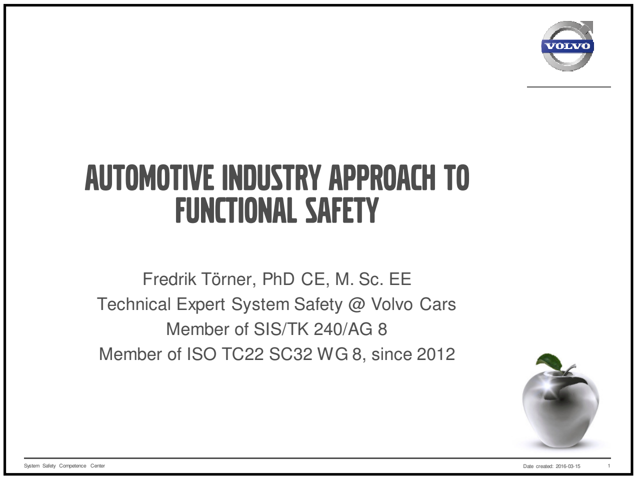
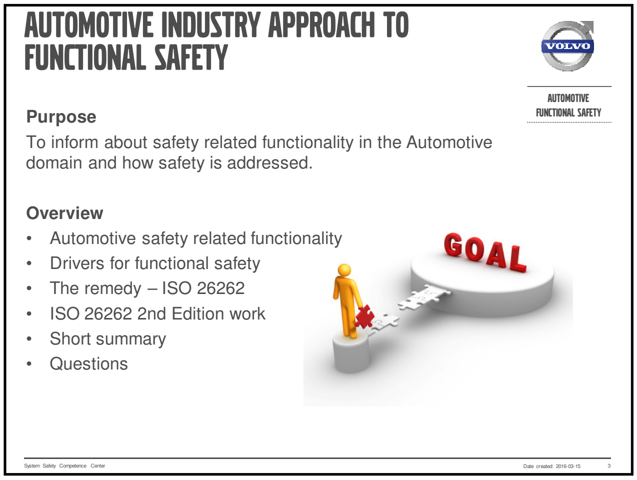


AUTOMOTIVE INDUSTRY APPROACH TO FUNCTIONAL SAFETY

Fredrik Törner, PhD CE, M. Sc. EE
Technical Expert System Safety @ Volvo Cars
Member of SIS/TK 240/AG 8
Member of ISO TC22 SC32 WG 8, since 2012



AUTOMOTIVE INDUSTRY APPROACH TO FUNCTIONAL SAFETY

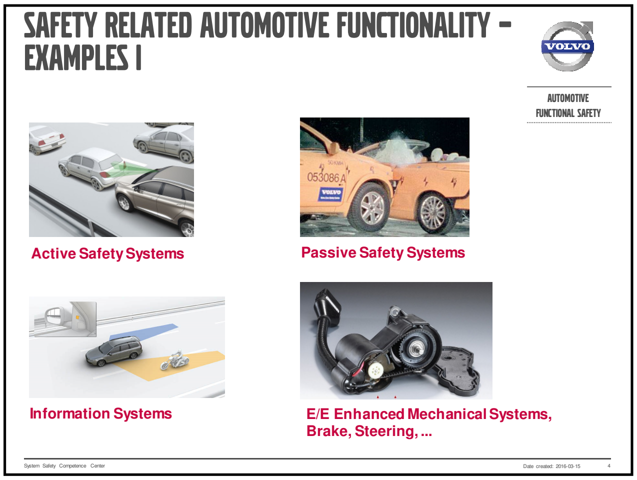
AUTOMOTIVE FUNCTIONAL SAFETY

Purpose

To inform about safety related functionality in the Automotive domain and how safety is addressed.

Overview

- Automotive safety related functionality
- Drivers for functional safety
- The remedy – ISO 26262
- ISO 26262 2nd Edition work
- Short summary
- Questions



SAFETY RELATED AUTOMOTIVE FUNCTIONALITY – EXAMPLES I

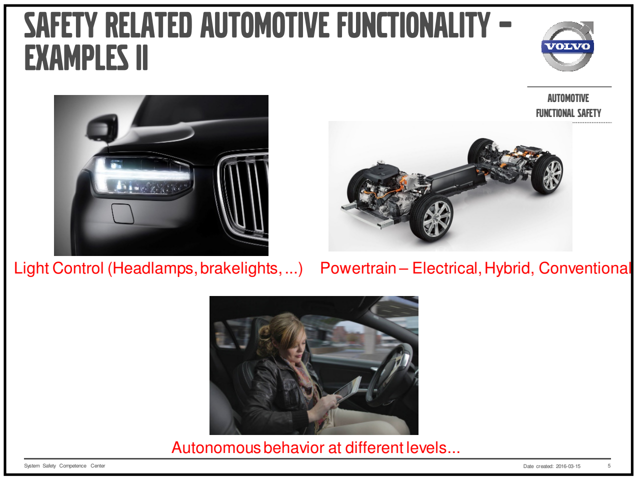
AUTOMOTIVE FUNCTIONAL SAFETY

Active Safety Systems

Passive Safety Systems

Information Systems

E/E Enhanced Mechanical Systems, Brake, Steering, ...



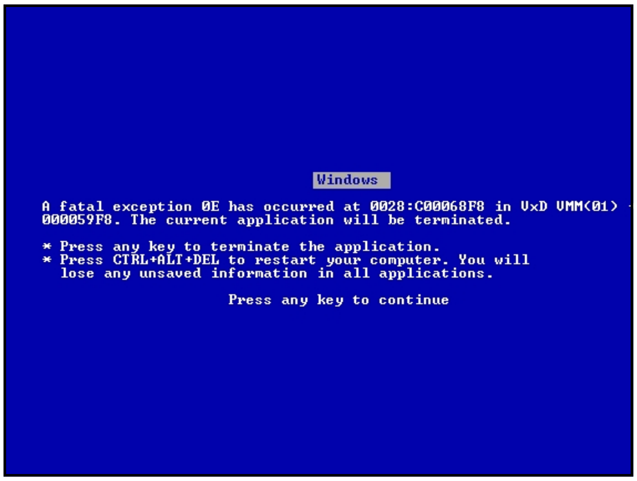
SAFETY RELATED AUTOMOTIVE FUNCTIONALITY – EXAMPLES II

AUTOMOTIVE FUNCTIONAL SAFETY

Light Control (Headlamps, brakelights, ...)

Powertrain – Electrical, Hybrid, Conventional

Autonomous behavior at different levels...



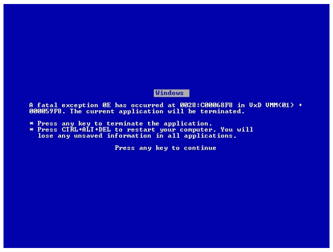
```
                           Windows

 A fatal exception 0E has occurred at 0028:C00068F8 in VxD VMM(01) +
 000059F8. The current application will be terminated.

 * Press any key to terminate the application.
 * Press CTRL+ALT+DEL to restart your computer. You will
   lose any unsaved information in all applications.

                    Press any key to continue
```

WINDOWS BLUE SCREENS…



```
                           Windows

 A fatal exception 0E has occurred at 0028:C00068F8 in VxD VMM(01) +
 000059F8. The current application will be terminated.

 * Press any key to terminate the application.
 * Press CTRL+ALT+DEL to restart your computer. You will
   lose any unsaved information in all applications.

                    Press any key to continue
```

... are annoying in windows computers…

…but could be **safety concerns** in embedded systems!

SAFETY RELATED FAILURE MODES

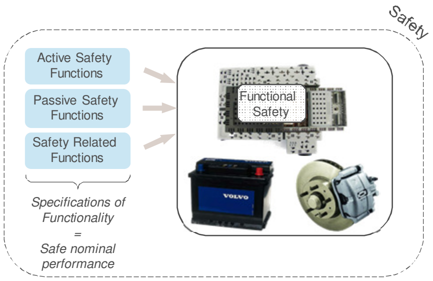
”Obvious”

- Sudden Acceleration
- Unintended activation of airbag
- Unintended brake
- ...

Maybe not so obvious...

- Sudden unintended Power Seat movement

SCOPE OF FUNCTIONAL SAFETY



Safety

Active Safety Functions

Passive Safety Functions

Safety Related Functions

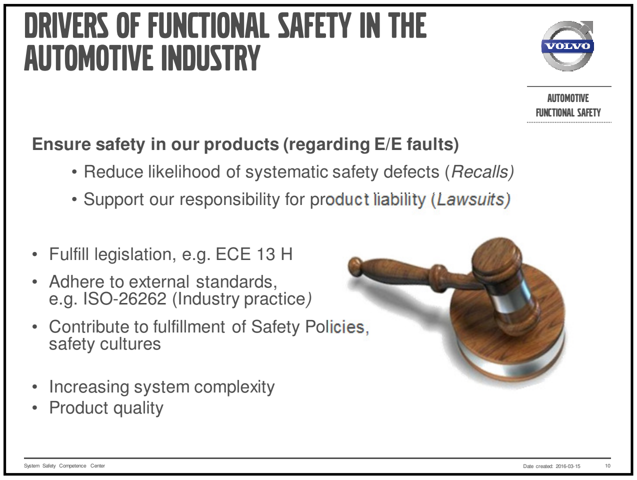
Functional Safety

Specifications of Functionality

=

Safe nominal performance

Functional Safety - absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems [ISO 26262-1:2011]



DRIVERS OF FUNCTIONAL SAFETY IN THE AUTOMOTIVE INDUSTRY

AUTOMOTIVE
FUNCTIONAL SAFETY

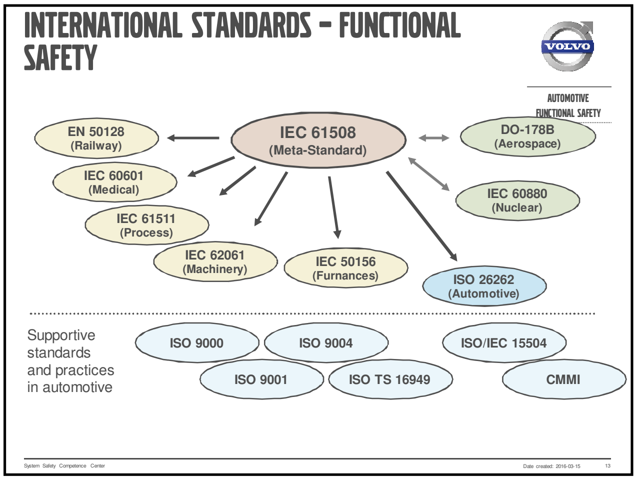
Ensure safety in our products (regarding E/E faults)

- Reduce likelihood of systematic safety defects (*Recalls)*
- Support our responsibility for product liability (*Lawsuits)*

- Fulfill legislation, e.g. ECE 13 H
- Adhere to external standards, e.g. ISO-26262 (Industry practice*)*
- Contribute to fulfillment of Safety Policies, safety cultures

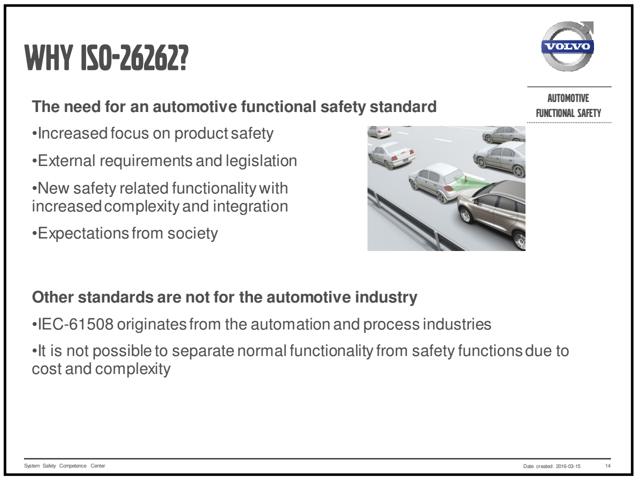
- Increasing system complexity
- Product quality

FUNCTIONAL SAFETY STANDARDS & ISO-26262



INTERNATIONAL STANDARDS – FUNCTIONAL SAFETY

Supportive standards and practices in automotive



WHY ISO-26262?

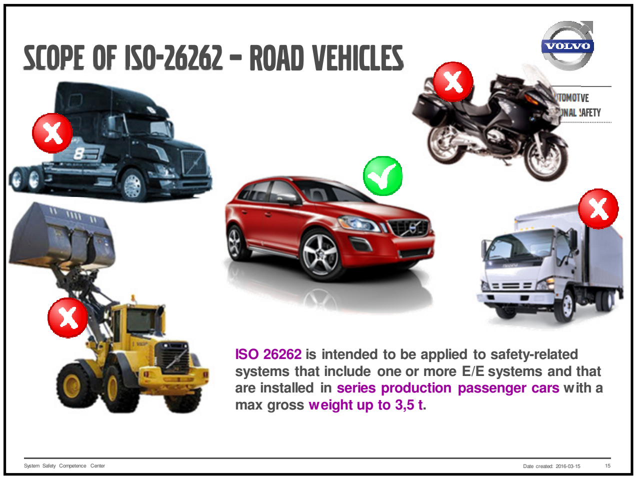
AUTOMOTIVE
FUNCTIONAL SAFETY

The need for an automotive functional safety standard

- Increased focus on product safety
- External requirements and legislation
- New safety related functionality with increased complexity and integration
- Expectations from society

Other standards are not for the automotive industry

- IEC-61508 originates from the automation and process industries
- It is not possible to separate normal functionality from safety functions due to cost and complexity

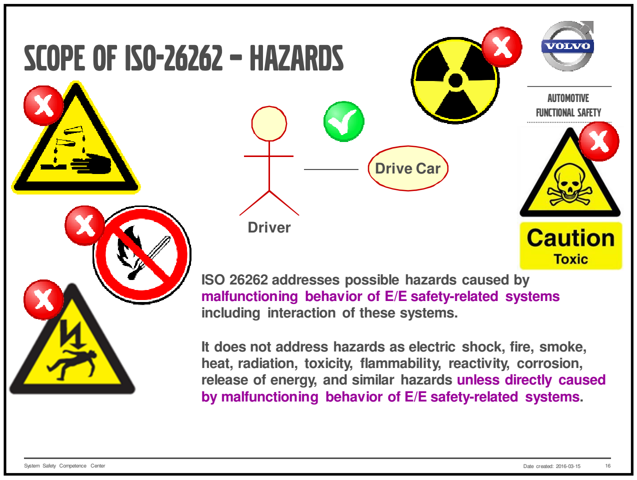


SCOPE OF ISO-26262 – ROAD VEHICLES

VOLVO
TOMOTIVE
NAL SAFETY

ISO 26262 is intended to be applied to safety-related systems that include one or more E/E systems and that are installed in series production passenger cars with a max gross weight up to 3,5 t.

System Safety Competence Center Date created: 2016-03-15 15



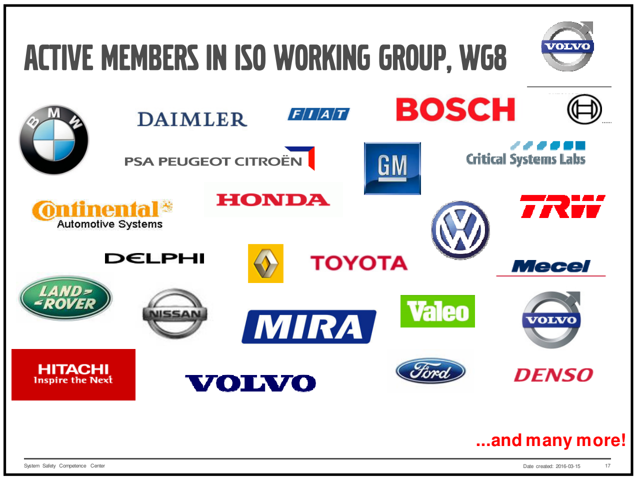
SCOPE OF ISO-26262 – HAZARDS

VOLVO
AUTOMOTIVE
FUNCTIONAL SAFETY
Driver
Drive Car
Caution
Toxic

ISO 26262 addresses possible hazards caused by malfunctioning behavior of E/E safety-related systems including interaction of these systems.

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

System Safety Competence Center Date created: 2016-03-15 16

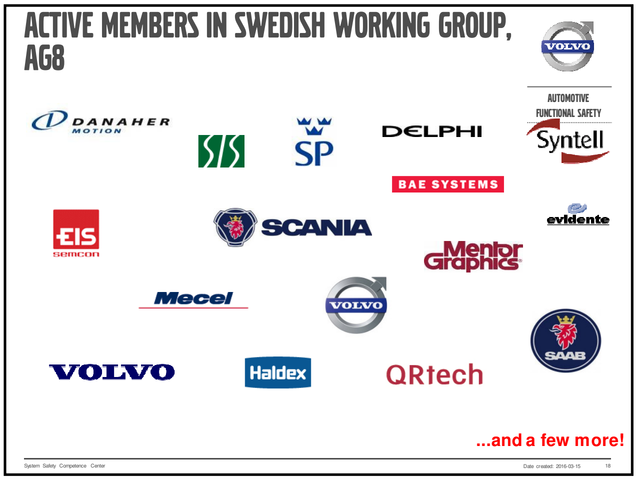


ACTIVE MEMBERS IN ISO WORKING GROUP, WG8

VOLVO
BMW
DAIMLER
FIAT
BOSCH
PSA PEUGEOT CITROËN
GM
Critical Systems Labs
Continental
Automotive Systems
HONDA
TRW
DELPHI
TOYOTA
Mecel
LAND ROVER
NISSAN
MIRA
Valeo
VOLVO
HITACHI
Inspire the Next
VOLVO
Ford
DENSO

...and many more!

System Safety Competence Center Date created: 2016-03-15 17



ACTIVE MEMBERS IN SWEDISH WORKING GROUP, AG8

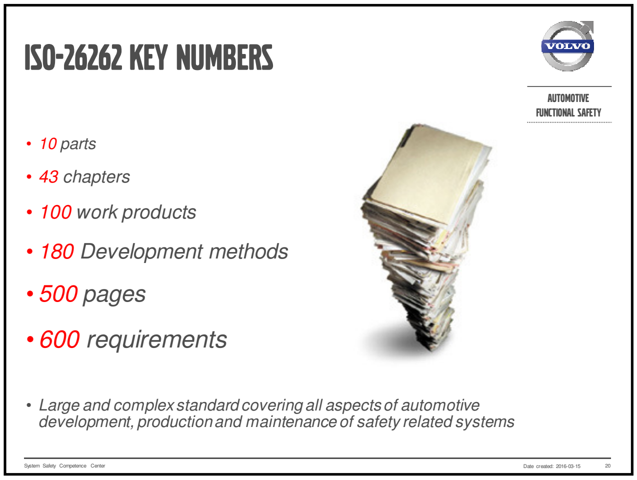
VOLVO
AUTOMOTIVE
FUNCTIONAL SAFETY
DANAHER
MOTION
SIS
SP
DELPHI
Syntell
BAE SYSTEMS
EIS
semcon
SCANIA
evidente
Mentor Graphics
Mecel
VOLVO
SAAB
VOLVO
Haldex
QRtech

...and a few more!

System Safety Competence Center Date created: 2016-03-15 18

OVERVIEW OF ISO-26262

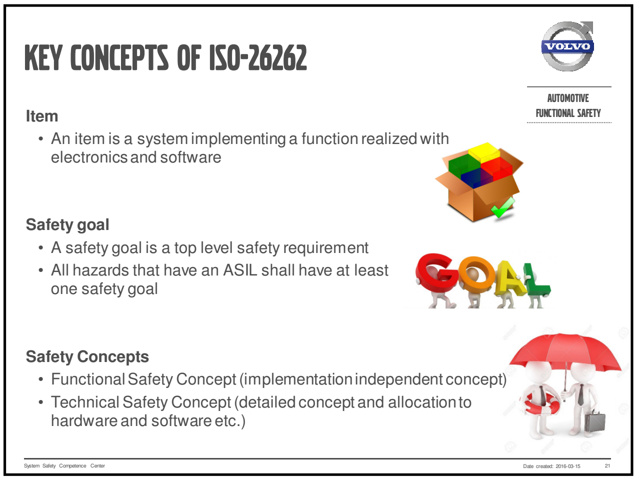
Part by part of the standard



ISO-26262 KEY NUMBERS

- *10 parts*
- *43 chapters*
- *100 work products*
- *180 Development methods*
- *500 pages*
- *600 requirements*

- *Large and complex standard covering all aspects of automotive development, production and maintenance of safety related systems*



KEY CONCEPTS OF ISO-26262

Item

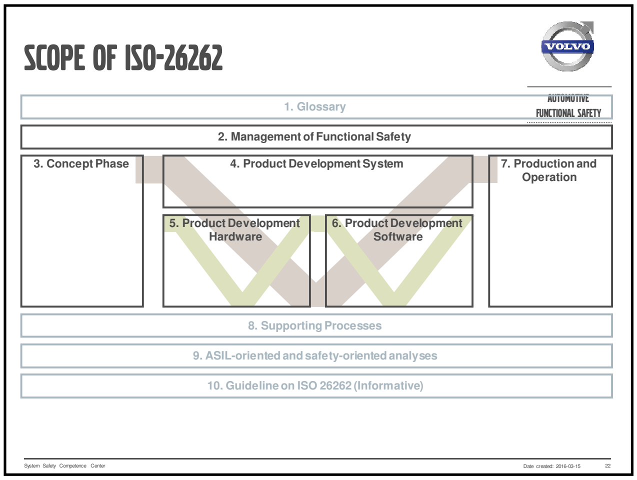
- An item is a system implementing a function realized with electronics and software

Safety goal

- A safety goal is a top level safety requirement
- All hazards that have an ASIL shall have at least one safety goal

Safety Concepts

- Functional Safety Concept (implementation independent concept)
- Technical Safety Concept (detailed concept and allocation to hardware and software etc.)



SCOPE OF ISO-26262

1. Glossary

2. Management of Functional Safety

3. Concept Phase

4. Product Development System

5. Product Development Hardware

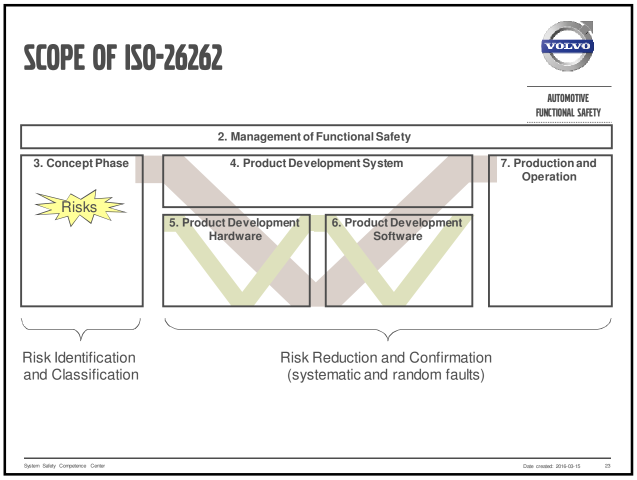
6. Product Development Software

7. Production and Operation

8. Supporting Processes

9. ASIL-oriented and safety-oriented analyses

10. Guideline on ISO 26262 (Informative)



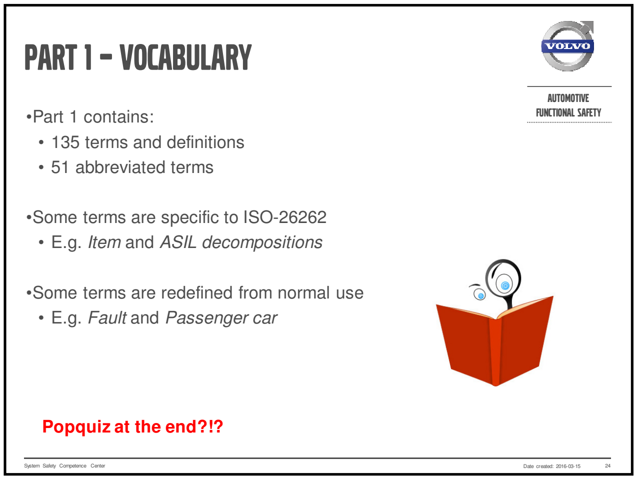
SCOPE OF ISO-26262

AUTOMOTIVE FUNCTIONAL SAFETY

2. Management of Functional Safety
3. Concept Phase
Risks
4. Product Development System
5. Product Development Hardware
6. Product Development Software
7. Production and Operation

Risk Identification and Classification

Risk Reduction and Confirmation (systematic and random faults)



PART 1 – VOCABULARY

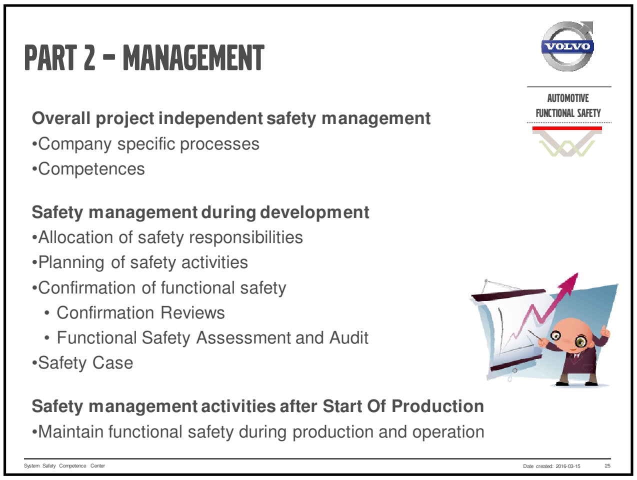
AUTOMOTIVE FUNCTIONAL SAFETY

•Part 1 contains:
- 135 terms and definitions
- 51 abbreviated terms

•Some terms are specific to ISO-26262
- E.g. *Item* and *ASIL decompositions*

•Some terms are redefined from normal use
- E.g. *Fault* and *Passenger car*

Popquiz at the end?!?



PART 2 – MANAGEMENT

AUTOMOTIVE FUNCTIONAL SAFETY

Overall project independent safety management

•Company specific processes

•Competences

Safety management during development

•Allocation of safety responsibilities

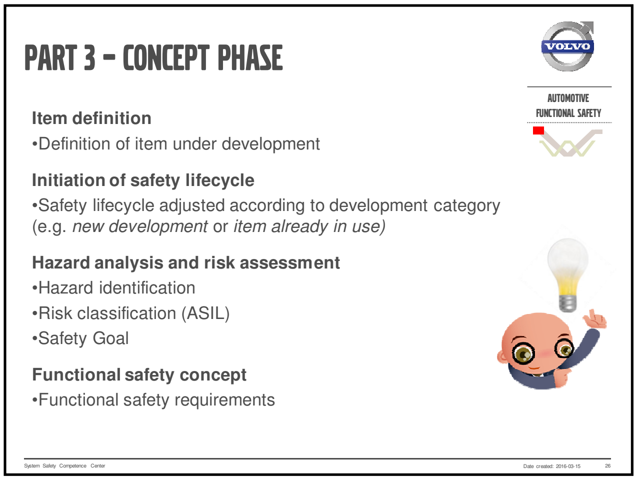
•Planning of safety activities

•Confirmation of functional safety
- Confirmation Reviews
- Functional Safety Assessment and Audit

•Safety Case

Safety management activities after Start Of Production

•Maintain functional safety during production and operation



PART 3 – CONCEPT PHASE

AUTOMOTIVE FUNCTIONAL SAFETY

Item definition

•Definition of item under development

Initiation of safety lifecycle

•Safety lifecycle adjusted according to development category (e.g. *new development* or *item already in use)*

Hazard analysis and risk assessment

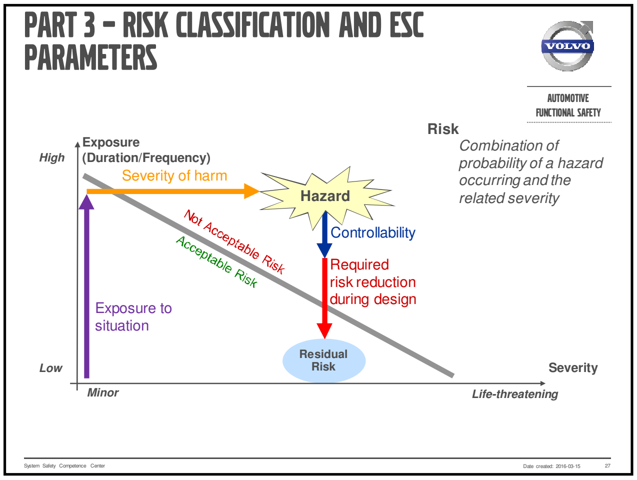
•Hazard identification

•Risk classification (ASIL)

•Safety Goal

Functional safety concept

•Functional safety requirements

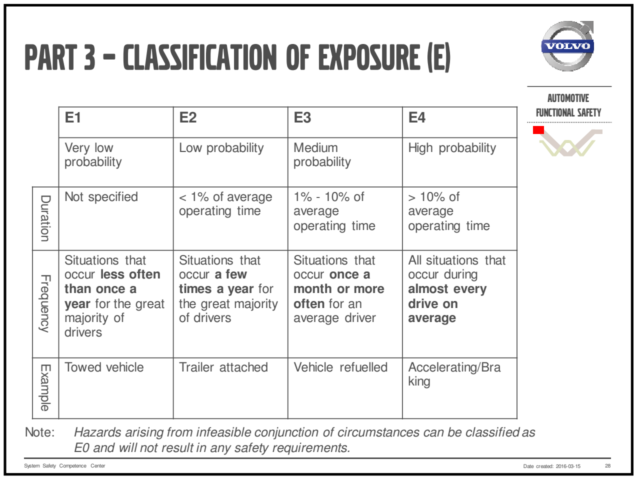


PART 3 – RISK CLASSIFICATION AND ESC PARAMETERS

AUTOMOTIVE FUNCTIONAL SAFETY

Risk

Combination of probability of a hazard occurring and the related severity

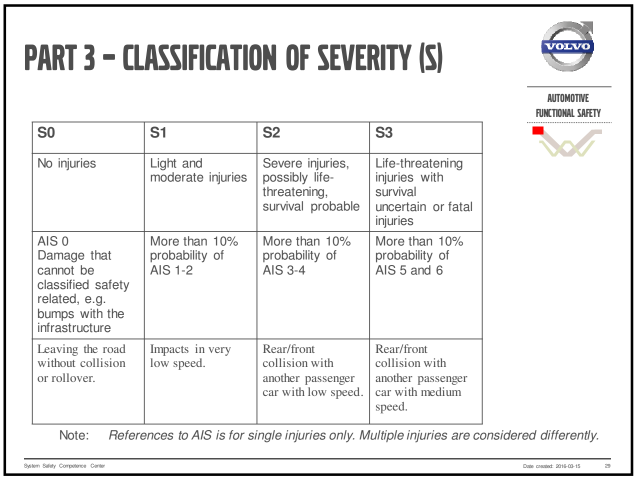


PART 3 – CLASSIFICATION OF EXPOSURE (E)

AUTOMOTIVE FUNCTIONAL SAFETY

	E1	E2	E3	E4
	Very low probability	Low probability	Medium probability	High probability
Duration	Not specified	< 1% of average operating time	1% - 10% of average operating time	> 10% of average operating time
Frequency	Situations that occur **less often than once a year** for the great majority of drivers	Situations that occur **a few times a year** for the great majority of drivers	Situations that occur **once a month or more often** for an average driver	All situations that occur during **almost every drive on average**
Example	Towed vehicle	Trailer attached	Vehicle refuelled	Accelerating/Bra king

Note: *Hazards arising from infeasible conjunction of circumstances can be classified as E0 and will not result in any safety requirements.*

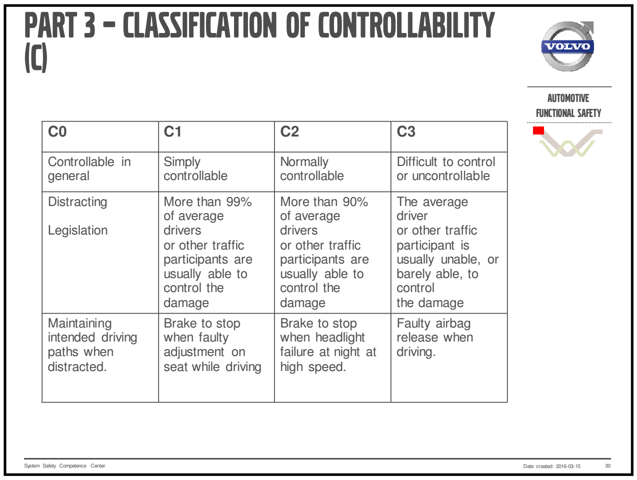


PART 3 – CLASSIFICATION OF SEVERITY (S)

AUTOMOTIVE FUNCTIONAL SAFETY

S0	S1	S2	S3
No injuries	Light and moderate injuries	Severe injuries, possibly life-threatening, survival probable	Life-threatening injuries with survival uncertain or fatal injuries
AIS 0 Damage that cannot be classified safety related, e.g. bumps with the infrastructure	More than 10% probability of AIS 1-2	More than 10% probability of AIS 3-4	More than 10% probability of AIS 5 and 6
Leaving the road without collision or rollover.	Impacts in very low speed.	Rear/front collision with another passenger car with low speed.	Rear/front collision with another passenger car with medium speed.

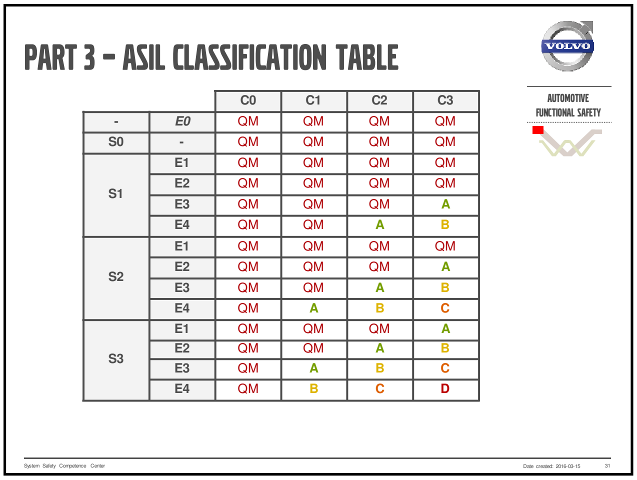
Note: *References to AIS is for single injuries only. Multiple injuries are considered differently.*



PART 3 – CLASSIFICATION OF CONTROLLABILITY (C)

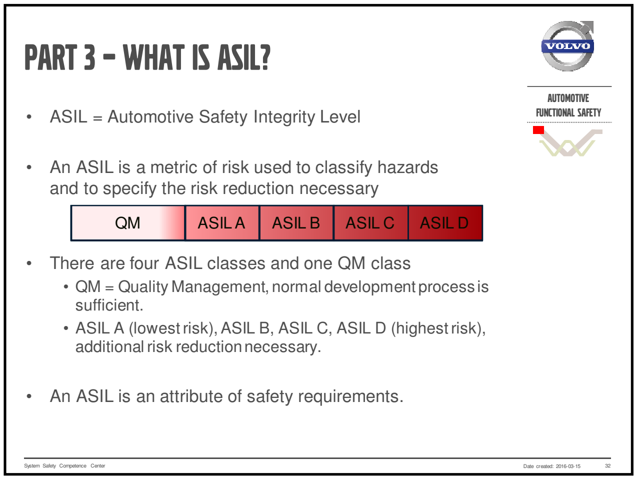
AUTOMOTIVE FUNCTIONAL SAFETY

C0	C1	C2	C3
Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable
Distracting Legislation	More than 99% of average drivers or other traffic participants are usually able to control the damage	More than 90% of average drivers or other traffic participants are usually able to control the damage	The average driver or other traffic participant is usually unable, or barely able, to control the damage
Maintaining intended driving paths when distracted.	Brake to stop when faulty adjustment on seat while driving	Brake to stop when headlight failure at night at high speed.	Faulty airbag release when driving.



PART 3 – ASIL CLASSIFICATION TABLE

		C0	C1	C2	C3
-	*E0*	QM	QM	QM	QM
S0	-	QM	QM	QM	QM
S1	E1	QM	QM	QM	QM
	E2	QM	QM	QM	QM
	E3	QM	QM	QM	A
	E4	QM	QM	A	B
S2	E1	QM	QM	QM	QM
	E2	QM	QM	QM	A
	E3	QM	QM	A	B
	E4	QM	A	B	C
S3	E1	QM	QM	QM	A
	E2	QM	QM	A	B
	E3	QM	A	B	C
	E4	QM	B	C	D

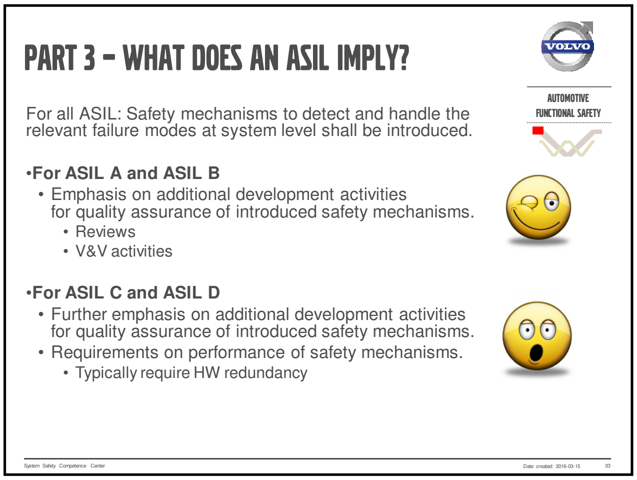


PART 3 – WHAT IS ASIL?

- ASIL = Automotive Safety Integrity Level
- An ASIL is a metric of risk used to classify hazards and to specify the risk reduction necessary

QM	ASIL A	ASIL B	ASIL C	ASIL D

- There are four ASIL classes and one QM class
  - QM = Quality Management, normal development process is sufficient.
  - ASIL A (lowest risk), ASIL B, ASIL C, ASIL D (highest risk), additional risk reduction necessary.
- An ASIL is an attribute of safety requirements.



PART 3 – WHAT DOES AN ASIL IMPLY?

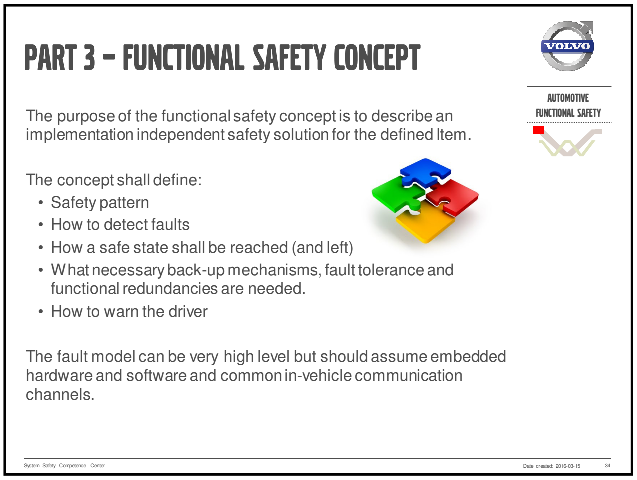
For all ASIL: Safety mechanisms to detect and handle the relevant failure modes at system level shall be introduced.

•For ASIL A and ASIL B

- Emphasis on additional development activities for quality assurance of introduced safety mechanisms.
  - 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



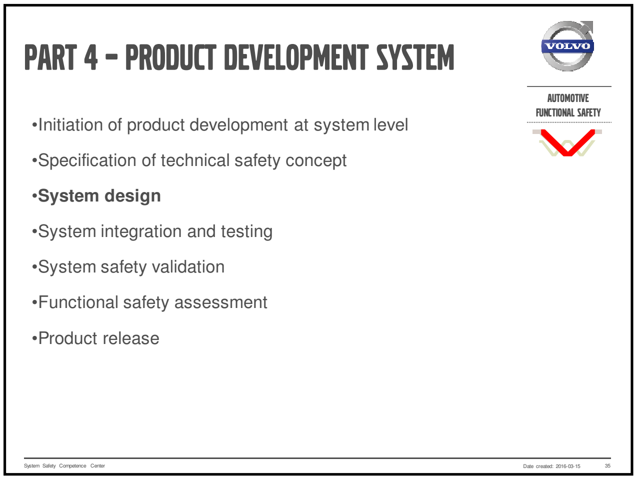
PART 3 – FUNCTIONAL SAFETY CONCEPT

The purpose of the functional safety concept is to describe an implementation independent safety solution for the defined Item.

The concept shall define:

- Safety pattern
- How to detect faults
- How a safe state shall be reached (and left)
- What necessary back-up mechanisms, fault tolerance and functional redundancies are needed.
- How to warn the driver

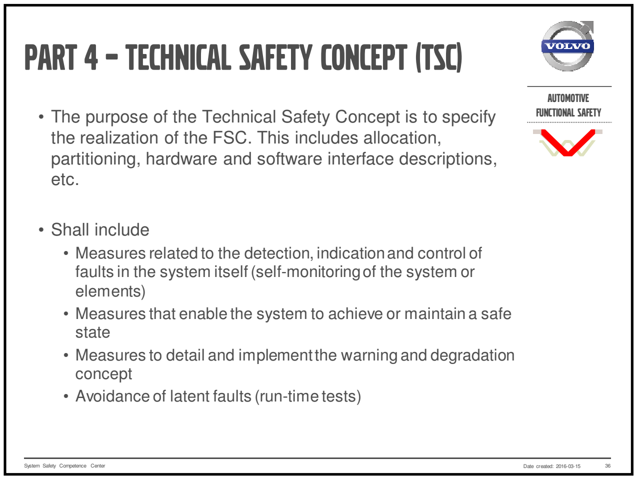
The fault model can be very high level but should assume embedded hardware and software and common in-vehicle communication channels.



PART 4 – PRODUCT DEVELOPMENT SYSTEM

AUTOMOTIVE FUNCTIONAL SAFETY

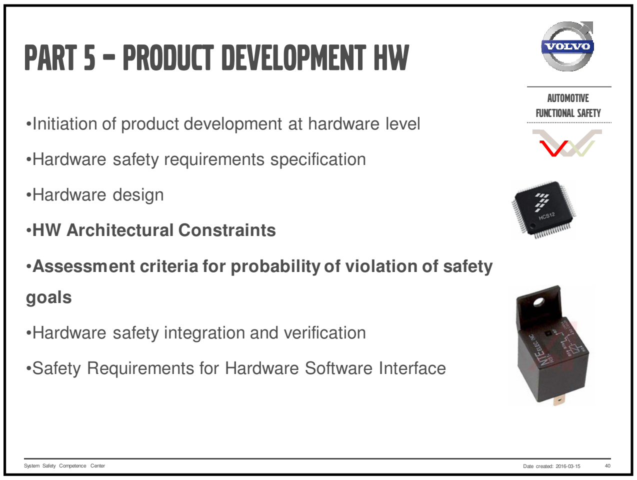
- •Initiation of product development at system level
- •Specification of technical safety concept
- **•System design**
- •System integration and testing
- •System safety validation
- •Functional safety assessment
- •Product release



PART 4 – TECHNICAL SAFETY CONCEPT (TSC)

AUTOMOTIVE FUNCTIONAL SAFETY

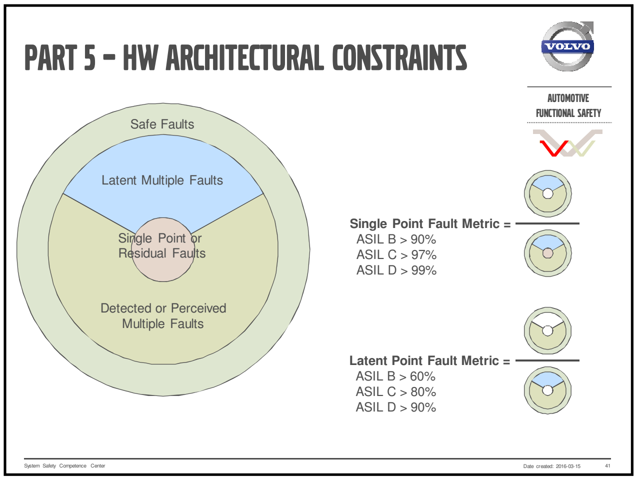
- The purpose of the Technical Safety Concept is to specify the realization of the FSC. This includes allocation, partitioning, hardware and software interface descriptions, etc.
- Shall include
  - Measures related to the detection, indication and control of faults in the system itself (self-monitoring of the system or elements)
  - Measures that enable the system to achieve or maintain a safe state
  - Measures to detail and implement the warning and degradation concept
  - Avoidance of latent faults (run-time tests)



PART 5 – PRODUCT DEVELOPMENT HW

AUTOMOTIVE FUNCTIONAL SAFETY

- •Initiation of product development at hardware level
- •Hardware safety requirements specification
- •Hardware design
- **•HW Architectural Constraints**
- **•Assessment criteria for probability of violation of safety goals**
- •Hardware safety integration and verification
- •Safety Requirements for Hardware Software Interface



PART 5 – HW ARCHITECTURAL CONSTRAINTS

AUTOMOTIVE FUNCTIONAL SAFETY

Safe Faults

Latent Multiple Faults

Single Point or Residual Faults

Detected or Perceived Multiple Faults

Single Point Fault Metric =

ASIL B > 90%

ASIL C > 97%

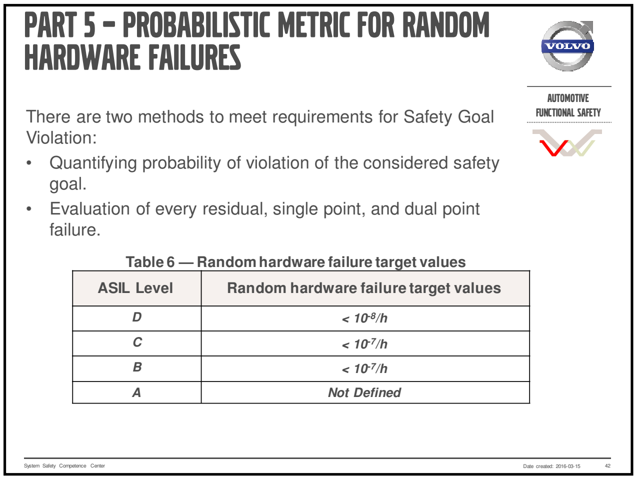
ASIL D > 99%

Latent Point Fault Metric =

ASIL B > 60%

ASIL C > 80%

ASIL D > 90%



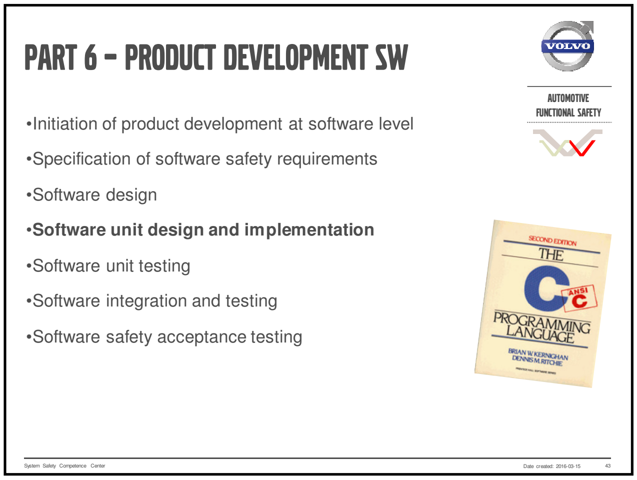
PART 5 – PROBABILISTIC METRIC FOR RANDOM HARDWARE FAILURES

There are two methods to meet requirements for Safety Goal Violation:

- Quantifying probability of violation of the considered safety goal.
- Evaluation of every residual, single point, and dual point failure.

Table 6 — Random hardware failure target values

ASIL Level	Random hardware failure target values
D	*< 10^{-8}/h*
C	*< 10^{-7}/h*
B	*< 10^{-7}/h*
A	*Not Defined*



PART 6 – PRODUCT DEVELOPMENT SW

•Initiation of product development at software level

•Specification of software safety requirements

•Software design

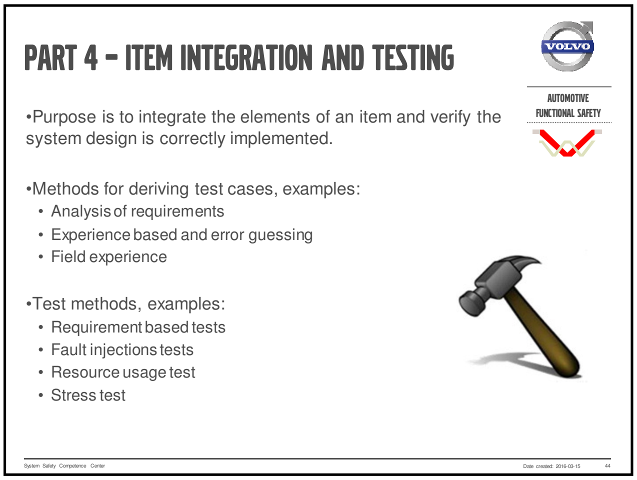
•Software unit design and implementation

•Software unit testing

•Software integration and testing

•Software safety acceptance testing

SECOND EDITION
THE
C
ANSI C
PROGRAMMING LANGUAGE
BRIAN W. KERNIGHAN
DENNIS M. RITCHIE

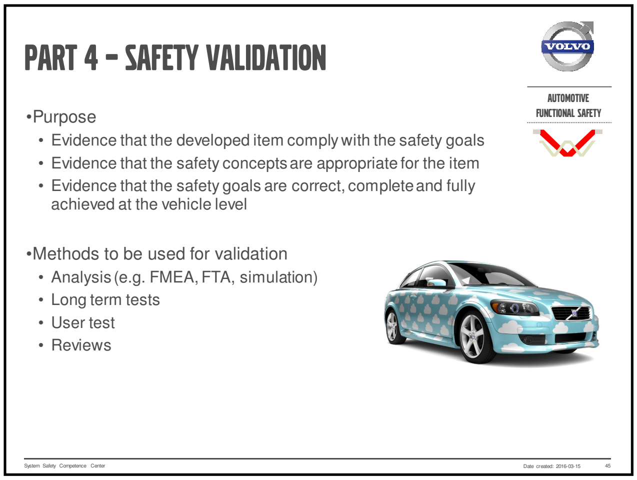


PART 4 – ITEM INTEGRATION AND TESTING

•Purpose is to integrate the elements of an item and verify the system design is correctly implemented.

•Methods for deriving test cases, examples:
- Analysis of requirements
- Experience based and error guessing
- Field experience

•Test methods, examples:
- Requirement based tests
- Fault injections tests
- Resource usage test
- Stress test



PART 4 – SAFETY VALIDATION

•Purpose
- Evidence that the developed item comply with the safety goals
- Evidence that the safety concepts are appropriate for the item
- Evidence that the safety goals are correct, complete and fully achieved at the vehicle level

•Methods to be used for validation
- Analysis (e.g. FMEA, FTA, simulation)
- Long term tests
- User test
- Reviews

PART 7 – PRODUCTION AND OPERATION

AUTOMOTIVE FUNCTIONAL SAFETY

Production

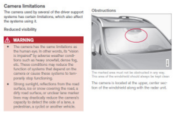
•Functional safety shall be ensured during production.

Operation, service, and decommissioning

•Assures that the required functional safety is maintained during operation of the vehicle.

•Includes requirements on

- user manual, (e.g. warnings/discalimer and safe usage)
- service instructions,
- field monitoring,
- Decommissioning instructions



Camera limitations

The camera used by several of the driver support systems has certain limitations, which also affect the systems using it.

Reduced visibility

⚠ WARNING

- The camera has the same limitations as the human eye. In other words, its "vision is impaired" by adverse weather conditions such as heavy snowfall, dense fog, etc. These conditions may reduce the function of systems that depend on the camera or cause these systems to temporarily stop functioning.
- Strong sunlight, reflections from the road surface, ice or snow covering the road, a dirty road surface, or unclear lane marker lines may drastically reduce the camera's capacity to detect the side of a lane, a pedestrian, a cyclist or another vehicle.

Obstructions

The marked area must not be obstructed in any way. This area of the windshield should always be kept clean

The camera is located at the upper, center section of the windshield along with the radar unit.

PART 8 – SUPPORTING PROCESSES

AUTOMOTIVE FUNCTIONAL SAFETY

•Interfaces within Distributed Development

•Overall Management of Safety Requirements

•Configuration Management

•Change Management

•**Verification**

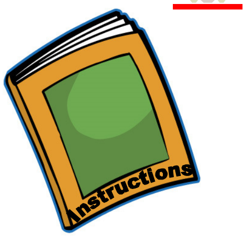
•Documentation

•Confidence in the use of Software Tools

•Qualification of Software Components

•Qualification of Hardware Components

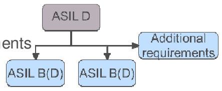
•Proven-in-use Argument



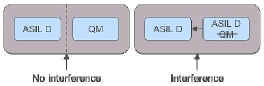
PART 9 – ASIL-ORIENTED AND SAFETY-ORIENTED ANALYSES

AUTOMOTIVE FUNCTIONAL SAFETY

- ASIL Decomposition
  - Decomposition of ASILs resulting in lower ASILs for redundant requirements



- Freedom from Interference
  - Addresses co-existence of elements with different ASILs (e.g. how to achieve independence between elements)



- Analysis of Dependent Failures
- Safety Analysis
  - Includes qualitative and quantitative analysis (e.g. FMEA, FTA)

PART 10 – GUIDELINE ON ISO-26262

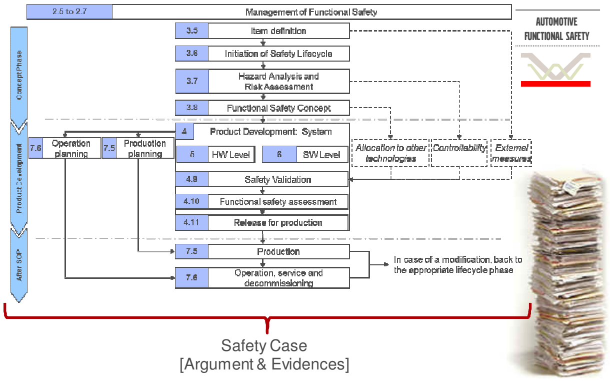
AUTOMOTIVE FUNCTIONAL SAFETY

Part 10 includes further informative guidelines of ISO-26262:

- General concepts
- Understanding Safety Case
- Introduction to the Safety Lifecycle concept
- Example of ASIL Decomposition

SUMMARY – ISO26262 SAFETY LIFECYCLE

AUTOMOTIVE FUNCTIONAL SAFETY


2.5 to 2.7
Management of Functional Safety
Concept Phase
Product Development
After SOP
3.5 Item definition
3.6 Initiation of Safety Lifecycle
3.7 Hazard Analysis and Risk Assessment
3.8 Functional Safety Concept
4 Product Development: System
7.6 Operation planning
7.5 Production planning
5 HW Level
6 SW Level
Allocation to other technologies
Controllability
External measures
4.9 Safety Validation
4.10 Functional safety assessment
4.11 Release for production
7.5 Production
7.6 Operation, service and decommissioning
In case of a modification, back to the appropriate lifecycle phase

Safety Case
[Argument & Evidences]

AUTOMOTIVE FUNCTIONAL SAFETY

ISO 26262 SECOND EDITION

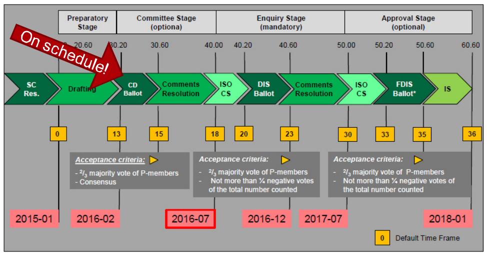
Revision Work

ISO International Organization for Standardization

ISO/TC22/SC32/WG8
Functional Safety

AUTOMOTIVE FUNCTIONAL SAFETY

Schedule for 2nd edition of ISO 26262



Acceptance criteria:
- $^2/_3$ majority vote of P-members
- Consensus

Acceptance criteria:
- $^2/_3$ majority vote of P-members
- Not more than ¼ negative votes of the total number counted

Acceptance criteria:
- $^2/_3$ majority vote of P-members
- Not more than ¼ negative votes of the total number counted

Egbert Fritzsche, VDA, 2014-12-12 4

ISO International Organization for Standardization

ISO/TC22/SC32/WG8
Functional Safety

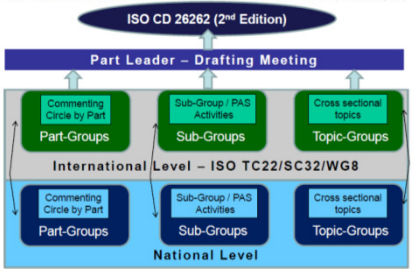
AUTOMOTIVE FUNCTIONAL SAFETY

Workflow for revision of ISO 26262 towards 2nd ED (see also following slides)

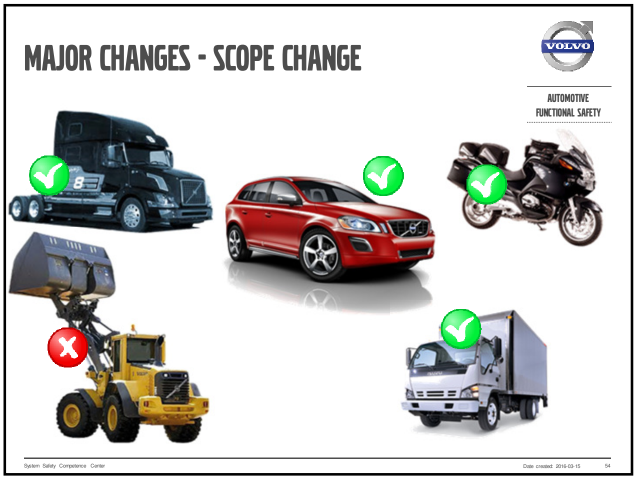
Commenting team
Working on Part level, will continue part handling after CD-Ballot
(lead by PL)

Sub-Groups:
To be created for CD-development, to be closed after CD-Publication
(lead by SGL)

Topic Groups:
To be created for CD-development, to be closed after CD-Publication
(lead by TL)

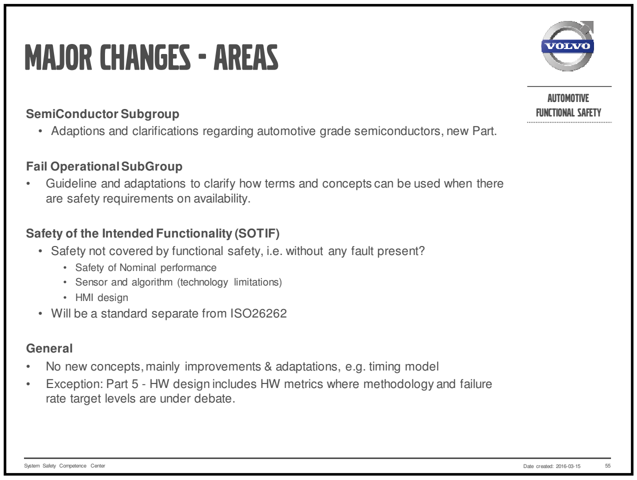

ISO CD 26262 (2nd Edition)
Part Leader – Drafting Meeting
Commenting Circle by Part
Part-Groups
Sub-Group / PAS Activities
Sub-Groups
Cross sectional topics
Topic-Groups
International Level – ISO TC22/SC32/WG8
Commenting Circle by Part
Part-Groups
Sub-Group / PAS Activities
Sub-Groups
Cross sectional topics
Topic-Groups
National Level

Egbert Fritzsche, VDA 2014-12-12 6



MAJOR CHANGES - SCOPE CHANGE

AUTOMOTIVE FUNCTIONAL SAFETY



MAJOR CHANGES - AREAS

AUTOMOTIVE FUNCTIONAL SAFETY

SemiConductor Subgroup

- Adaptions and clarifications regarding automotive grade semiconductors, new Part.

Fail Operational SubGroup

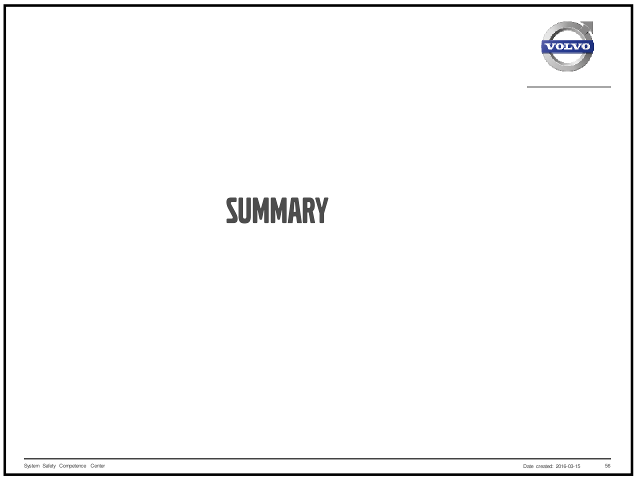
- Guideline and adaptations to clarify how terms and concepts can be used when there are safety requirements on availability.

Safety of the Intended Functionality (SOTIF)

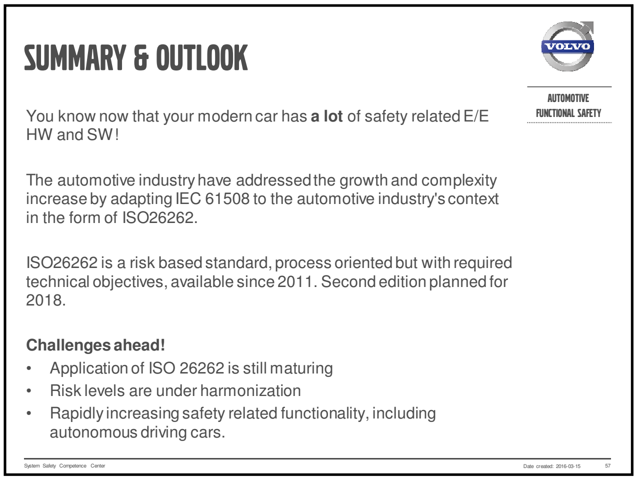
- Safety not covered by functional safety, i.e. without any fault present?
  - Safety of Nominal performance
  - Sensor and algorithm (technology limitations)
  - HMI design
- Will be a standard separate from ISO26262

General

- No new concepts, mainly improvements & adaptations, e.g. timing model
- Exception: Part 5 - HW design includes HW metrics where methodology and failure rate target levels are under debate.



SUMMARY



SUMMARY & OUTLOOK

AUTOMOTIVE FUNCTIONAL SAFETY

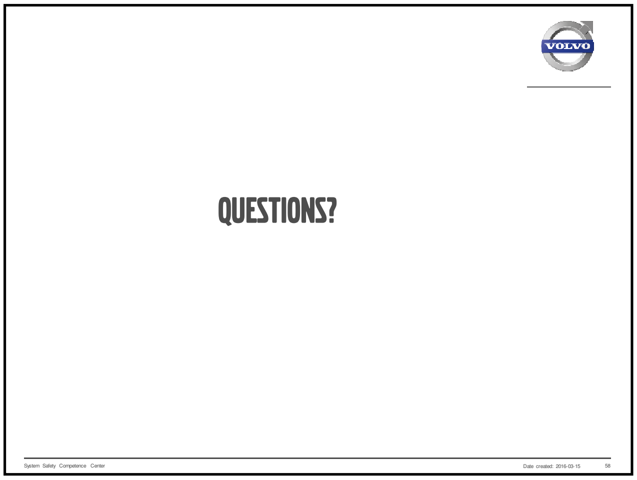
You know now that your modern car has **a lot** of safety related E/E HW and SW!

The automotive industry have addressed the growth and complexity increase by adapting IEC 61508 to the automotive industry's context in the form of ISO26262.

ISO26262 is a risk based standard, process oriented but with required technical objectives, available since 2011. Second edition planned for 2018.

Challenges ahead!

- Application of ISO 26262 is still maturing
- Risk levels are under harmonization
- Rapidly increasing safety related functionality, including autonomous driving cars.



QUESTIONS?