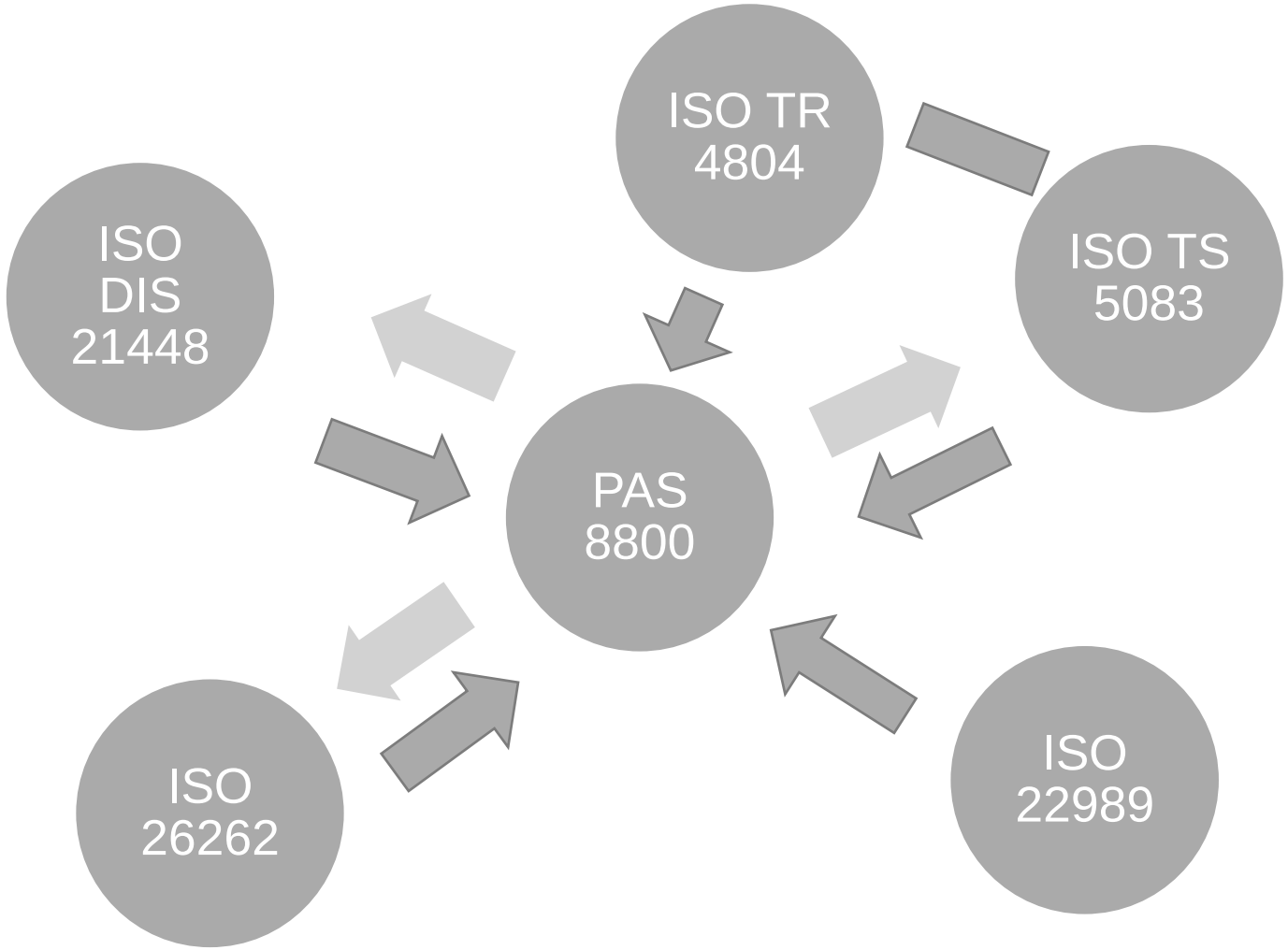


CURRENT STANDARDS

Mostly under development

- ISO TR 4804 using deep neural networks
- ISO TS5083 AI and ADS
- PAS 8800 Road vehicles Safety and AI
- ISO 26262 Functional Safety
- ISO/DIS 21448 implications for ML
- ISO 22989 AI definitions
- TR 5469 indep. Framework

RELATIONS BETWEEN STANDARDS



Thank you for your attention!

Become a certified functional safety practitioner
Get free information on in-house trainings focused on ISO 26262, SOTIF and ISO/SAE 21434 by clicking **here**