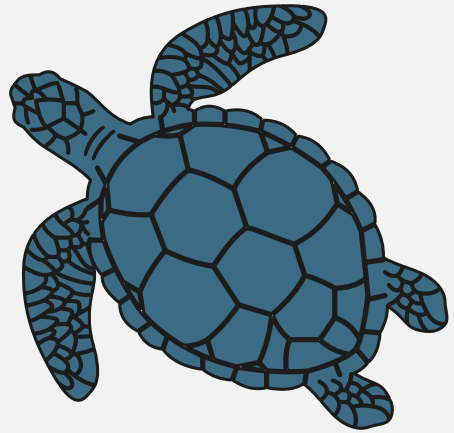
FuSa (ISO26262)

Quick overview

v. 240827

License



https://creativecommons.org/licenses/by-nc-nd/4.0/

Dmitry Samersoff

Lead of VW Quality Support at Luxoft Automotive

MEB-Platform, starting with the Volkswagen ID.3. **It is the first software component developed by Luxoft to achieve the VW series production quality level for the MEB platform.**

dms@samersoff.net

www.samersoff.net

Process and Quality consultant.

VDA licensed ASPICE Provisioning Assessor

OpenJDK Reviewer, JVM senior developer.

ORACLE Sun microsystems Luxoft A DXC Technology Company

FuSA Key TeRMS

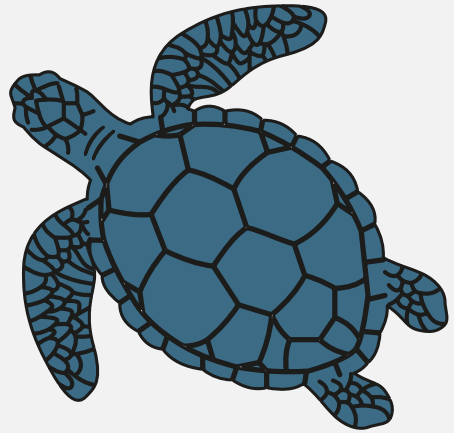
DEFINITION OF FUNCTIONAL SAFETY by ISO 26262-1

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

- FUSA is dedicated for Electric and Electronic (E/E) systems
- FUSA dictates additional measures to reduce the risk in case of malfunction
- Gaps in required functionality are not a subject of FUSA
- Special purpose vehicles are not covered by ISO 26262
- Trucks and buses partially covered by 2nd edition
- Motorcycles are covered by special subset of ISO 26262
- Safety of intended functionality and ADAS is SOTIF, not ISO 26262

The part of vehicle that is subject of safety concept is **Item**, items are defined on a vehicle level.

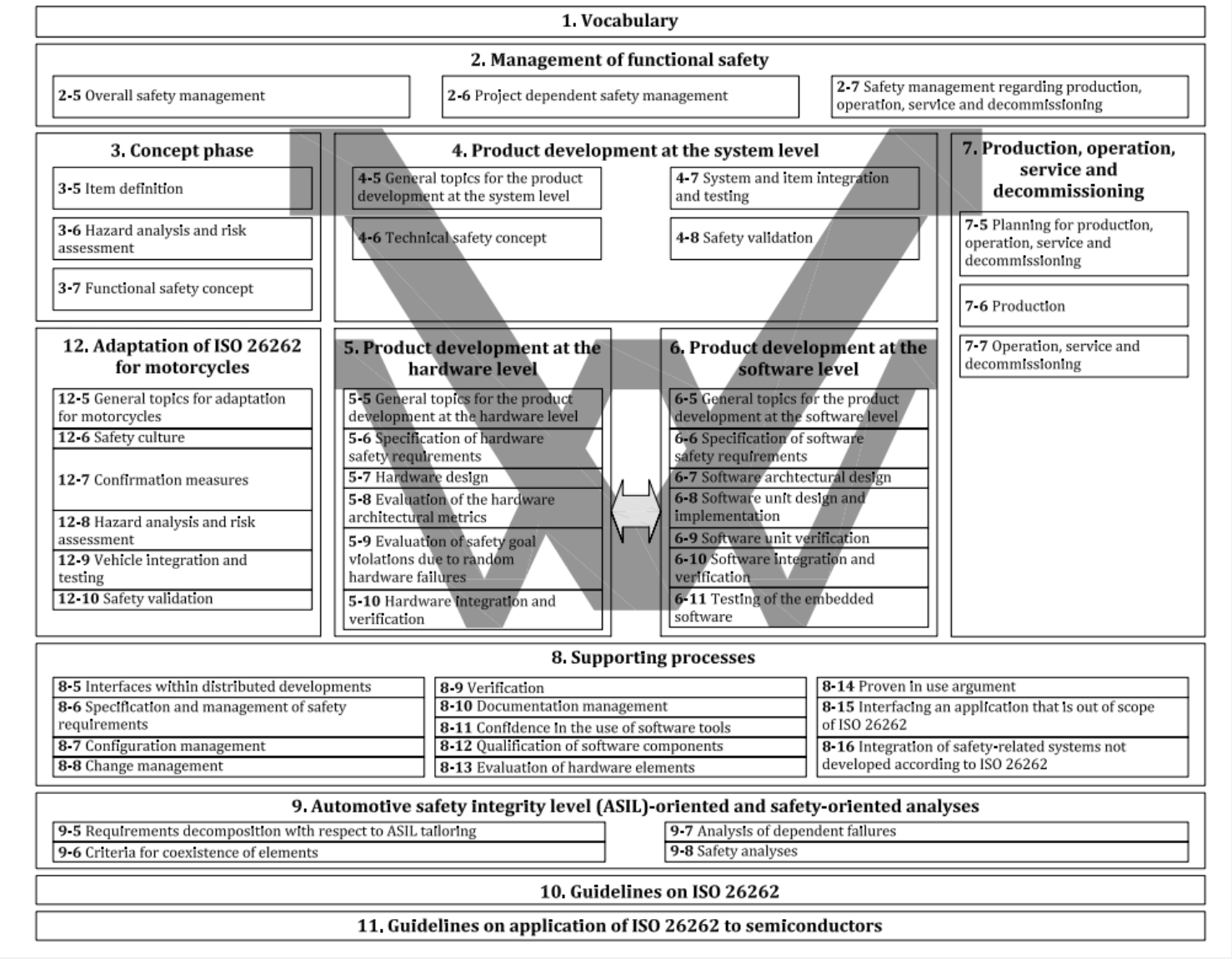
The minimal entity of safety concept is **Element**



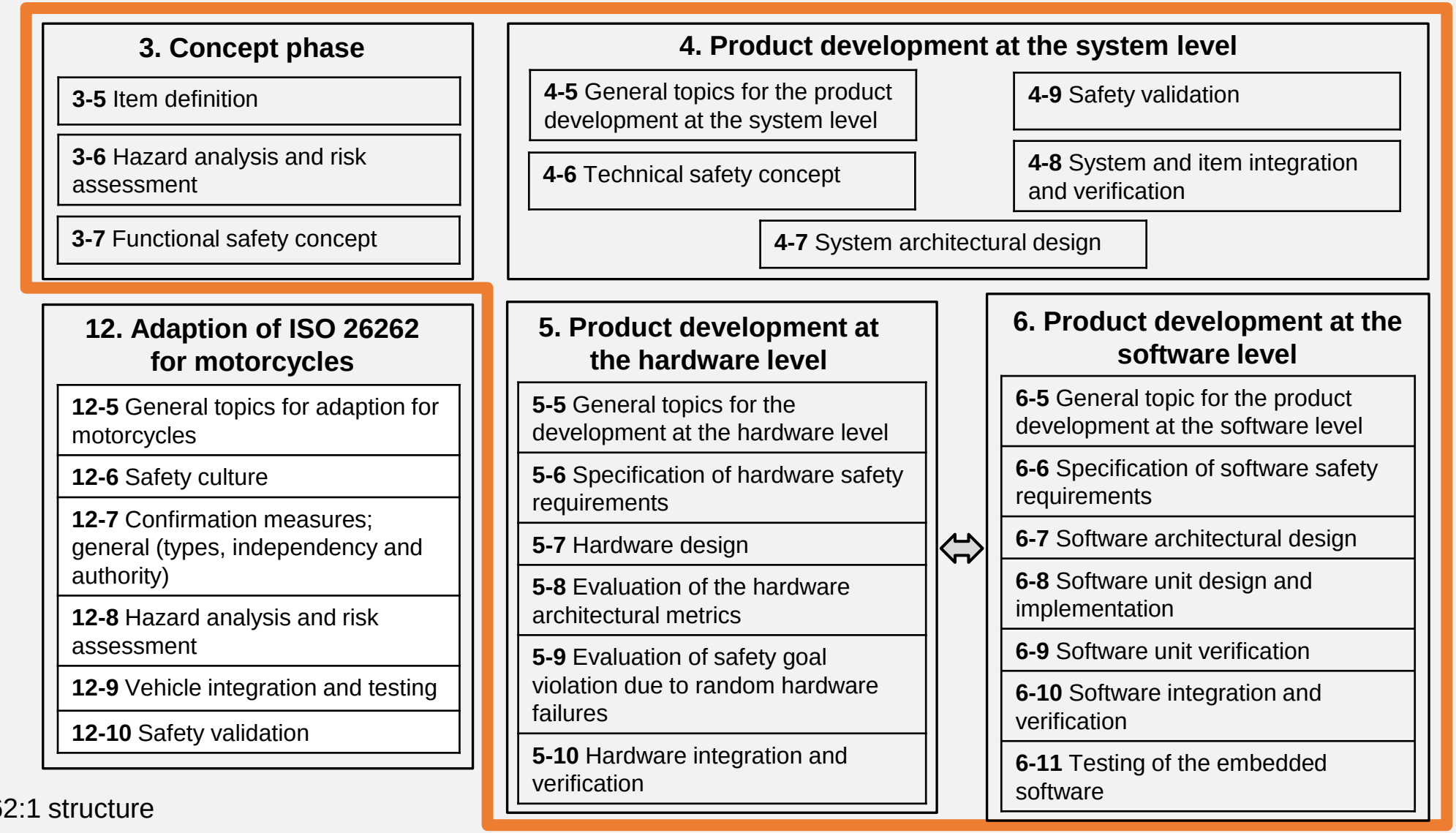
Safety manager role

- to define and assign the roles and responsibilities regarding the safety activities
- to perform an impact analysis at the item level
- to perform an impact analysis at the element level
- to define the tailored safety activities
- to plan the safety activities
- to coordinate and track the progress of the safety activities
- to plan the distributed developments
- to ensure a correct progression of the safety activities
- to create a comprehensible safety case
- to judge whether the item achieves functional safety
- to decide at the end of development whether the item, or element(s), can be released

Overview of standard

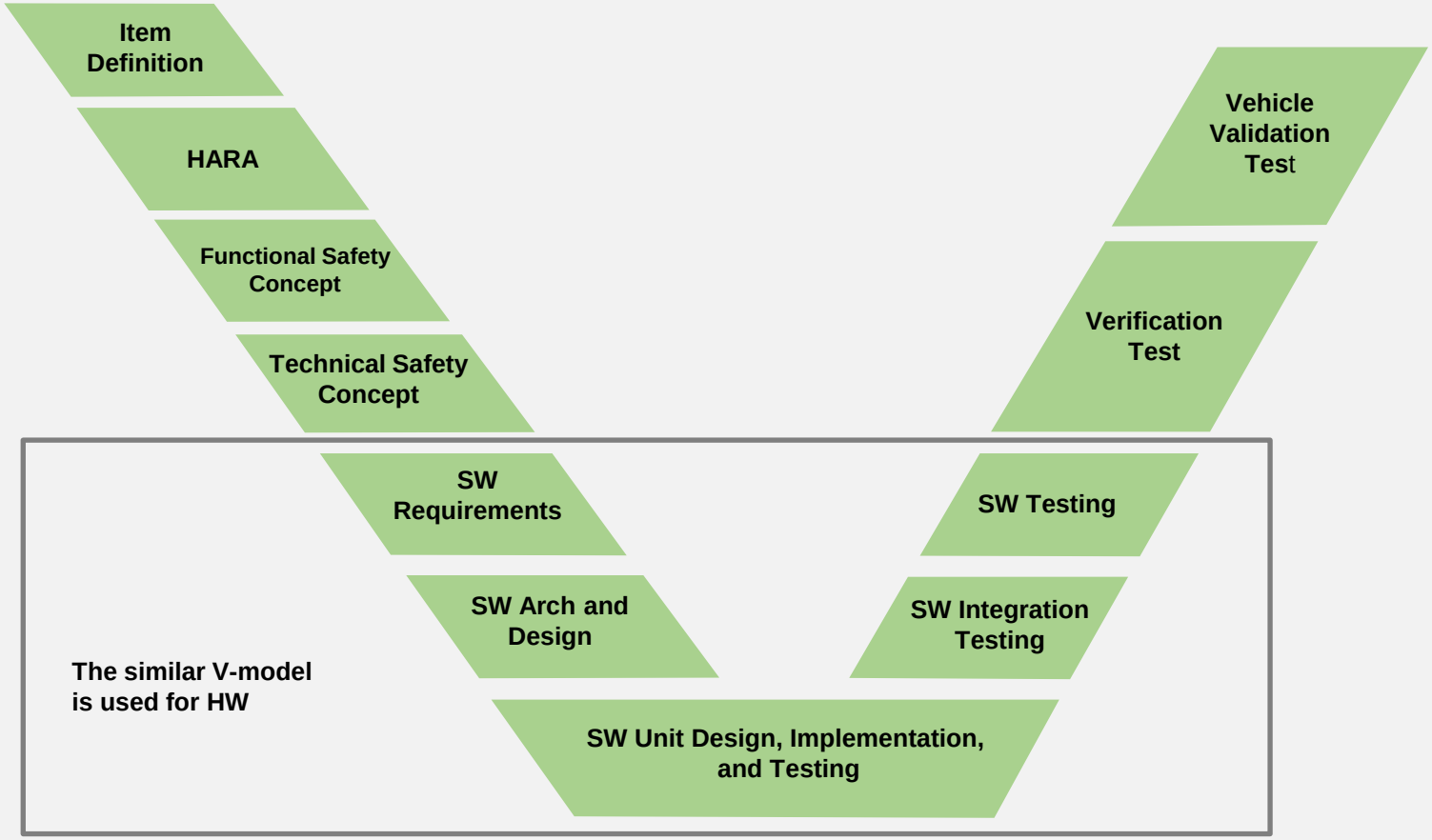


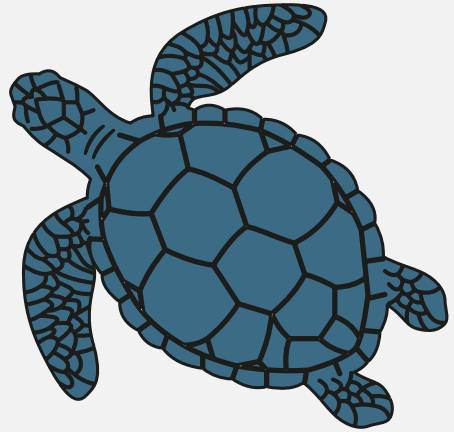
Development Process



ISO 26262:1 structure

V-model


Item Definition
HARA
Functional Safety Concept
Technical Safety Concept
SW Requirements
SW Arch and Design
SW Unit Design, Implementation, and Testing
SW Integration Testing
SW Testing
Verification Test
Vehicle Validation Test
The similar V-model is used for HW

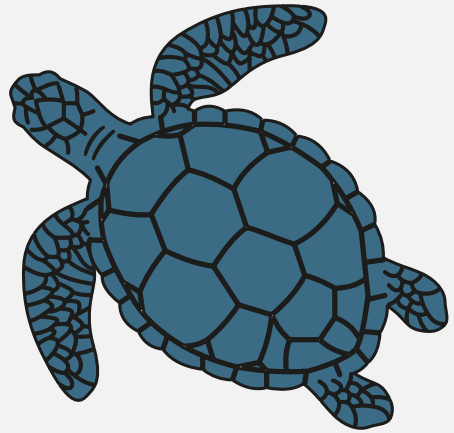


Supporting processes

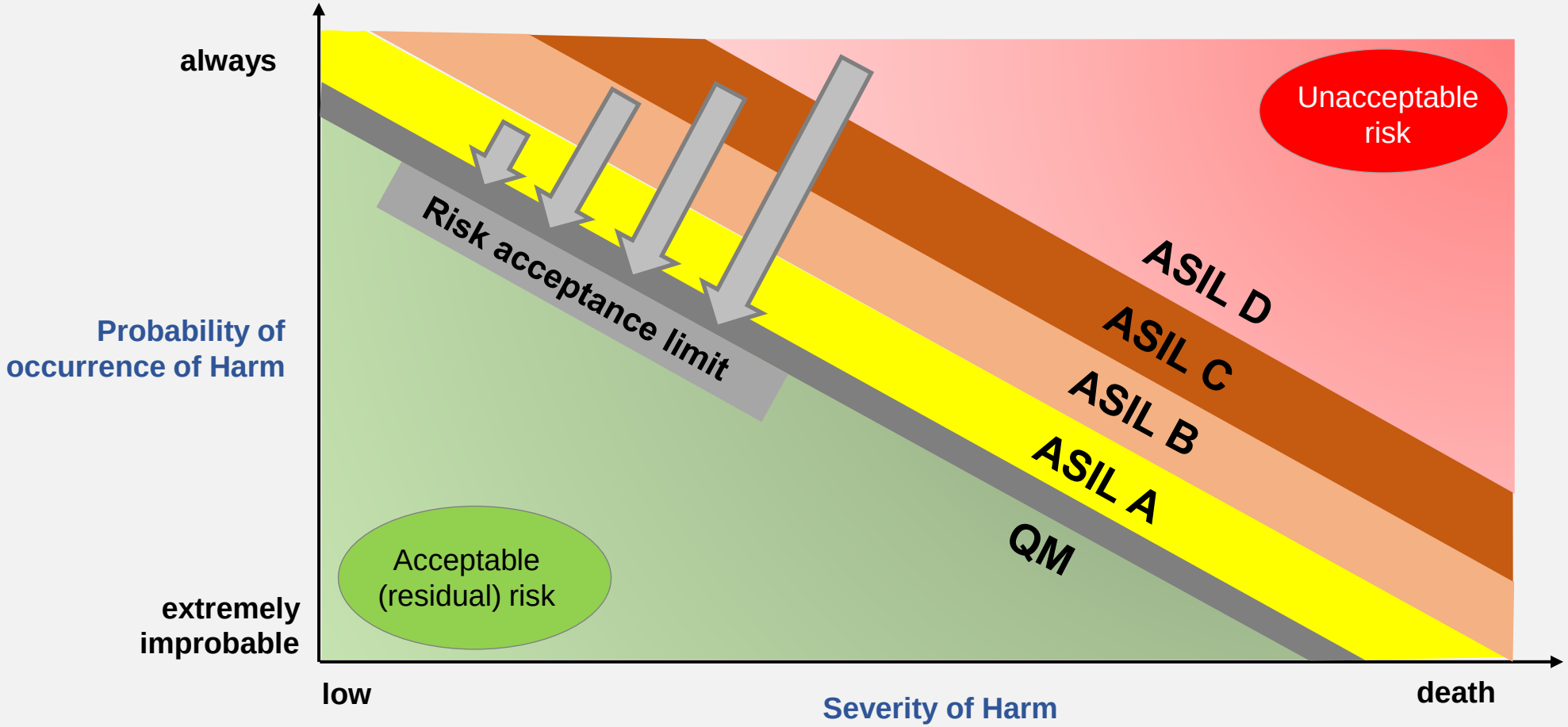
- Quality management – *set up overall quality framework, FuSa requires additional measures on top of regular quality assurance.*
- Requirements management – *set up requirements elicitation, modification, review and traceability with respect to FuSa.*
- Configuration management – *set up release and baselining policy to ensure consistence of verification and validation.*
- Change management – *set up a process to ensure that direct and indirect FuSa implication of any changes is carefully evaluated.*
- Problem resolution management – *set up cross-team escalation path, to ensure that all FuSa related deviations are recorded and properly addressed.*

Automotive Safety Integrity Level (ASIL)

- 5-step scale (QM, A, B, C, D). ASIL D is the highest value
- ASIL X is the attribute of requirement, on the each level
- QM means that standard quality assurance (see IATF 16949 or ISO 9001) is sufficient
- ASIL X means that additional risk reduction measures are required
- The defined safety goals at a vehicle level are the top-level safety requirements
- Underlying requirements inherit ASIL level
- ASIL level could be lowered for redundant paths or secondary faults
- High ASIL level could be achieved by several redundant paths with lower level



RISK: the probability + extent to damage



The ASIL is described as the distance from the risk acceptance limit

HARA: Hazard Analysis and Risk Assessment

- Severity

  (S0 – no injuries … S3 – head detached)
- Exposure (Duration or Frequency)

  (E0 – incredible … E4 high probable, more than 10% operational time)
- Controllability

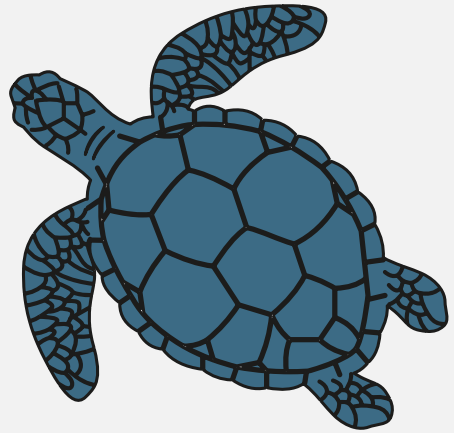
  (C0 – controllable in general … C3 uncontrollable, less than 90% can control)

HARA: Hazard Analysis and Risk Assessment

		C1	C2	C3
S1	E3			ASIL A
S1	E4		ASIL A	ASIL B
S2	E2			ASIL A
S2	E3		ASIL A	ASIL B
S2	E4	ASIL A	ASIL B	ASIL C
S3	E1			ASIL A
S3	E2		ASIL A	ASIL B
S3	E3	ASIL A	ASIL B	ASIL C
S3	E4	ASIL B	ASIL C	ASIL D

IN and OUT context development

- The requirements are car specific
- The Car Maker is responsible to provide HARA results to a vendor
- The development is IN-Context if exact requirements of exact car are defined
- The development is OUT-of-Context if it is based on a set of assumptions treated as requirements
- VDA-702 – pre ranked situation catalog for out-of-context development



Verification steps

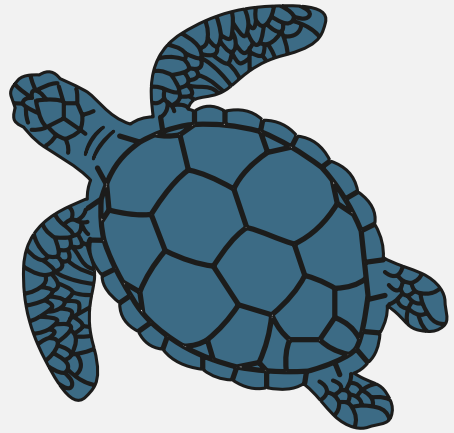
Method		ASIL			
		A	B	C	D
1a	Verification by walk-through	++	+	o	o
1b	Verification by inspection	+	++	++	++
1c	Semi-formal verification	+	+	++	++

Test method	SW Unit tests				Software Integration test			
	A	B	C	D	A	B	C	D
Requirements based test	++	++	++	++	++	++	++	++
Interface test	++	++	++	++	++	++	++	++
Fault injection test	+	+	+	++	+	+	++	++
Resource usage test	+	+	+	++	+	+	+	++
Back-to-back test	+	+	++	++	+	+	++	++

Method to verify the structural coverage	Software Unit level			
	A	B	C	D
Statement coverage	++	++	++	++
Branch coverage	++	++	++	++
MC/DC (Modified Condition / Decision Coverage)	+	+	+	++

Legend:
++ - required
+ - recommended
o - neither recommended nor not recommended

- Software verification plan and other work products are required
- No target goals are defined by ISO 26262
- Project-specific goals have to be set and justified
- Exceptions from MISRA etc rules have to be justified



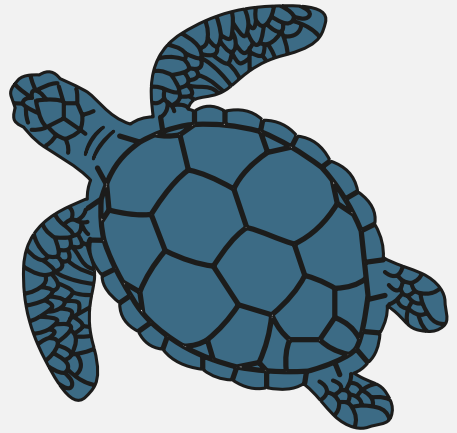
Example: Steering wheel lock

- Safety goal 1:

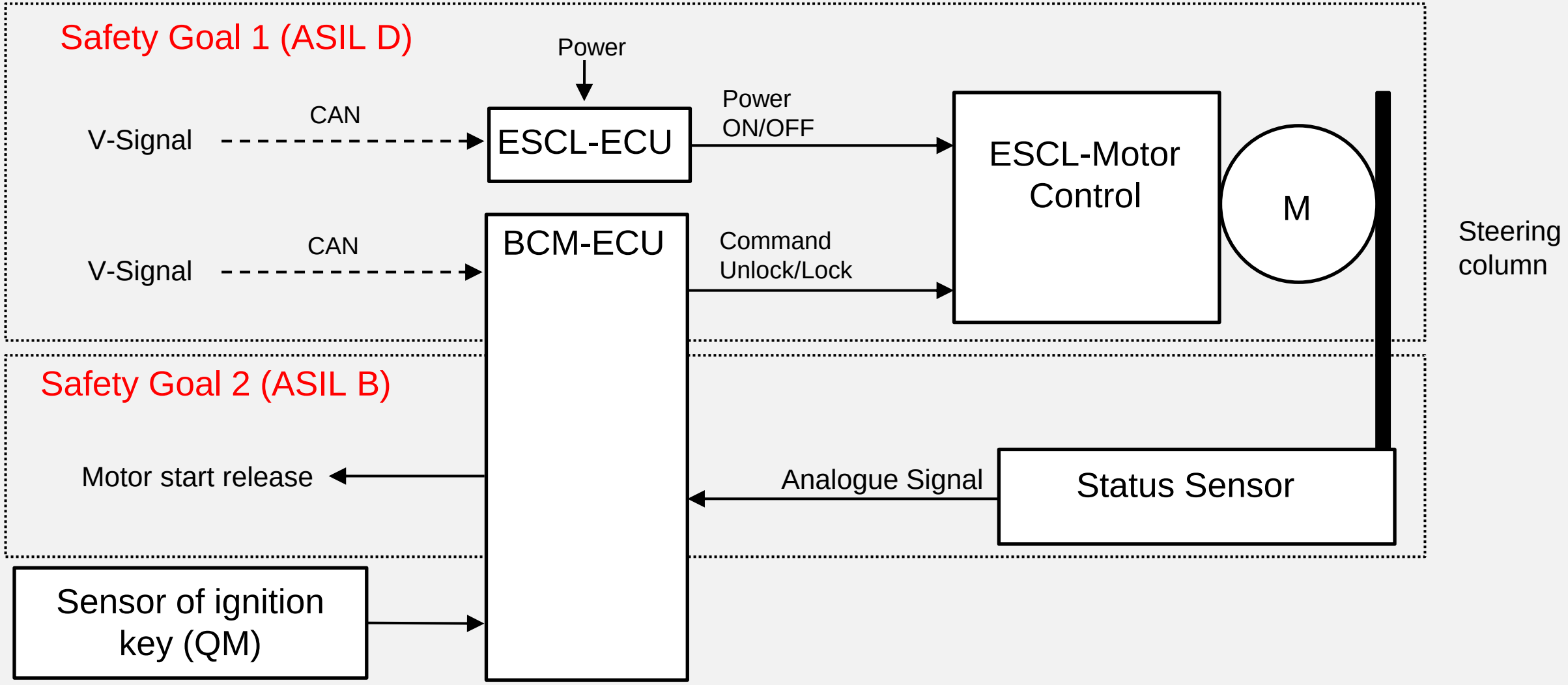
  When the car is moving, the steering wheel must not be locked.

- Safety goal 2:

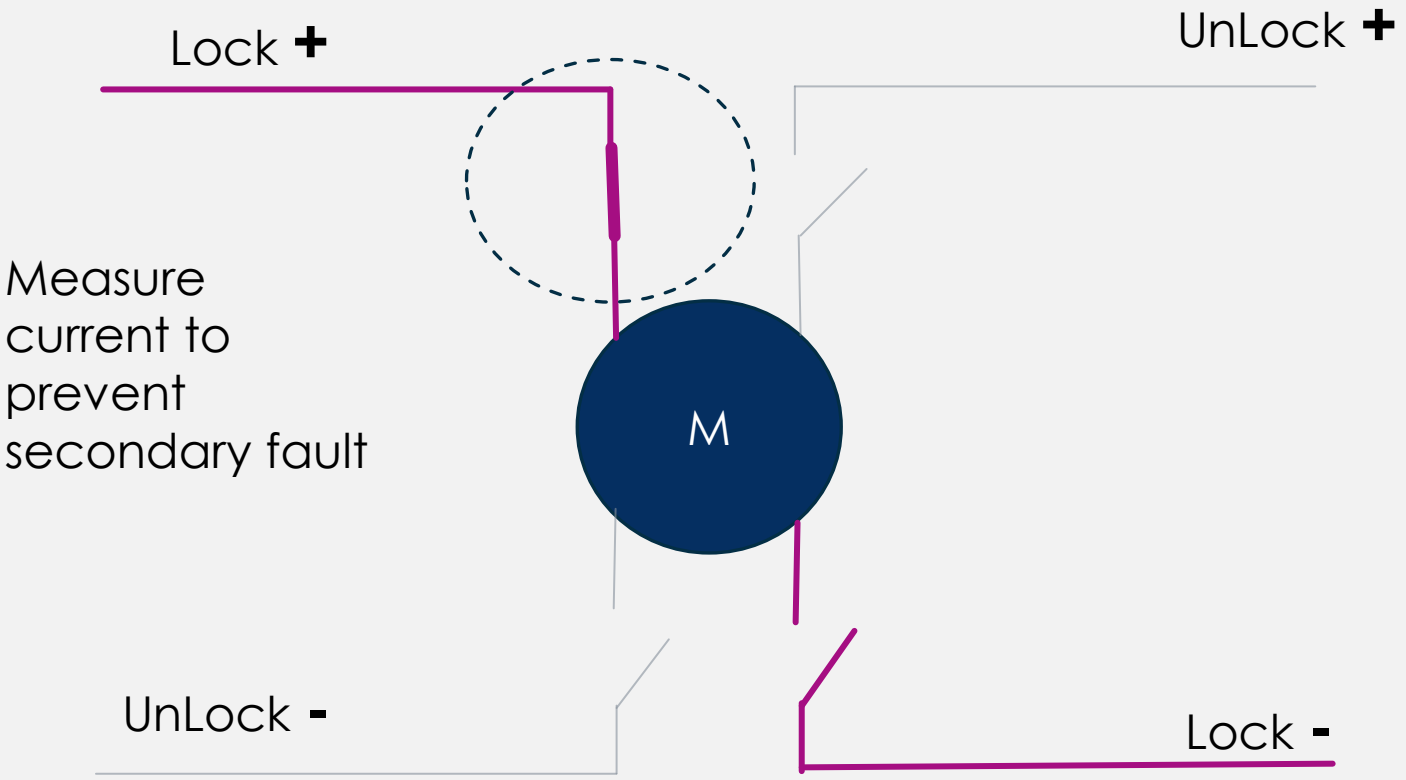
  If the steering wheel is not unlocked, the car must not start moving.



ASIL B(D) decomposition

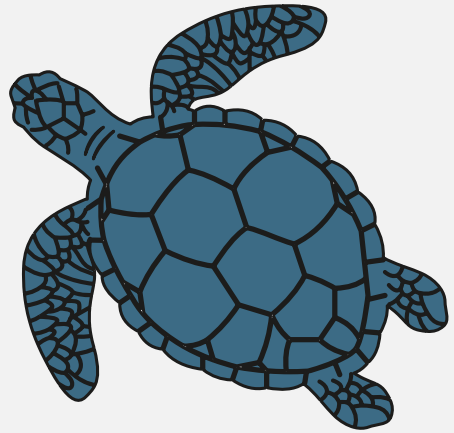


Secondary fault



SOTIF and other standards

Cause of hazardous event	Within scope of
E/E System or Software failure	ISO 26262
Performance limitations or insufficient situation awareness, with or without reasonable foreseeable misuse	ISO/PAS 21448:2019 (SOTIF)
Reasonable foreseeable misuse (user confusion, user overload)	ISO/PAS 21448:2019 (SOTIF)
Attack exploiting vehicle security vulnerabilities	ISO 21434/SAE J3061
Impact from active Infrastructure or V-to-V communication, external devices and cloud services	ISO 20077
Impact from car surrounding (passive infrastructure, environmental conditions)	ISO/PAS 21448:2019 (SOTIF)



Key SOTIF Concept

- SOTIF define Use-Case, Scene, Scenario
- The scenarios classified to: (1) known safe, (2) known unsafe, (3) unknown unsafe, (4) unknown safe.
- The goal of SOTIF : maximize (1), evaluate (2), minimize (3)
- SOTIF methods are:
  - Identify and evaluate risks associated with the intended functionality
  - Identify and evaluate hazardous use cases
  - Improve the system design as necessary through functional improvement or use case restriction to reduce risk
- Verify and validate the appropriateness of the design with respect to the SOTIF
- STPA (Systems-Theoretic Process Analysis) is a SOTIF hazard analysis technique
  - Accidents are caused by inadequate control.
  - Control actions are provided to affect a controlled process;
- See Nancy Leveson's book “Engineering a Safer World”

Thank you!

https://www.samersoff.net

dms@samersoff.net