VOLVO

# The Automotive Safety Confusion – What's the Fuzz with Functional Safety, SOTIF and Positive Risk Balance?



1

VOLVO

## Who Am I?


- Technical Specialist System Safety, VCC
- PhD in Computer Engineering, Chalmers
- International & National Expert within ISO for ISO26262 / ISO21448 / ISO TS 5083, current Head of Swedish Delegation for ISO TS 5083 (Safety of Autonomous Drive).



2

VOLVO

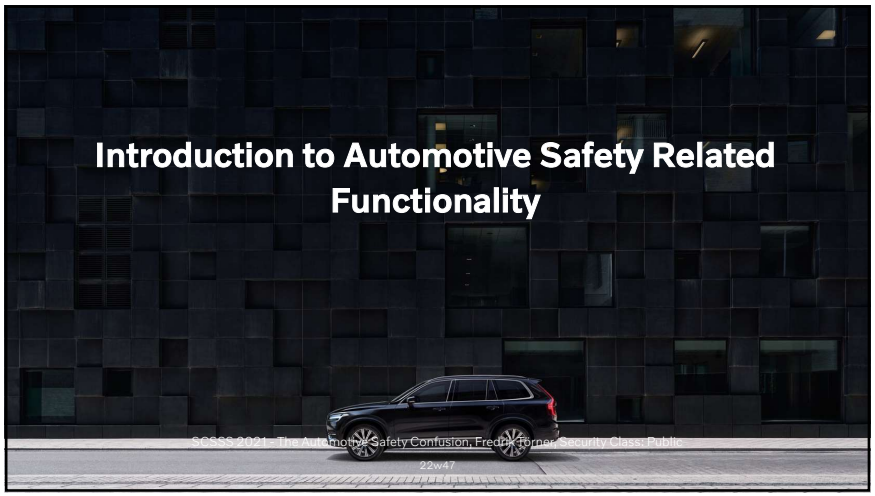
## Keynote Outline

1. Introduction to Automotive Safety Related Functionality
2. Society Perspective – The Legal Landscape
3. Product Safety In Regard To SW & E/E Technology
   - Product Cybersecurity
   - Functional Safety
   - Safety of the Intended Functionality
4. A Common View on ISO26262 & ISO21448
5. But What About Autonomous Drive?
6. Summary
7. Questions & Answers



3

# Introduction to Automotive Safety Related Functionality



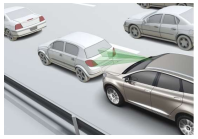


4

VOLVO

## Safety Related Automotive Functionality

Propulsion Functionality



Active Safety Functionality

Passive Safety Functionality

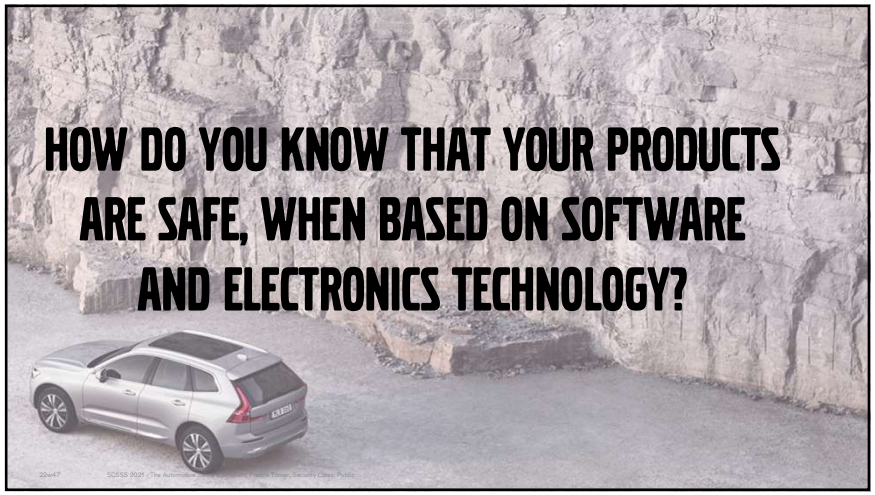
Information/Body Functionality

Autonomous Drive Functionality

Chassis Functionality



5

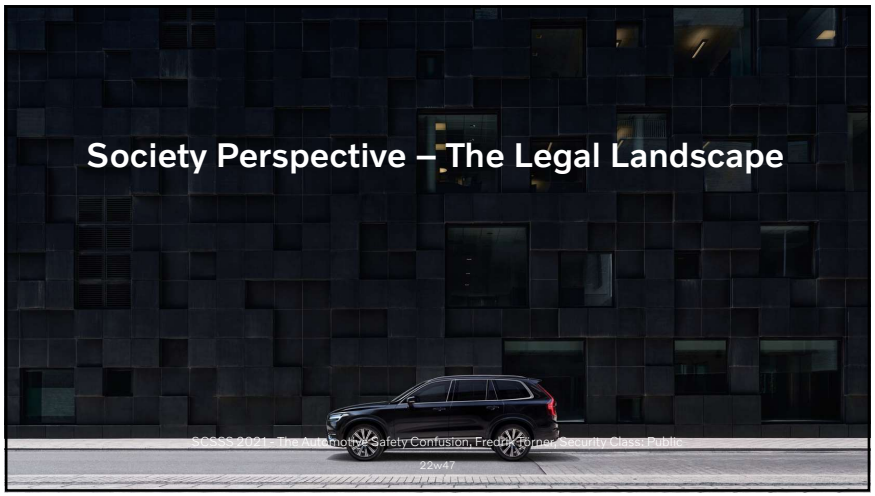



6

**What is Safe?**




7




8

VOLVO

## A Legal Perspective on Safety in the Automotive Industry

**Product Safety/Liability Regulation**
- **OEMs** releasing a product on the market, **are responsible for its safety**.
- Releasing a product on the market is an implicit claim of safety.
- The **market is monitored** by OEM/public/government for potential safety issues caused by **systematic safety defects**.
- Recalls may be necessary to maintain safe products in the field, during the product lifetime.

**UNECE e.g. European Union**
- Type Approvals of products, with requirements on safety, to get access to the market.
- Specific legal requirements.

**US**
- FMVSS (Federal Motor Vehicle Safety Standards) – Specific functional and technical requirements on safety-related designs.

**China**
- Type approval setup, adapted UNECE type approval requirements often including more details as GB/T standards.



9

VOLVO

## Government Legal Frameworks for ADS – Under Development!

**UNECE type approvals**
- ADS exemption process available from ECE type approvals for Brake/Steer systems etc.
- ALKS type approval.

**NHTSA - USA**
- Federal Automated Vehicles Policy (v1 to v4)
  - Provides guidance (e.g. important areas and standards)
  - Asks for Voluntary Safety Self Assessment Letter
- No ADS specific FMVSS, but difficulties with some current requiring a driver.

**China**
- Type approval under development.

**Challenges**
- Legal requirements put in place before technology maturity.
- Speed of development and continuous improvement put stress on the current system with "type approvals and field monitoring"



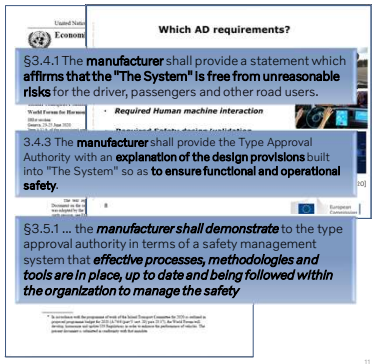

10

VOLVO

## Type Approval for ALKS - Automated Lane Keeping System

ALKS for low speed application is a system which is **activated by the driver** and which **keeps the vehicle within its lane** for travelling speed of **60 km/h or less** by controlling the lateral and longitudinal movements of the vehicle for extended periods **without the need for further driver input**.

**Includes e.g.:**
- Required driving behavior (e.g. minimal distances)
- System Safety and Fail-safe Response
- HMI / Operator Information
- Object and Event Detection and Response
- Data Storage
- Cybersecurity and Software-Updates
- Annex on "Special requirements to be applied to the functional and operational safety aspects"





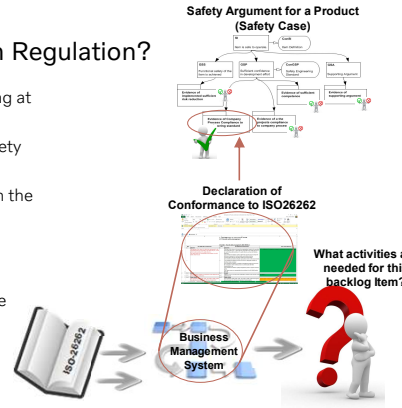

11

VOLVO

## Why Requirements on Processes in Regulation?

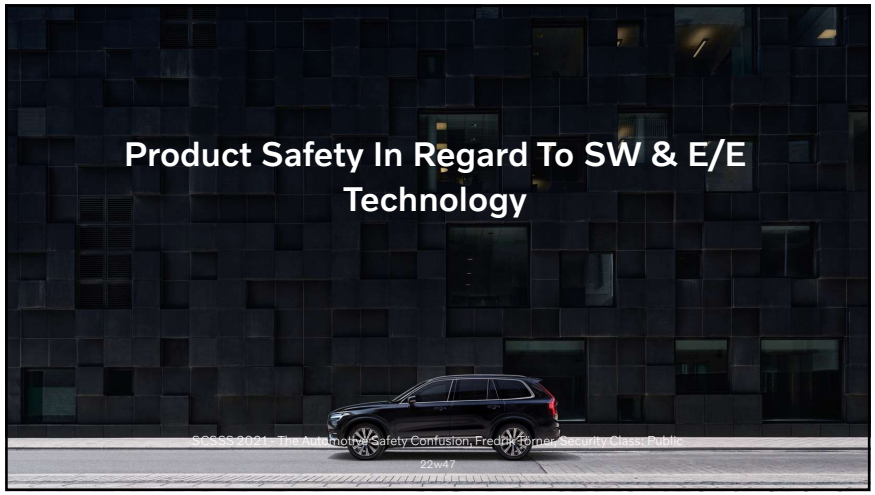
To **demonstrate achieved safety**, an argument including at least the following is necessary:
- **Product Argument -** Demonstrate fulfillment of safety requirements including V&V
- **Process Argument -** Gives the **confidence** placed in the product argument.

**A Process Argument Requires:**
1. Well-defined development process specifying the risk reduction related development activities.
2. Demonstrated fulfillment of the development activities






12




13

VOLVO

## Product Safety – A SW & E/E Technology Perspective

Product Safety

Safety of SW&E/E Technology

| Mechanical Safety<br>...<br>Chemical Safety | Safety Of The Intended Functionality (SOTIF)<br>Safe functional behaviour and nominal performance (including technical limitations). | Functional Safety (FuSa)<br>Handling of safety issues of malfunctions due to systematic and random faults in implementation. | Product Cybersecurity<br>Protection against an adversary gaining control of a safety related system. | Electrical Safety<br>Protection against electric chock and electric fire due to short circuits and insufficient insulation/EMI. |
|---|---|---|---|---|



14


15

VOLVO

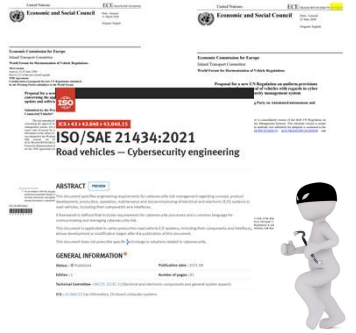
## Product Cybersecurity

Protection of vehicle systems and connected vehicle services from adversarial threats that may have safety, legislative, privacy, operational or financial impact.

The safety contribution is to protect the asset “Control of a safety related system”

Addressed by Management System, Security by Design, and Detection & Response.

UN regulations R-155 Cybersecurity and R-156 SUMS, which are addressed by e.g. ISO/SAE 21434:2021






16

VOLVO

# Functional Safety

17

VOLVO

## Functional Safety - Introduction

**Introduction of risk concept**

**Safety -** absence of **unreasonable risk** [ISO26262:2018]

**Functional Safety** - absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems [ISO26262:2018]

**Unreasonable risk** - risk judged to be unacceptable in a certain context according to valid societal moral concepts [ISO26262:2018]

Malfunctioning behaviour can in Software and Electrical and/or Electronic systems come from two types of sources:

- Systematic Faults – "Bugs" in SW and E/E designs.
- Random Hardware Faults – Ageing and Wear & Tear of HW.

Addressed in e.g. type approval requirements with special requirements on "electronic control systems".

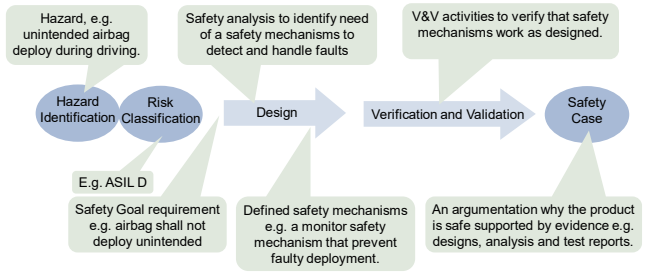


18

VOLVO

## Functional Safety - Fundamentals

*Functional Safety is a structured method to **identify potential hazards** of a function and to **reduce the risks** of these hazards by implementing **safety mechanisms** and ensuring their **integrity**.*






19

VOLVO

## ISO 26262 - Road vehicles — Functional safety

ISO-26262 is the **functional safety standard** for the automotive industry, released in November 2011 and in a **2nd edition December 2018**.

ISO-26262 is applicable to all **development of electrical and electronic systems** that are related to safety, e.g. active safety systems and brake systems.

**All major automotive OEMs and suppliers** have been active in this standardization effort.

The **automotive industry are broadly applying the standard**, as it provides a common view on what is needed.

To achieve functional safety, the ISO 26262 series of standards:

- provides an automotive-specific risk-based approach to determine integrity levels and adequate risk reductions measures.
- provides requirements for functional safety management, design, implementation, verification, validation and confirmation measures; and
- provides requirements for relations between customers and suppliers.

**Explicit Limitations**

It does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy and similar hazards, unless directly caused by malfunctioning behaviour of safety-related E/E systems.

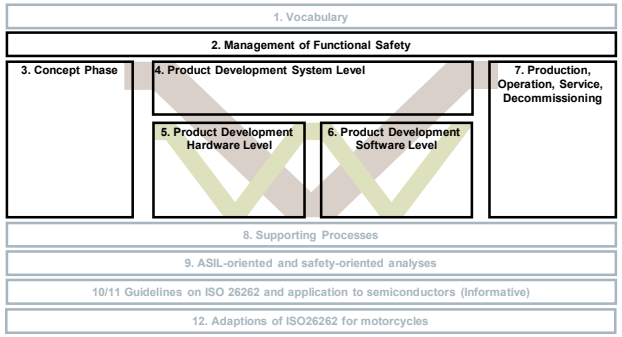
**"ISO 26262 does not address the nominal performance of E/E systems"**



20

VOLVO

## Structure of ISO-26262

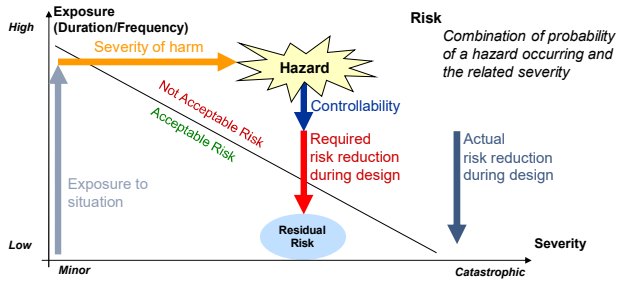





21

VOLVO

## Part 3 – Risk Classification and ESC Parameters






22

VOLVO

## Part 3 – What Does an ASIL Imply?

**For all ASIL**
Safety mechanisms to detect and handle the relevant failure modes at system level shall be introduced.

### For ASIL A and ASIL B

- Emphasis on additional development activities for quality assurance of introduced safety mechanisms, e.g.
  - Reviews, V&V activities

### For ASIL C and ASIL D

- Further emphasis on additional development activities for quality assurance of introduced safety mechanisms.
- Requirements on performance of safety mechanisms.
  - Typically require HW redundancy



23

VOLVO

## Part 3 – Structure and Importance of Correct ASIL

Objective: The objective of this clause is to ensure the compliance of the developed hardware with the hardware safety requirements.

Requirement: **10.4.6** The hardware integration and verification activities shall verify the durability and robustness of hardware against environmental and operational stress factors. To achieve these objectives, the methods listed in Table 12 shall be considered.

Guidance on how to meet the Requirement, dimensioning for engineering effort.

**Part 5 (HW), Table 12 — Hardware integration test (edited)**

| | Methods and Measures | ASIL A | B | C | D |
|---|---|---|---|---|---|
| 1 | Functional testing under environmental conditions | ++ | ++ | ++ | ++ |
| 2 | Environmental testing | ++ | ++ | ++ | ++ |
| 3 | Accelerated life test | + | + | ++ | ++ |
| 4 | Statistical testing | o | o | + | ++ |
| 5 | Worst case testing | o | o | o | + |
| ... | | | | | |

Note: "++" = Highly Recommended, "+"= Recommended, and "o"= No Recommendation [ISO 26262:2018]



24

VOLVO

## ISO26262 Provides a Framework for Development of Safety Related Systems of Different Technologies

**ISO 26262:2018 Requirements on Base Development Process**

- Existence of a Quality Management System (IATF16949/ISO9001)
- Development process for Function, System, Component – Including design, analysis and V&V.
- Development Interface Agreements
- Requirement Handling
- Configuration Management
- Change Management
- Verification Management
- Document Management
- Confidence In the Use of SW Tools
- ...

Isn´t it safe as long as we just do the Functional Safety activities?

**No!**
... because the safety activities cannot be done in a vacuum! We need to have a Product Development Process that provides designs that we can apply safety activities on.

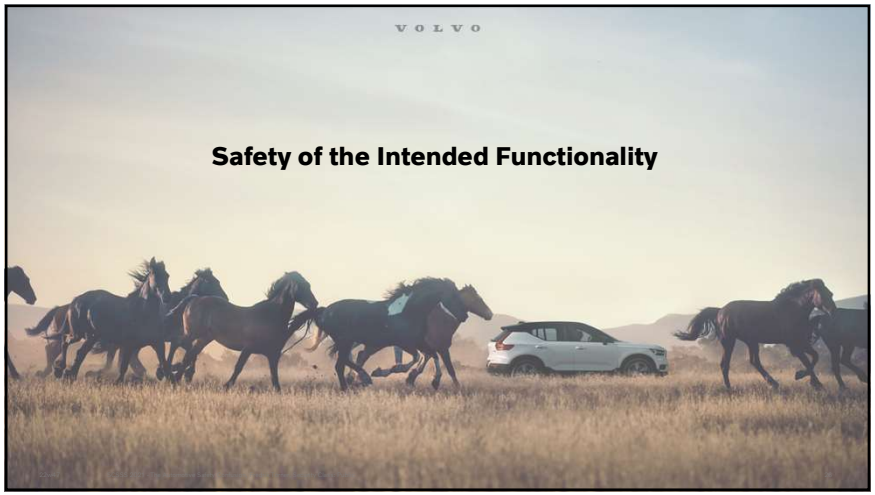
Each organization need a well defined, controlled and complete development process to be able to achieve safety.



25

VOLVO

## Safety of the Intended Functionality



26

VOLVO

## Safety of the Intended Functionality

**Safety –** absence of **unreasonable risk** [ISO26262:2018]

**SOTIF** - absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or its implementation. [ISO FDIS* 21448]

- **SOTIF is a concept** – Necessary for any safety related product!
- The SOTIF **ISO FDIS 21448** has a **limited scope** of "AD/ADAS**" but provides objectives and a Way of Working that could be used for all type of functionality.

**Functional Insufficiencies lead to Hazardous behaviour and** can come from two type of sources:

**Insufficiency of Specification** - specification, possibly incomplete, contributing to either a hazardous behaviour or an inability to prevent or detect and mitigate a reasonably foreseeable indirect misuse when activated by one or more triggering conditions.

E.g. an Emergency Brake function defined with too strong brake intervention.

**Performance Insufficiency** - limitation of the technical capability contributing to a hazardous behaviour or inability to prevent or detect and mitigate reasonably foreseeable indirect misuse when activated by one or more triggering conditions.

E.g. radar sensor technology has difficulties to detect stationary objects.

*ISO FDIS 21448:2021 candidate

** This document is applicable to intended functionalities where proper situational awareness is essential to safety and where such situational awareness is derived from complex sensors and processing algorithms, especially functionalities of emergency intervention systems and systems having levels of driving automation from 1 to 5.

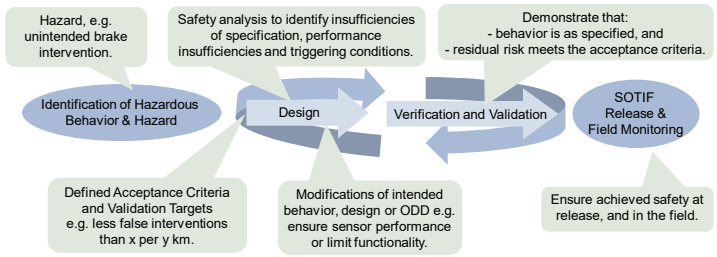


27

VOLVO

## Safety of the Intended Functionality - Fundamentals

*SOTIF is a structured method to **identify potential hazards of a functionality** and to **ensure that the risks** of these hazards are acceptable by ensuring that the **intended behavior is in parity with the technical capabilities** of the implementation.*






28

VOLVO

## Identification and Evaluation of Hazards & Identification and Evaluation of Hazardous Behaviour

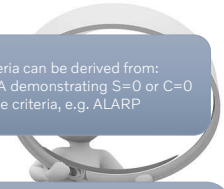
Systematic analysis of the Functionality has to be done to identify and evaluate:

- Hazards from intended functionality at vehicle level
- Hazardous Behaviour with scenarios

⇒ Defined Acceptance Criteria and Validation Targets

- Insufficiencies of specification
- Performance insufficiencies
- Triggering conditions

⇒ Documented SOTIF issues and evaluations



Acceptance Criteria can be derived from:
- A FuSa HARA demonstrating S=0 or C=0
- Risk tolerance criteria, e.g. ALARP

Guidance on effective analysis methods e.g.
- Analysis of requirements

Guidance on what parameters to consider:
- Known algorithm limitation
- Sun glare
- Direct and indirect misuse



29

VOLVO

## Functional Modifications Addressing SOTIF-Related Risks

The **identified SOTIF issues** has to be sufficiently addressed by **modifications** of the intended behavior, the design/implementation or limitations to the ODD.

**System modification**
- Improved sensor technology

**Functional restrictions**
- Limit an ADAS intervention in strength or time.

**Handing over authority**
- HMI design to hand over control to a driver.

**Addressing reasonably foreseeable misuse**
- HMI improvements.



30

VOLVO

## Verification and Validation

It is required to **demonstrate** that:

- the product behavior is **as specified**,
- the residual risk **meets the Acceptance Criteria** (via met Validation Targets)

...with **sufficient coverage** for both **known and unknown hazardous scenarios**.

The demonstration includes a V&V strategy with justified validation targets & V&V methods and supporting evidences (e.g. analysis and test reports).

Guidance is given on suitable V&V methods, e.g.

- Sensor performance tests
- Robustness tests
- Vehicle long term tests
- ...

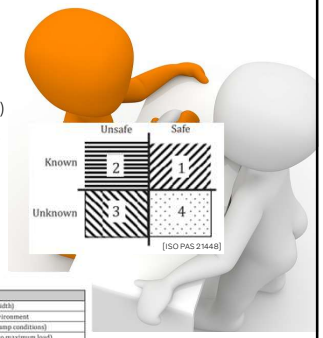



**Table 7 — Actuation verification**

| | Methods |
|---|---|
| A | Requirements-based test (e.g. precision, resolution, timing constraints, bandwidth) |
| B | Verification of actuator characteristics, when integrated within the vehicle environment |
| C | Actuator test under different environmental conditions (e.g. cold conditions, damp conditions) |
| D | Actuator test between different preload conditions (e.g. change from medium to maximum load) |
| E | Verification of actuator ageing effects (e.g. accelerated life testing) |
| F | In the loop testing (e.g. SIL/HIL/MIL) on selected SOTIF relevant use cases and scenarios |
| G | Vehicle level testing on selected SOTIF relevant use cases and scenarios |

[ISO PAS 21448]



31

VOLVO

## SOTIF Release & Field Monitoring

**At Product Release**

- Quality assurance of the work products
- An argument for achieving SOTIF, e.g. safety case
- The product Release decision must include an evaluation of the argument for achieved SOTIF

=> The standard guides with a checklist!

**After Product Release**

- Functions which are dependent on awareness of vehicle surroundings are inherently affected by changes in the environment over time.
- A Field Monitoring process is required during the operational phase to continuously evaluate the SOTIF argument.



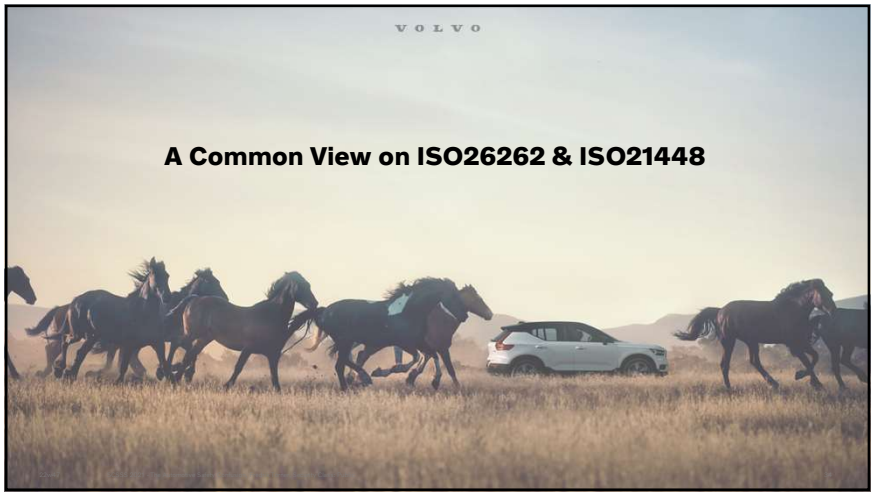
32

VOLVO

## Project Plan for ISO 21448 SOTIF


ISO FDIS 21448 will soon come out for international review and will replace ISO PAS 21448 in Q1 2022.

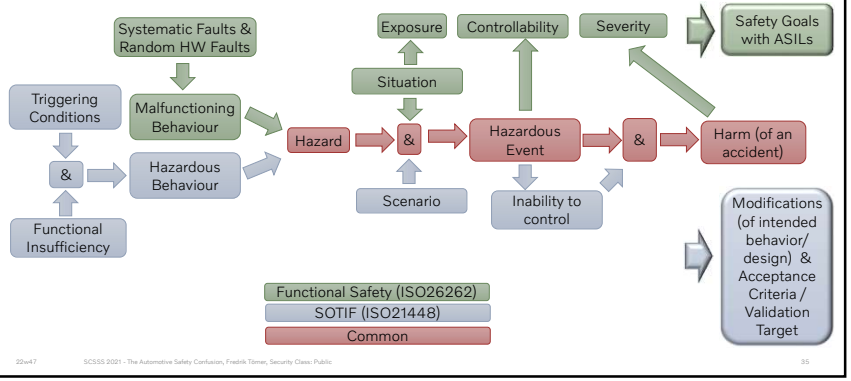
33




34

VOLVO

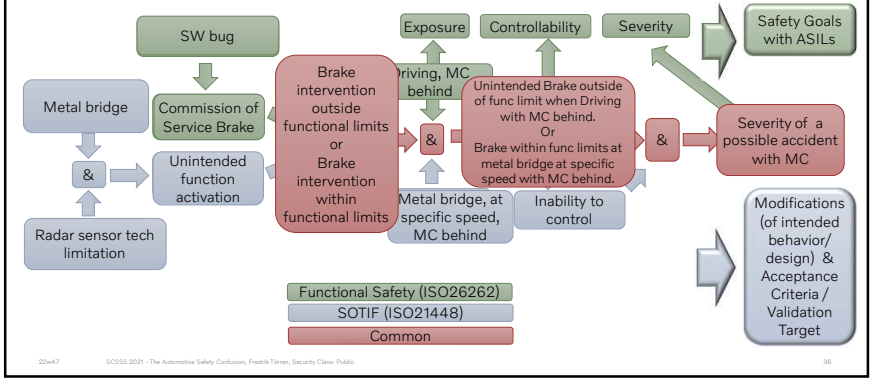
## Simplified "Cause and Effect" Model for ISO26262 and ISO21448



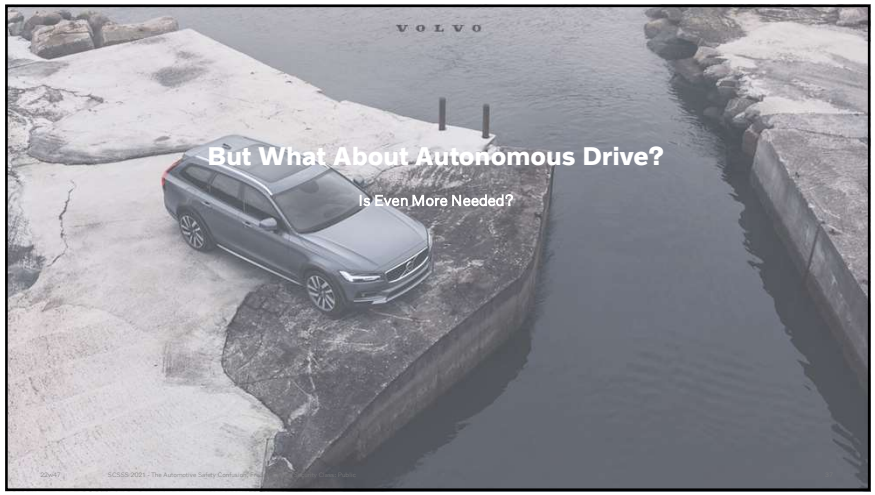

35

VOLVO

## Simplified "Cause and Effect" Model for ISO26262 and ISO21448




36




37

VOLVO

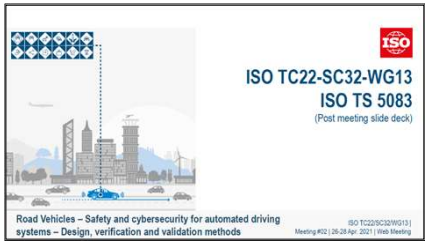
## ADS Standardization

ISO TC22-SC32-WG13 is the a newly formed ISO Working Group for Application standards on ADS.

**ISO Technical Specification 5083 "Road vehicles — Safety for automated driving systems — Design, verification and validation"**

It is intended as a continuation of the "Safety First" white paper, and the ISO TR 4804, with the difference on aiming for **normative content**.

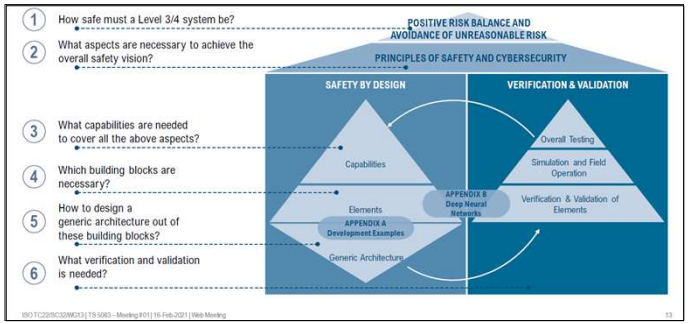
Intention is to be an **application standard** for ADS and **build on top** of other standards and explain how to use them in an ADS context.




38

VOLVO

## Intended Content of ISO TS 5083 (from ISO TS 4083)




39

VOLVO

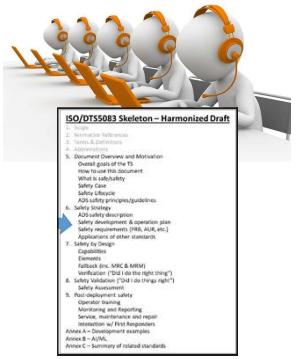
## Current Status

Ongoing work in international subteams analyzing and discussing the national proposal for content changes.

ISO TS 5083 document skeleton has been created.

**Open discussions**

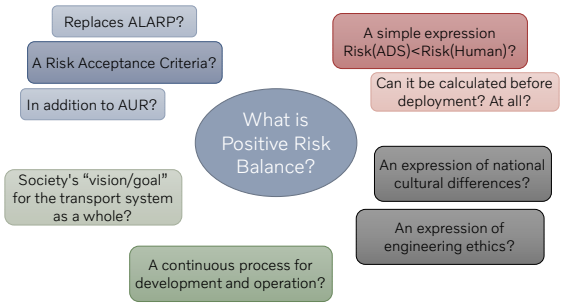
- Normative Objectives
- Verification & Validation
- Safety by Design
- Management of the Operational Phase Safety
- Positive Risk Balance and relation to Absence of Unreasonable Risk.




40

VOLVO

## Positive Risk Balance




**This demonstrates:**

- The complexity of defining Safe ADS.
- The need for international standardization activities to support ADS developers and societies with a common industry view.
- How rewarding it can be for participating individuals with open minds and willingness to find consensus!



41

VOLVO

## Workplan & Timeplan for ISO TS 5083

| | Principle schedule of WG13 plenary and sub-team meetings | Meeting dates: | |
|---|---|---|---|
| Alignment phase | ▪ 2nd WG13 Meeting<br>– Understand proposals on cluster and topics | 2nd WG13 plenary | 2021-02-16 |
| | ▪ 3rd/ 4th WG13 Meeting and sub-team workshops<br>– Align and detail proposals incl. initial drafting of text<br>– Decide on proposals for TS 5083 | 3rd WG13 plenary<br>4th WG13 plenary | 2021-07-26/27/28<br>2021-Nov. |
| Integration phase | ▪ 5th/ 6th WG13 Meeting and sub-team workshops<br>– Drafting of text and integration into TS 5083<br>– Create baseline after 6th meeting | 5th WG13 plenary<br>6th WG13 plenary | 2022-Mar.<br>2022-Jun. |
| Review phase | ▪ Official commenting via SC32 in ISO comments sheet<br>▪ 7th/ 8th WG13 Meeting<br>– Review and conclusion of comments | 7th WG13 plenary<br>8th WG13 plenary | 2022 late Sep. - early Oct.<br>2022 Dec. |

**Target publication date for ISO TS 5083 is Mid-2023**



42

## So? Back to the Original Question



43

## HOW DO YOU KNOW THAT YOUR PRODUCTS ARE SAFE, WHEN BASED ON SOFTWARE AND ELECTRONICS TECHNOLOGY?

**BY ENSURING THAT:**

- SUFFICIENT RISK REDUCTION MEASURES ARE TAKEN DURING PRODUCT DEVELOPMENT
- THE FUNCTIONAL CONTENT IS IN BALANCE WITH THE TECHNICAL CAPABILITIES OF YOUR PRODUCT
- THE TECHNICAL IMPLEMENTATION HAS SUFFICIENT INTEGRITY



44

VOLVO

## Summary

- For safe application of SW and Electronics technology there are regulation as well as industry best-practices in place.
  - Continuously developed and adapted, e.g. for ADS.
- Industry standards provides terminology and toolboxes to achieve safety and meet regulation.
- How to argue achievement of safe ADS is an open question which is being addressed through research, industry collaboration and standardization.



45

46