Model-Based Software Design

LAB 1

ISO26262:3

Concept Phase

Jacopo Sini

Politecnico di Torino

Dip. Automatica e Informatica

jacopo.sini@polito.it

Objectives of this laboratory

The objectives of this laboratory are to:

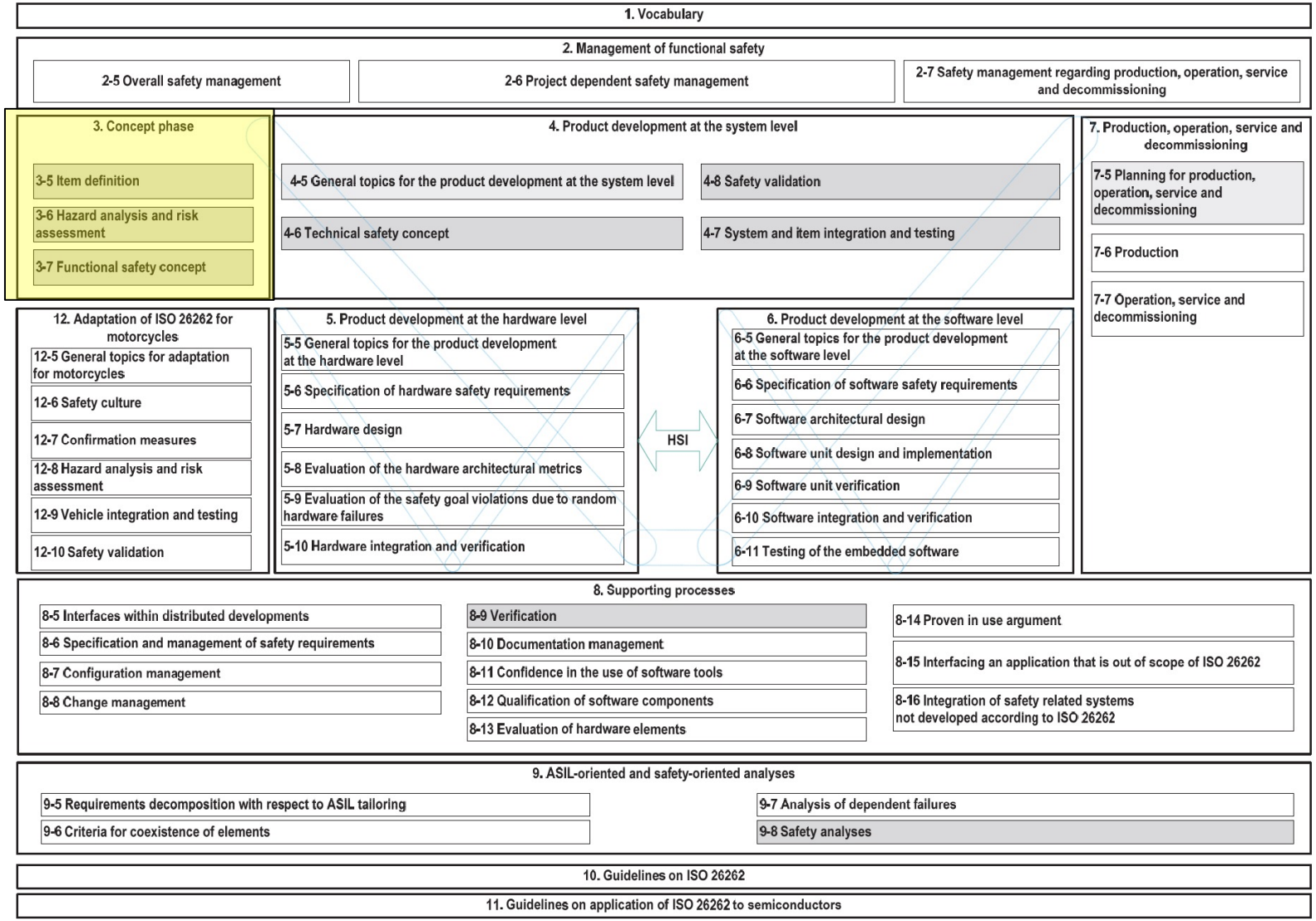
- Prepare the item definition for a Skyhook Controller (SHC)
- Perform the Hazard Analysis and Risk Assessment (HARA) on this item

Assessment information

The laboratory report must be delivered in PDF format by 19:00 on 23/03 through Elaborati section of the course page on Portale della Didattica.

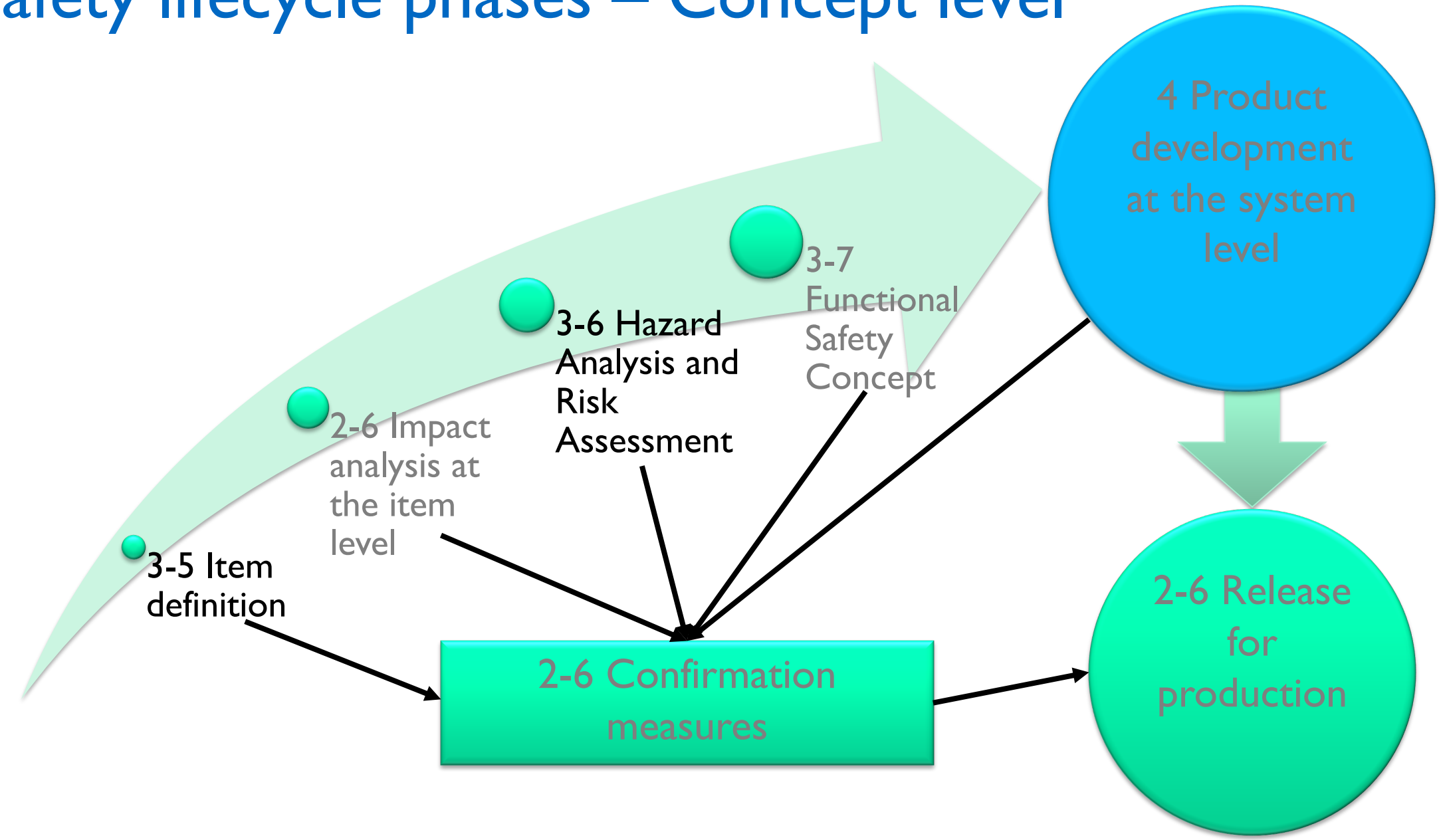
First page of the report must contain name, surname and student ID of the working group (max 2 people).

ISO 26262 Concept Phase



Source: ISO 26262:2018 Figure 1 — Overview of ISO 26262

Safety lifecycle phases – Concept level



Legal situation

Topics to be investigated:

- Legal requirements for homologation
  - Legally binding
    - EU directives (Europe)
    - ECE regulations (Europe)
    - FMVSS (USA)
- Product liability
  - Recommended application of IEC, ISO, EN or DIN standards (“state of the art”)

Steps in the concept phase

3-5 Item definition

- Scope (elements)
- Functional requirements, legal requirements, operating conditions, requirements by and upon other item

~~2-6 Impact analysis~~

- ~~Evaluate the implication of the modifications with regard to functional safety~~
- ~~Identify and descripe the safety activities to be performed, based on the impact of the modifications~~

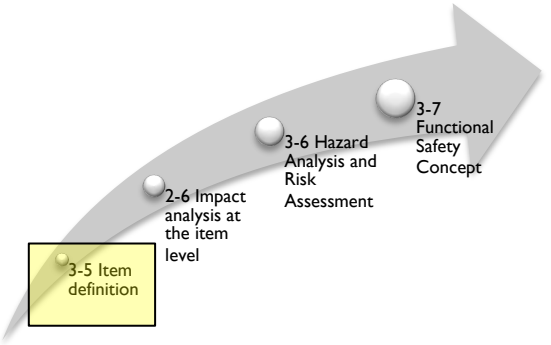
3-6 Hazard analysis

- Identification of potential hazards and establishing the risk potential by normative method
- Determining the required Automotive Safety integrity Level (ASIL) and the related safety goals

~~3-7 Functional safety concept~~

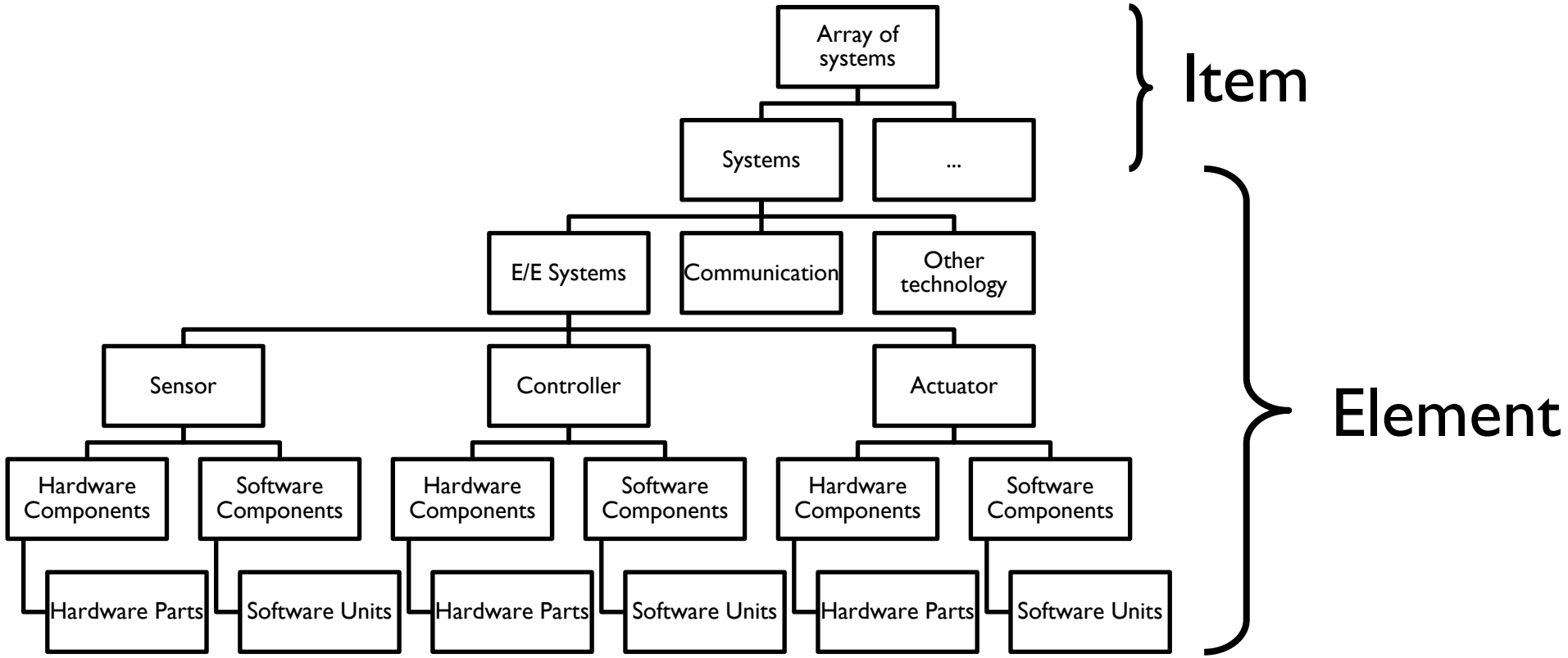
- ~~Functional concept to achieve the safety goals~~
- ~~Derivaton of parameters~~
  - ~~Safe State~~
  - ~~FTTI~~
  - ~~...~~

Item

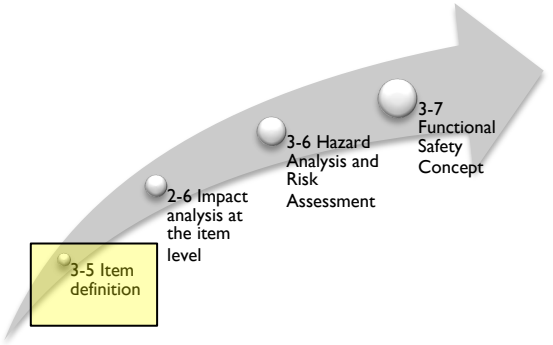


According to the ISO26262-1, an item is:

"System or combination of systems, to which ISO26262 is applied, that implements a function or part of a function at the vehicle level"

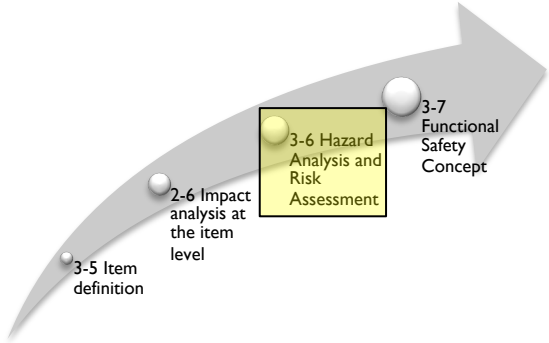


Item definition



- An item definition takes into account:
  - Functional requirements for the item
    - Item description
    - Functional behavior
    - Preliminary block diagram
  - Environmental conditions for the intended use
  - Legal requirements
  - Known safety requirements
  - Elements of the item
  - Requirements by and upon other items

Hazard analysis



1. Situation Analysis and Hazard Identification

- Systematic specification of the driving situation

2. Hazard Classification

- Derivation of the *risk parameters* in terms of **severity**, **exposure**, and **controllability**

3. ASIL determination

- Combining the risk parameters using the **Risk Matrix**

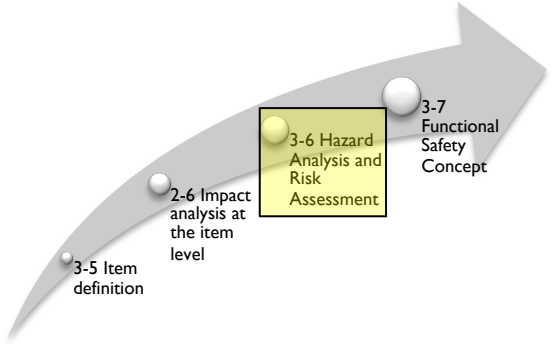
4. Safety Objectives Definition

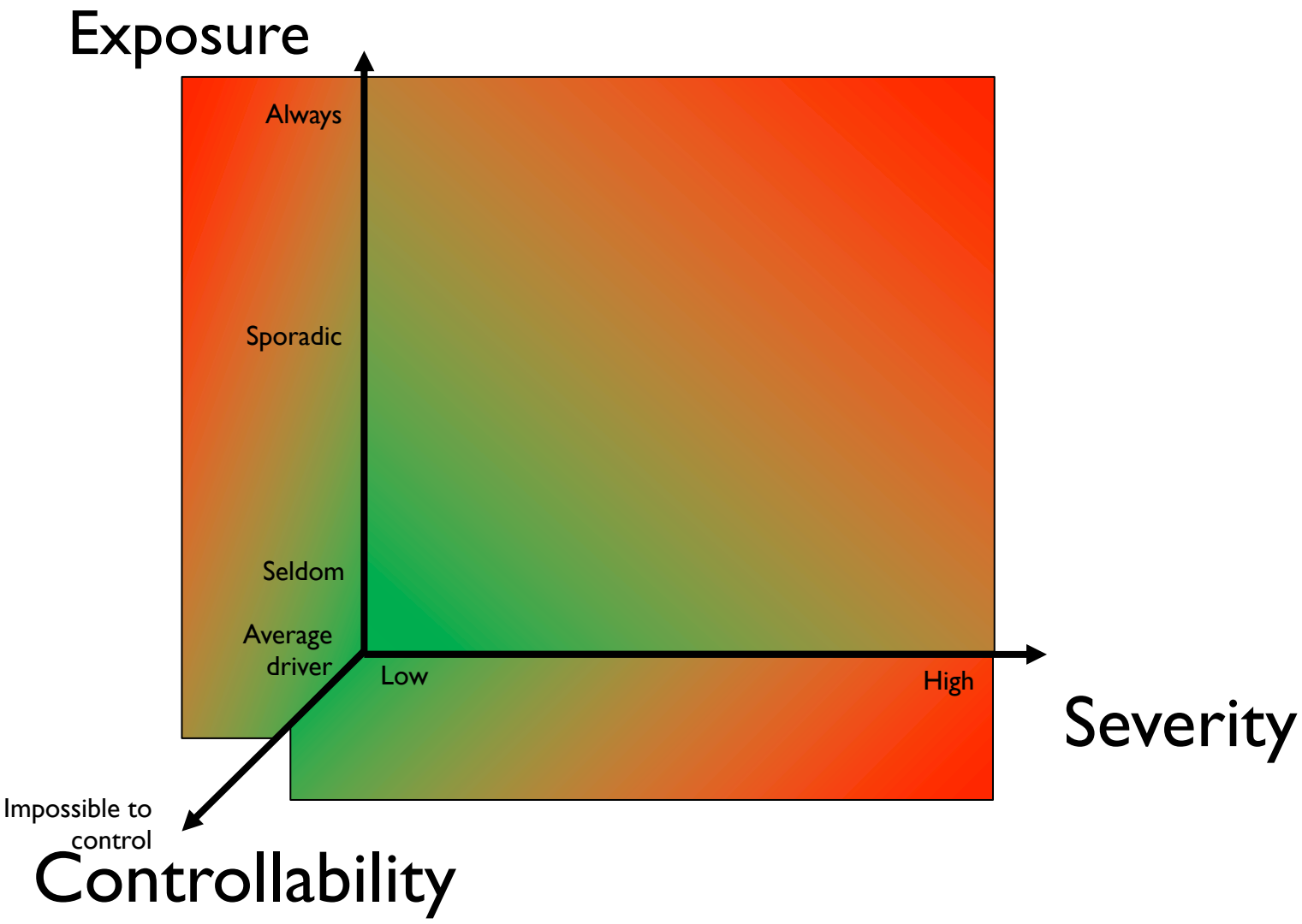
- Description of the **Safety Goals**

5. Review

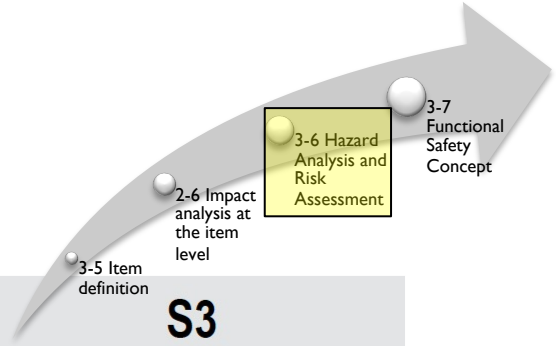
- Check for completeness, accuracy and consistency of the classifications

Derivation of risk parameters





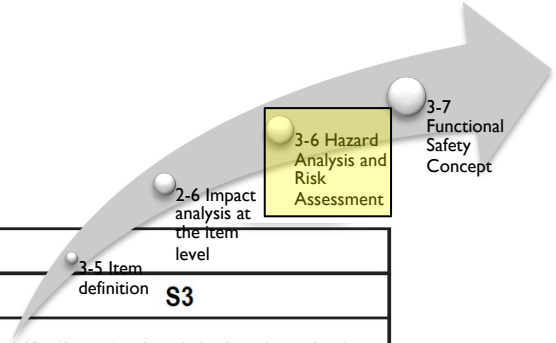
Severity (1)



ISO 26262-3 ,Table B.1: Examples of severity classification

Class	S0	S1	S2	S3
Description	No injuries	light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain) or fatal injuries
Reference for single injuries (from AIS scale)	AIS 0 and less than 10 % probability of AIS 1-6 Damage that cannot be classified safety-related	more than 10% probability of AIS 1-6 (and not S2 or S3)	more than 10% probability of AIS 3-6 (and not S3)	more than 10% probability of AIS 5-6

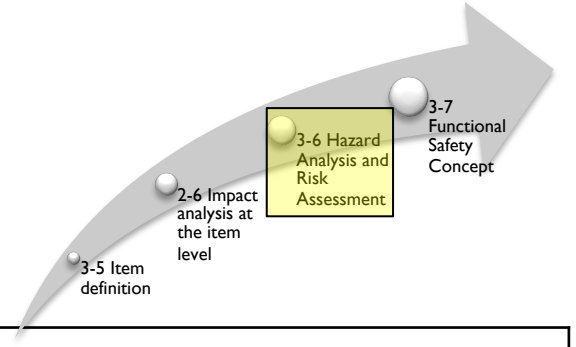
Severity (2)



ISO 26262-3 ,Table B.1: Examples of severity classification

	Class of severity			
	S0	**S1**	**S2**	**S3**
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries
Reference for single injuries **(from AIS scale)**	AIS 0 and less than 10 % probability of AIS 1-6 Damage that cannot be classified safety-related	More than 10 % probability of AIS 1-6 (and not S2 or S3)	More than 10 % probability of AIS 3-6 (and not S3)	More than 10 % probability of AIS 5-6
Examples	Bumps with road side infrastructure Pushing over roadside post, fence, etc. Light grazing damage Damage entering/ exiting parking space Leaving the road without collision or rollover	Side impact with a narrow stationary object, e.g. crashing into a tree (impact to passenger cell) **with very low speed** Rear/front collision with another passenger car **with very low speed** Front collision (e.g. rear ending another vehicle, semi trailer, etc.) **without passenger compartment deformation**	Side impact with a narrow stationary object, e.g. passenger car crashing into a tree (impact to passenger cell) **with low speed** Rear/front collision with another passenger car **with low speed** Pedestrian / bicycle accident **with low speed**	Side impact with a narrow stationary object, e.g. passenger car crashing into a tree (impact to passenger cell) **with medium speed** Rear/front collision with another vehicle **with medium speed** Front collision (e.g. rear ending another vehicle, semi trailer, etc.) **with passenger compartment deformation** Pedestrian / bicycle accident **(e.g. 2-lane road)**

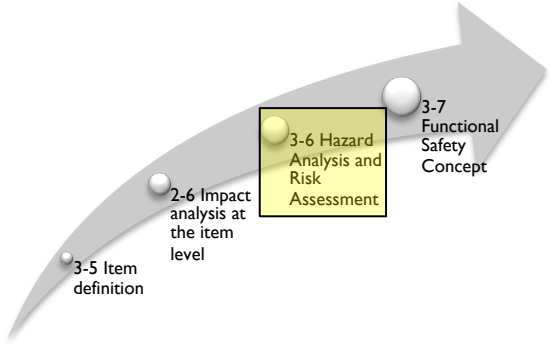
Exposure



ISO26262-3, Table 2: Classes of probability

	Class				
	E0	**E1**	**E2**	**E3**	**E4**
Description	Incredible	Very low probability	Low probability	Medium probability	High probability

Exposure (triggers)



A function fails

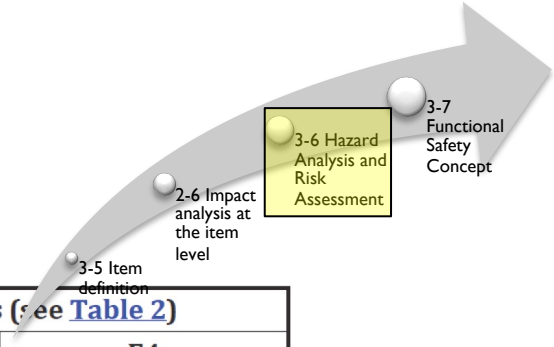
Failure is the trigger

Failure effect is directly recognizable → E parameter classification in the duration i.e, time range (how long)

Failure effect is only recognizable in defined situations → E parameter classification in the frequency range (how often)

Situation is the trigger

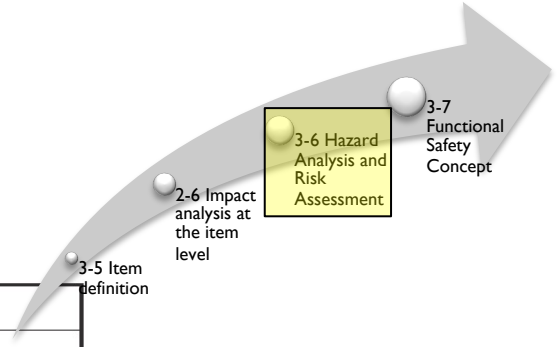
Exposure (Duration)



ISO26262-3, Table B.2: Classes of probability of exposure regarding duration in operational situations

	Class of probability of exposure in operational situations (see Table 2)			
	E1	**E2**	**E3**	**E4**
Description	Very low probability	Low probability	Medium probability	High probability
Duration (% of average operating time)	Not specified	<1 % of average operating time	1 % to 10 % of average operating time	>10 % of average operating time
Examples for road layout	—	— Country road intersection — Highway exit ramp	— One-way street (city street)	— Highway — Country road
Examples for road surface	—	— Snow and ice on road — Slippery leaves on road	— Wet road	—
Examples for vehicle stationary state	— Vehicle during jump start — In repair garage	— Trailer attached — Roof rack attached — Vehicle being refuelled	— Vehicle on a hill (hill hold)	—
Examples for manoeuvre	— Driving downhill with engine off (mountain pass)	— Driving in reverse — Overtaking — Parking (with trailer attached)	— Heavy traffic (stop and go)	— Accelerating — Decelerating — Stopping at traffic light (city street) — Lane change (highway)

Exposure (Frequency)

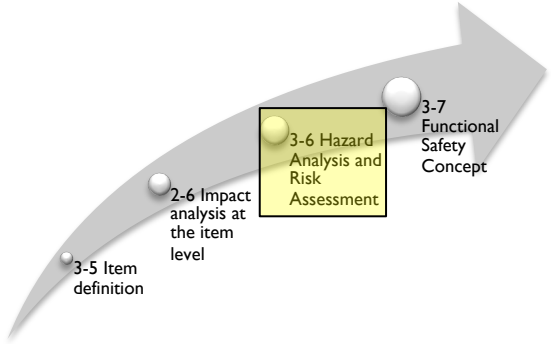


ISO26262-3, Table B.3

	Class of probability of exposure in operational situations (see Table 2)			
	E1	**E2**	**E3**	**E4**
Description	Very low probability	Low probability	Medium probability	High probability
Frequency of situation	Occurs less often than once a year for the great majority of drivers	Occurs a few times a year for the great majority of drivers	Occurs once a month or more often for an average driver	Occurs during almost every drive on average
Examples for road layout	—	— Mountain pass with unsecured steep slope	—	—
Examples for road surface	—	— Snow and ice on road	— Wet road	—
Examples for vehicle stationary state	— Stopped, requiring engine restart (at railway crossing) — Vehicle being towed	— Roof rack attached	— Vehicle being refuelled — Vehicle on a hill (hill hold)	—
Examples for manoeuvre	—	— Evasive manoeuvre, deviating from desired path	— Overtaking	— Shifting transmission gears — Executing a turn (steering) — Using indicators — Driving in reverse

Controllability

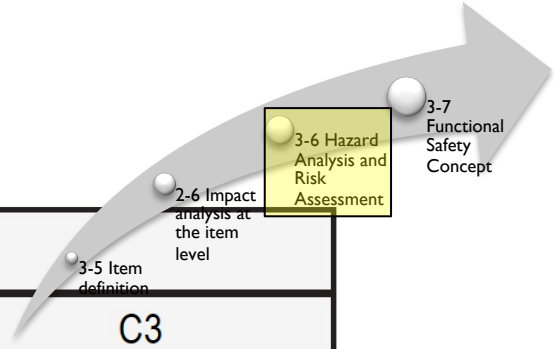
ISO26262-3, Table B.6



	Class of controllability (see Table 3)			
	C0	C1	C2	C3
Driving factors and scenarios	Controllable in general	More than 99 % of the average drivers or other traffic participants are able to avoid harm	Between 90 % an 99 % of the average drivers or other traffic participants are able to avoid harm	Less than 90 % of the average drivers or other traffic participants are able to avoid harm
Example situations that are considered distracting e.g. unexpected radio volume increase or warning message - fuel low	Maintain intended driving path	—	—	—
Example for unavailability of a driver assisting system that does not affect the safe operation of the vehicle	Maintain intended driving path	—	—	—
Example for unintended closing of window while driving	—	Remove arm from window	—	—
Example for blocked steering column when accelerating from standstill	—	Brake to slow/stop vehicle	—	—
Example for function with high automation where driver is not in the loop	—	—	—	No attempt to maintain intended driving path

	Class of controllability (see Table 3)			
	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable
Example for faulty driver airbag release when travelling at high speed	—	—	—	Maintain intended driving path, stay in lane, or brake to slow/stop vehicle
Example for excessive trailer swing during braking potential for jacknifing	—	—	—	Driver counter-steers and brakes in an attempt to maintain intended driving path
Example for failure of ABS during emergency braking	—	—	Maintain intended driving path	
Example for propulsion failure at high lateral acceleration	—	—	Maintain intended driving path	—
Example for inadvertent opening bus door while driving with passenger standing in doorway	—	—	Passenger grabs hand rail to avoid falling out of bus	—
Example for failure of brakes	—	—	—	Steer away from objects in driving path

ASIL determination



Severity S	Exposure E	Controllability C		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A[a]
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

Thanks for your attention