FUNCTIONAL SAFETY
COURSE #1

Dr. FRANCK GALTIE

DIRECTEUR AUTOMOTIVE FUNCTIONAL SAFETY

NXP

SECURE CONNECTIONS
FOR A SMARTER WORLD

General Agenda

- Course #1 :

Functional Safety awareness

- Course #2 :

Brainstorming on power inverter architecture, potential failures and safety mechanisms (ie. safety concept)

- Course #3:

Continue on Safety Concept

- Course #4:

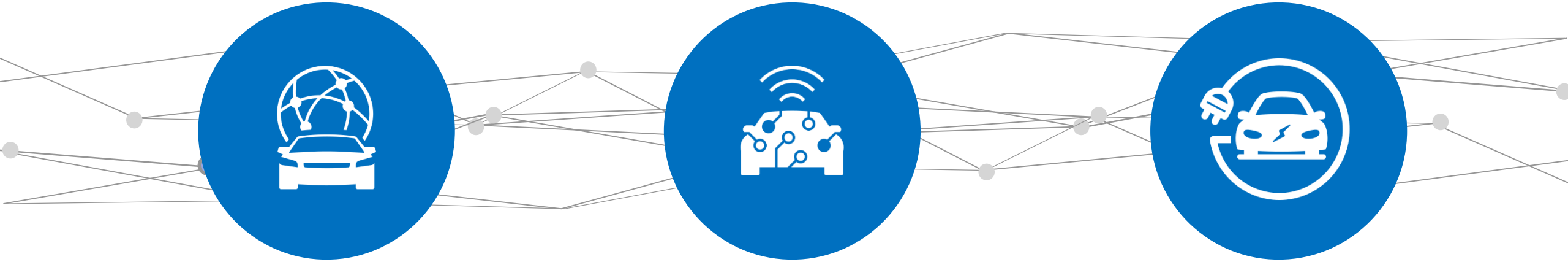
How to prove our concept and assess it

Course #1 agenda

- Introduction
- What is functional safety?
- How to manage functional safety
- Functional safety & Autonomous driving
- Conclusion

01.
Introduction

From Automotive to Safe and Secure Mobility



Connectivity

Enjoying Life. One hour per day in the car

Autonomy

Saving Lives. 1.3 M road fatalities every year

Electrification

Reducing CO^2. EU mandates 20% reduction by 2020

SAFE AND SECURE MOBILITY

Semi Value / Car more than doubles through next 10 Years

Road Traffic Accidents: The Causes

Critical Reasons	Number	%
Driver	2,046,000	94%
Vehicles	44,000	2%
Environment	52,000	2%
Unknown	47,000	2%
Total	2,189,000	100%

Data source: NMVCCS

Driver-Related Critical Reasons	Number	%
Recognition Error	845,000	41%
Decision Error	684,000	33%
Performance Error	210,000	11%
Non-performance Error (e.g. Sleep)	145,000	7%
Other	162,000	8%
Total	2,046,000	100%

Every year!

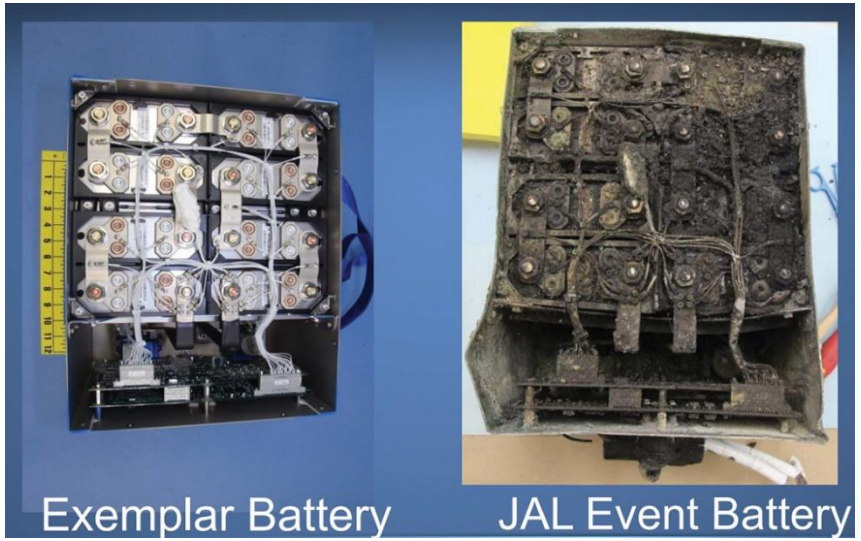
- ~1.3 M fatalities
- >50 M people seriously injured
- >$3 trillion cost of road accidents
- >90% caused by human mistakes

We need to get the *Human Factor* out of the equation!

Safety Incidents

Toyota Unintended Acceleration

The Ford Pinto Case



JAL B – 787

(Source: Tesla Motors Club)

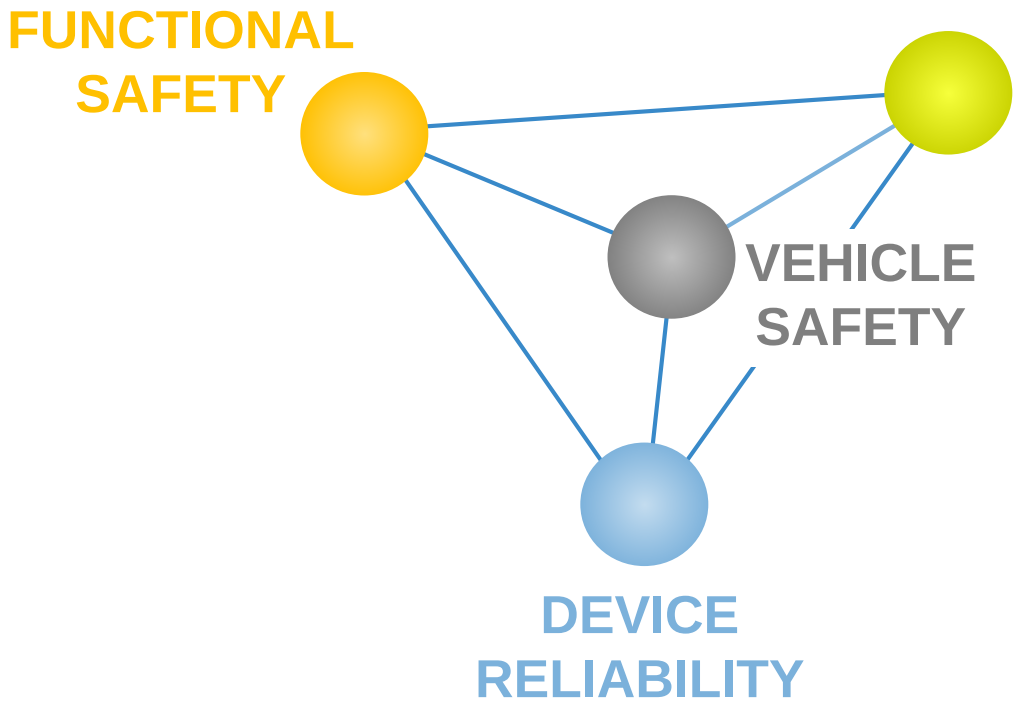
Tesla Crash

Tesla's Fatal Crash

Elements Of A Safe System

Zero accidents by system failures (ISO 26262)

Zero accidents by system hacks



Zero accidents by human error (ADAS & SOTIF)

Zero components failures (robust product)

SOTIF: Safety of the intended functionality

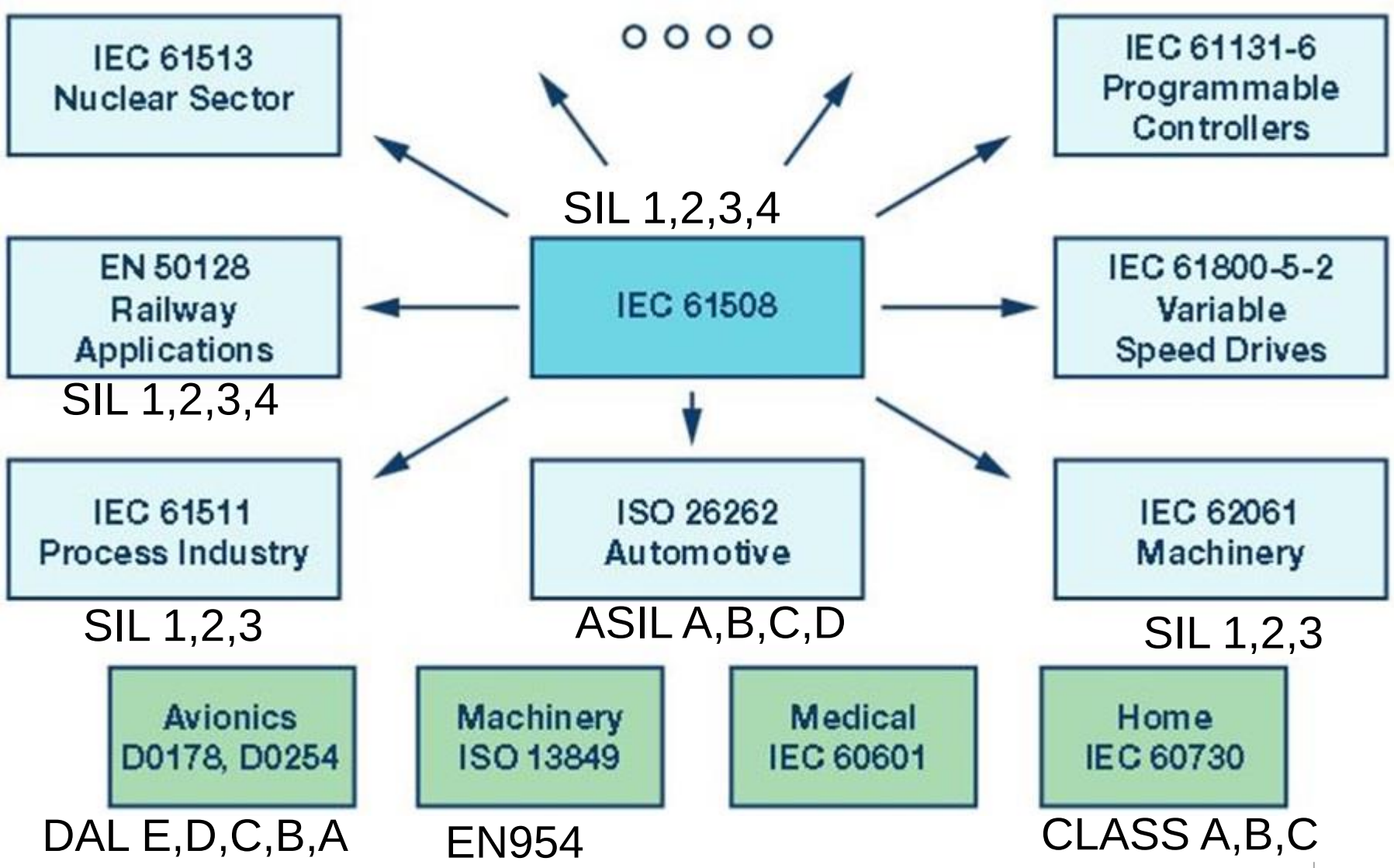
02.

What is Functional Safety ?

What is Functional Safety?

- Functional safety is the absence of unreasonable risk to do hazards caused by malfunctioning behavior
- Mitigation or control of risk

Functional Safety Standard Landscape



INTERNATIONAL STANDARD

ISO 26262-1

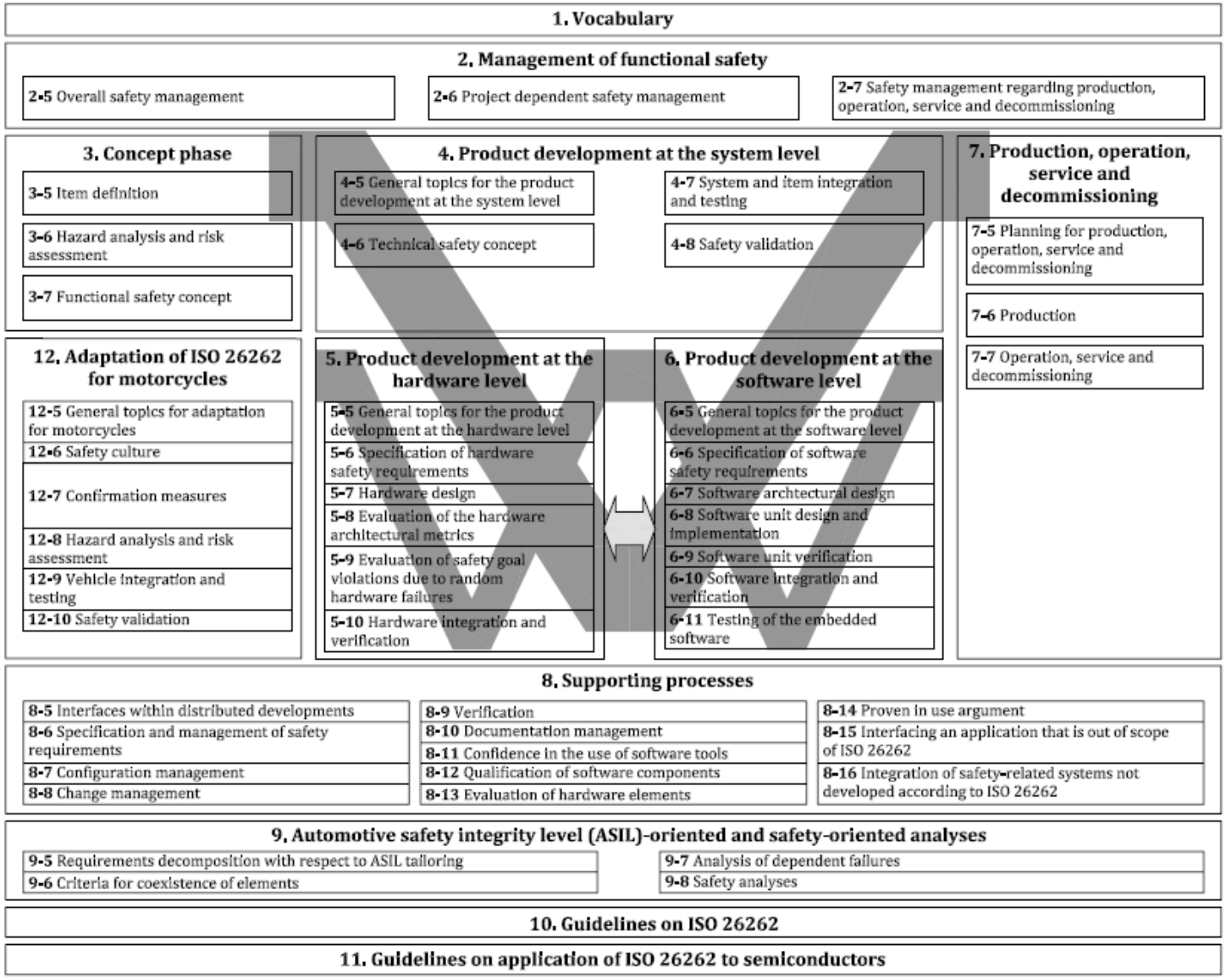
Second edition
2018-12

Road vehicles — Functional safety —

Part 1: Vocabulary

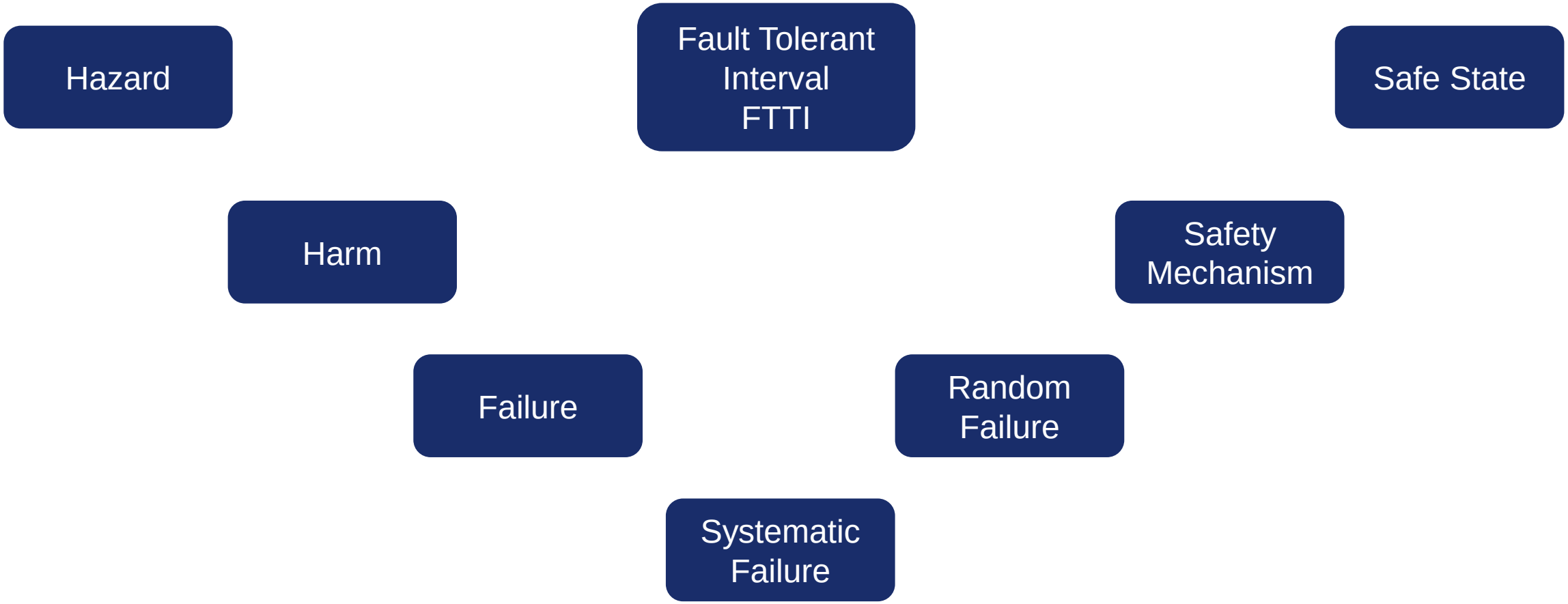
Véhicules routiers — Sécurité fonctionnelle —

Partie 1: Vocabulaire



Reference number
ISO 26262-1:2018(E)

Functional Safety: A Bit Of Wording



03.

How to Manage Functional Safety

Functional Safety - General Approach

Hazard and Risk Analysis

Safety Goals

Mitigation

Safety Measures
Safety Mechanims

SAFE System

Quantify A Risk: Automotive Safety Integrity Level (ASIL) Definition

Severity

Exposure

Controllability

What is the level of injury ?

How often is it likely to happen?

Can the hazard be controlled

An ASIL is defined for each Safety Goal

Functional Safety - Integrity Level Evaluation

E = Exposure

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

C = Controllability

Class	Description
C0	Controllable in general
C1	Simply controllable
C2	Normally controllable
C3	Difficult to control or uncontrollable

S = Severity

Class	Description
S0	No injuries
S1	Light and moderate injuries
S2	Severe and life-threatening injuries (survival probable)
S3	Life-threatening injuries (survival uncertain), fatal injuries

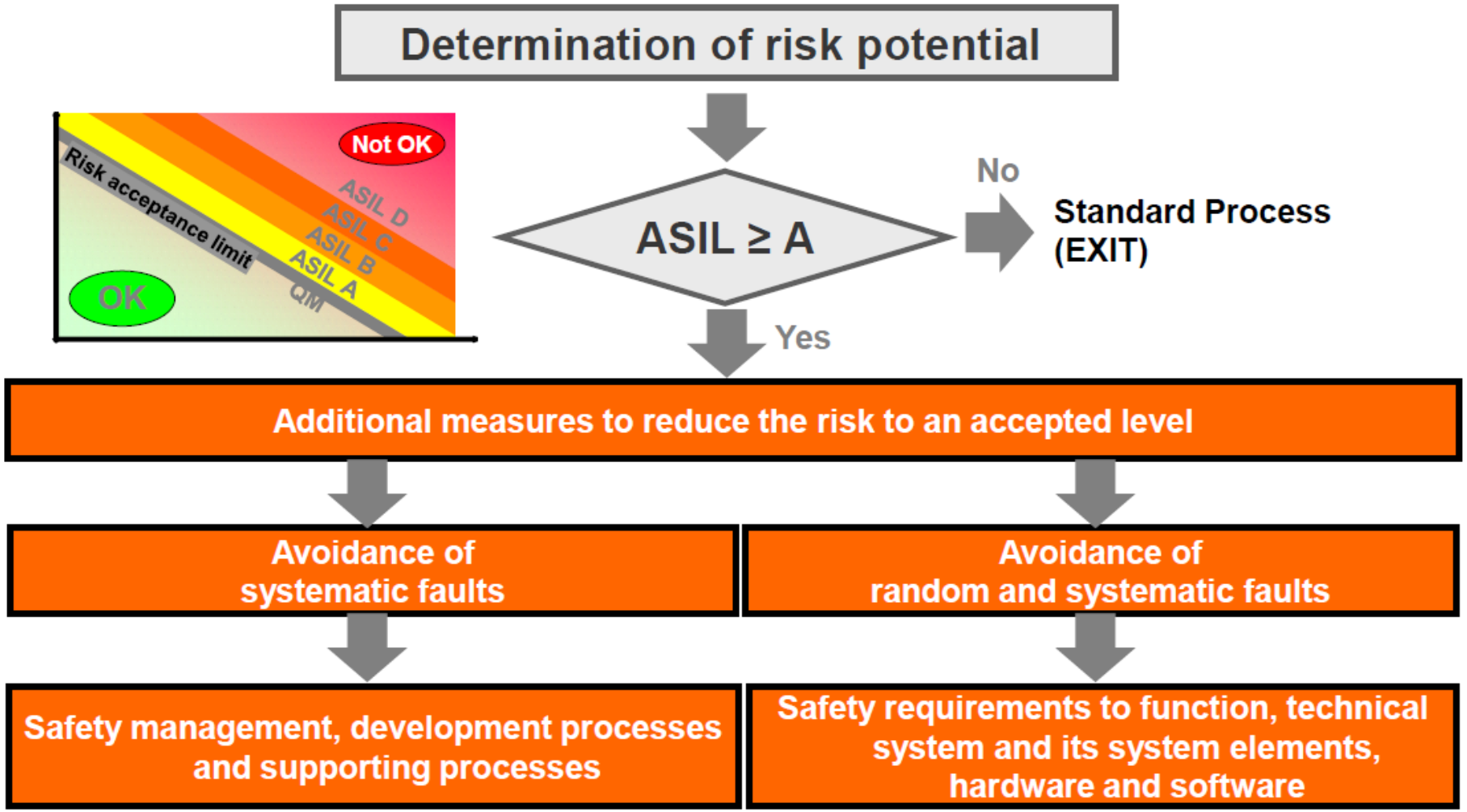
		C1 – SIMPLE	**C2** – NORMAL	**C3** – DIFFICULT
S1 LIGHT	E1 (very low)	QM	QM	QM
	E2 (low)	QM	QM	QM
	E3 (medium)	QM	QM	A
	E4 (high)	QM	A	B
S2 SEVERE	E1 (very low)	QM	QM	QM
	E2 (low)	QM	QM	A
	E3 (medium)	QM	A	B
	E4 (high)	A	B	C
S3 FATAL	E1 (very low)	QM	QM	A
	E2 (low)	QM	A	B
	E3 (medium)	A	B	C
	E4 (high)	B	C	D

(QM: "quality managed" → no requirements from standard applied explicitly)

Example of System and Corresponding Safety integrity Level

Application / System	ASIL
Wiper	A
Computer Vision – mono / stereo camera	B
Radar	B
Lighting – low beam	B
Battery Management system	D
Chassis dynamic – suspension / damping	C
Gateway – ADAS controller - Fusion	D
Transmission – Dual Clutch Automatic Gearbox	D
Braking – Electro-mechanic	D
Airbag – (unwanted deployment)	D
Electric Power steering	D

Functional Safety - Risk Management



Functional Safety – Risk Management

ANALYZE HAZARD & RISK (HARA)
DEFINE SAFETY GOALS (SG)
EVALUATE AUTOMOTIVE SAFETY INTEGRITY LEVEL (ASIL A, B, C or D)

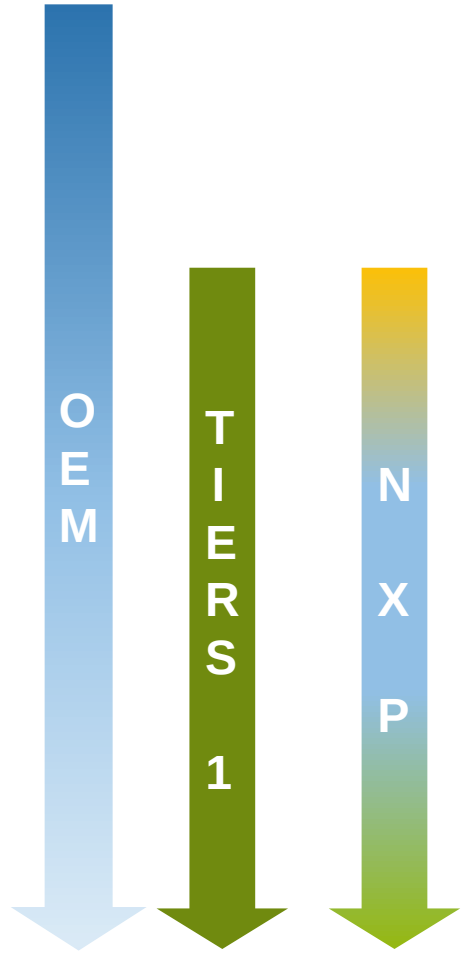
INDENTIFY FAULTS
IMPLEMENT M**EASURES** TO MITIGATE THE RISK

AVOID **SYSTEMATIC FAULTS**
(in development)

- Process
- Traceability
- Best practices
- Lessons learned
- Verification & validation

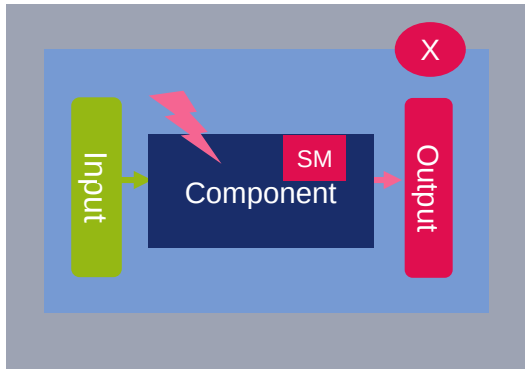
DETECT **HW RANDOM FAULTS**
(in operation)

- Safety concept / architecture
- Embedded **Safety mechanisms**
- Quantitative & qualitative analysis
- Fault injection
- Documentation

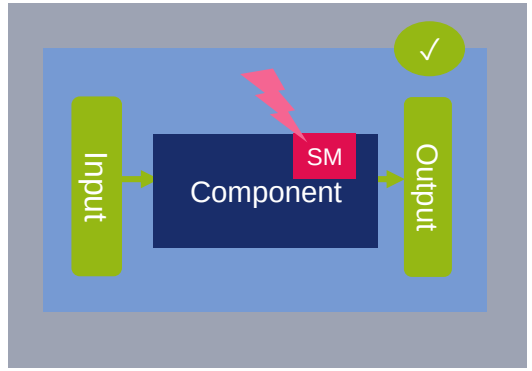


Functional Safety - Types of Faults

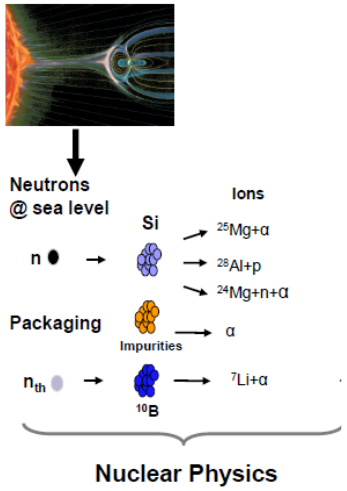
Single Point Fault



Latent Fault



Transient Fault

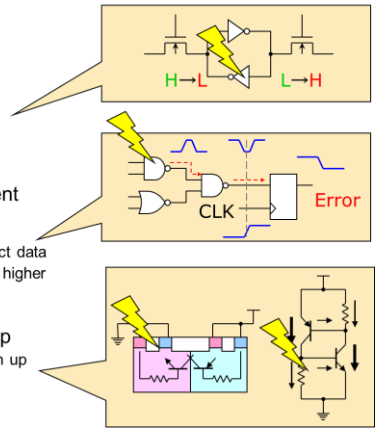


Soft Error Issue

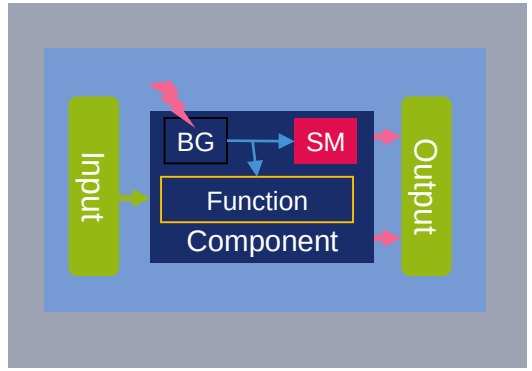
1. SEU = Single Event Upset
   - Data upset
   - DRAM
   - SRAM

2. SET = Single Event Transient
   - Temporary logic data upset
     ↓
     Error If Flip flop latch incorrect data
   - Error rate become higher as higher frequency clock

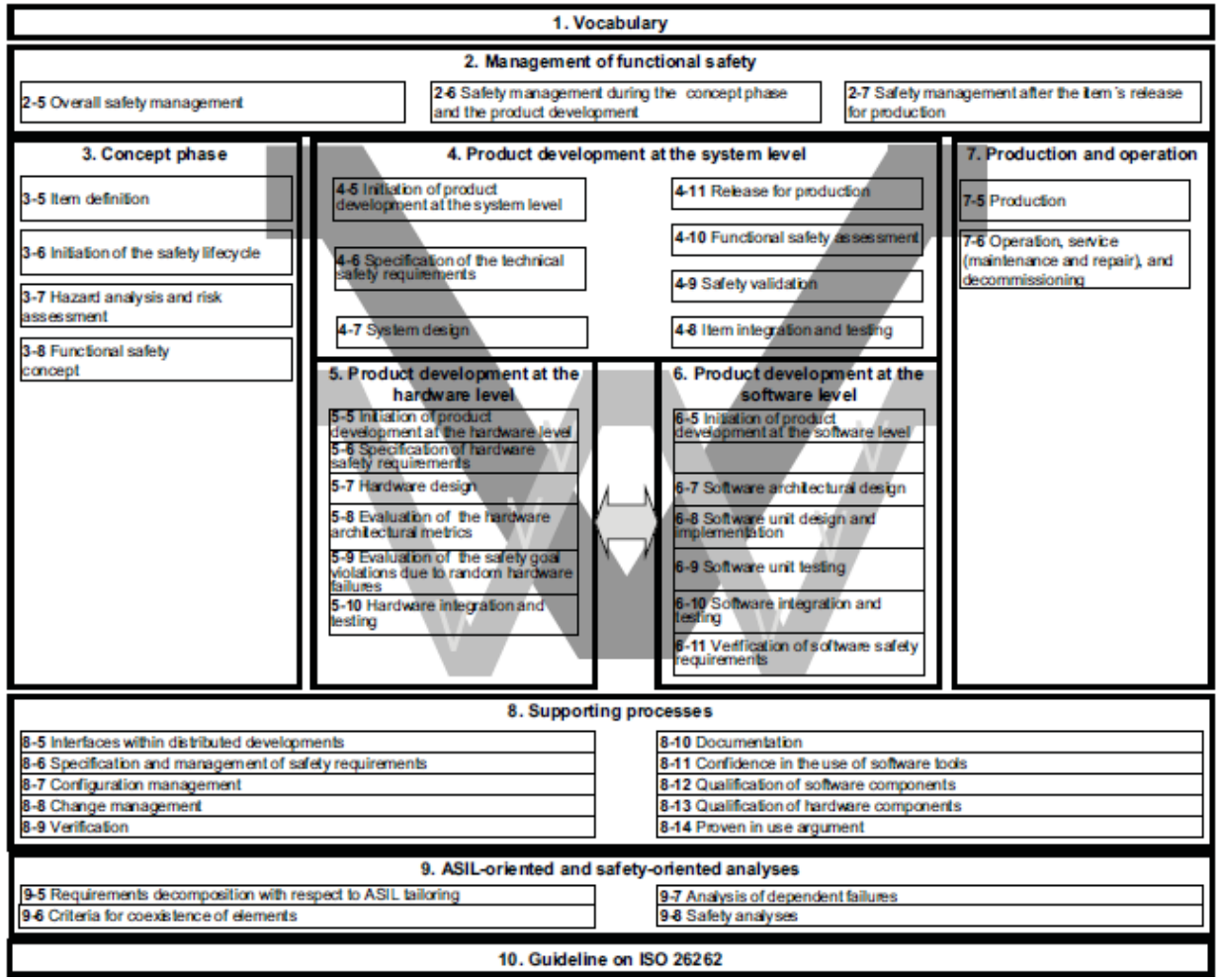
3. SEL = Single Event Latch up
   - Induced by PN isolation latch up



Common Cause Fault



Functional Safety - Vmodel & Responsibility



Reference ISO 26262-10:2012

ISO 26262

OEM

- Item definition
- Hazard analysis and risk assessment
- Safety Goals
- Functional Safety Concept

Safety Manual
Safety Analysis

Safety Requirements
DIA

Tier 1

- Technical Safety Concept
- Technical Safety Architecture
- ASIL Classification of Functions
- HW / SW design

Safety Manual
Safety Analysis

Safety Requirements
DIA

Tier 2 Supplier - NXP

- HW / SW "products"

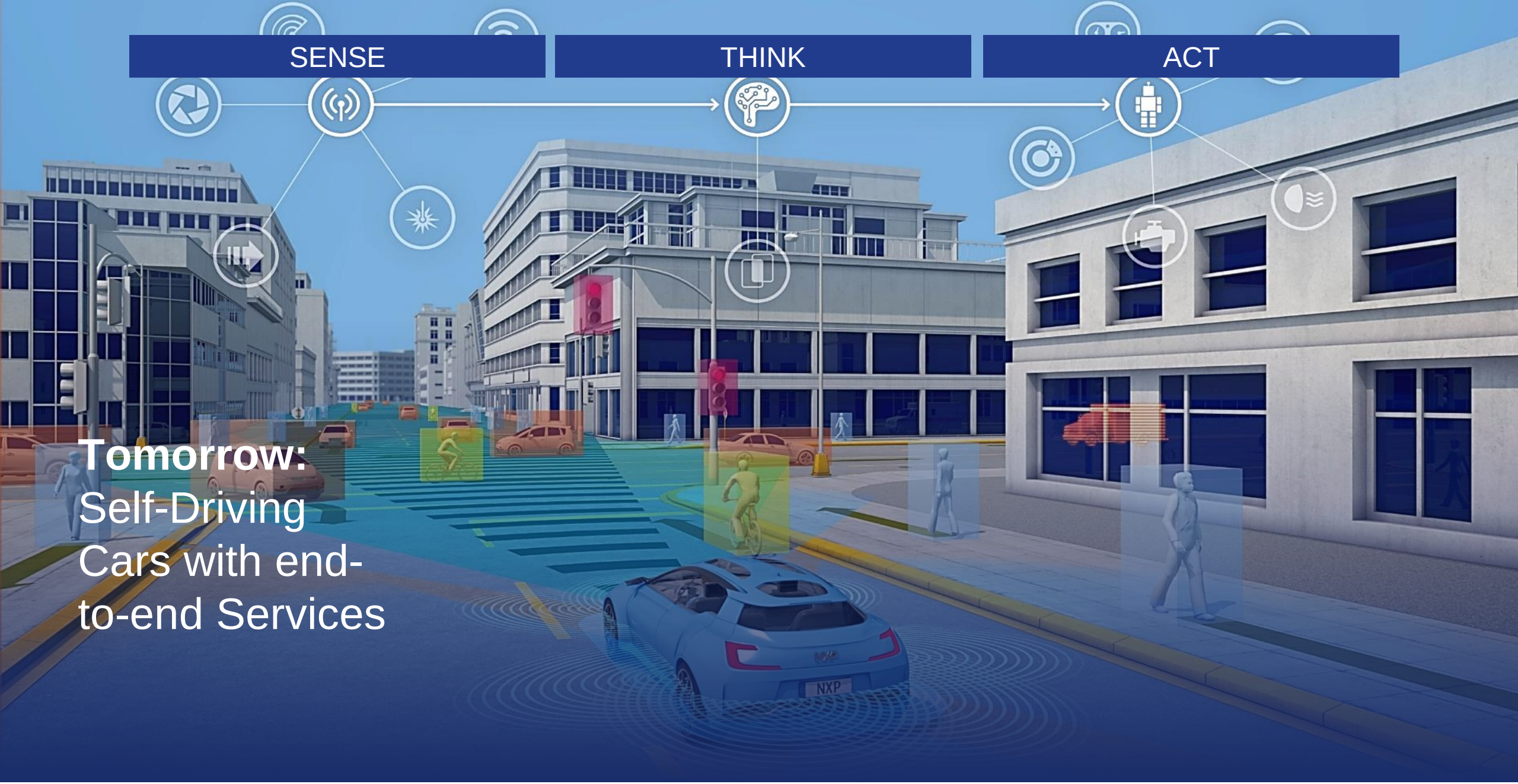
Product Safety Mechanisms
(implemented in offering, described in Safety Manual, quantified/qualified by Safety Analysis)

Development Process & Methods

QUALITY

04.

Functional Safety & Autonomous driving


SENSE
THINK
ACT
Tomorrow:
Self-Driving
Cars with end-
to-end Services

Autonomous Driving Levels

5 Full Automation

4 High Automation

3 Conditional Automation

2 Partial Automation

1 Driver Assistance

0 No Automation

Level 3-5
Automated Driving System
Performs entire dynamic driving task/monitors environment

Level 0-2
Human Driver
Performs part of dynamic driving task/monitors environment

SAE standard J3016

Different Innovation Strategies
EVOLUTION AND REVOLUTION

Revolutional

Evolutional

Safe, Secure Mobility

ACCELERATE AND WIN
IN BOTH WORLDS

Functional Safety: Autonomous Driving – SAE Levels

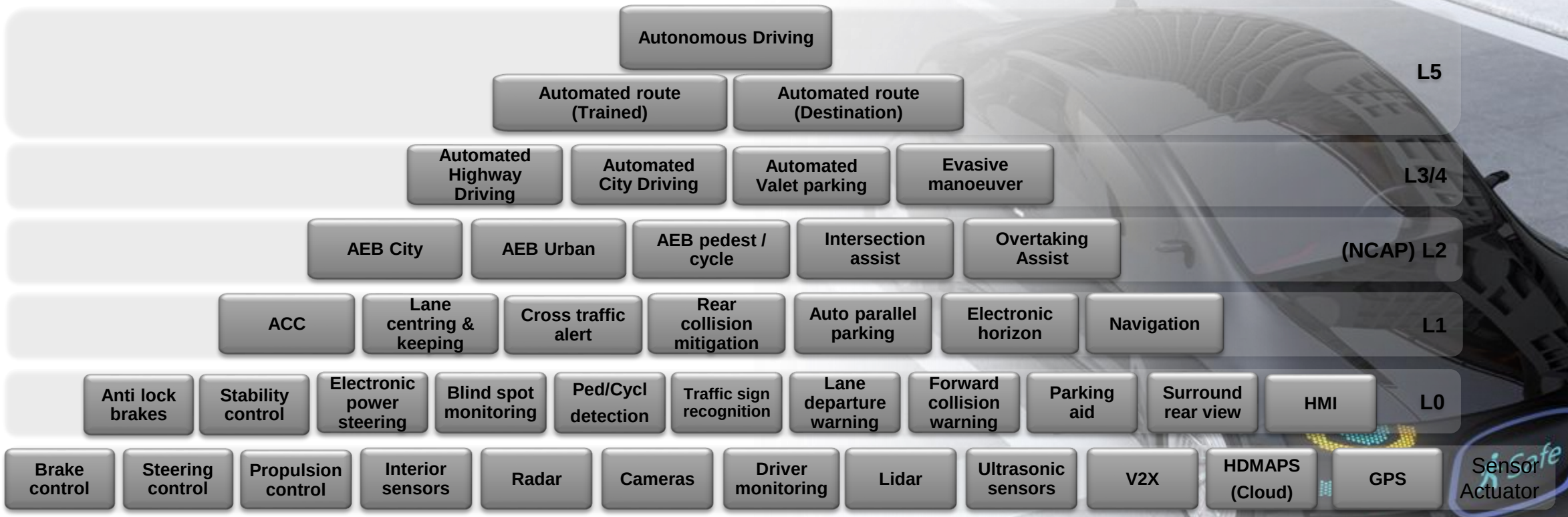
CONTROL OF THE SYSTEM

HUMAN → MACHINE

AVAILABILITY OF THE SYSTEM

FAIL-SAFE → DEGRADED → FAIL-OPERATIONAL

From ADAS to Highly Automated driving to Autonomous Driving



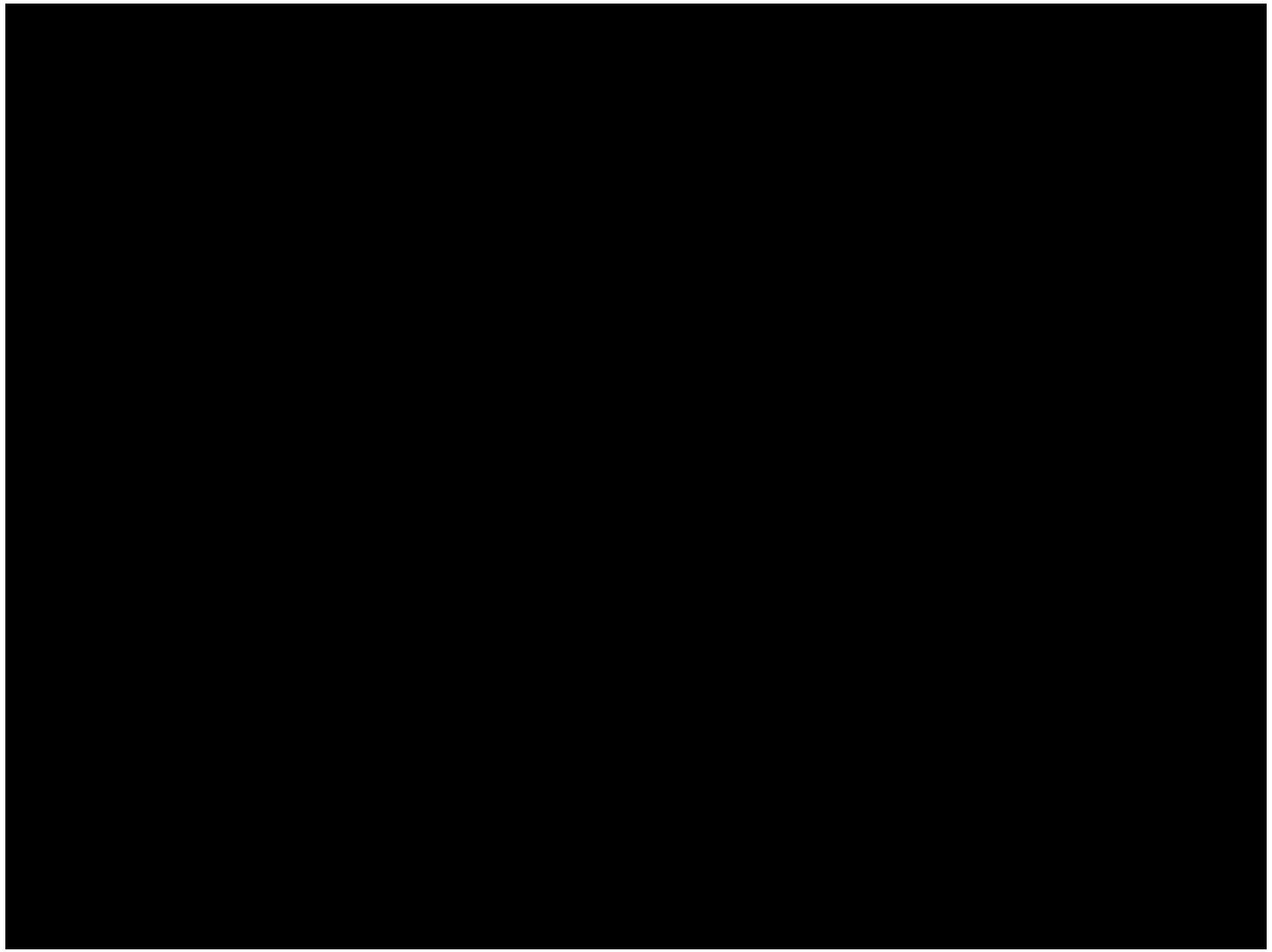
INTERNAL/PROPRIETARY

A couple of Case Studies

Uber Accident- March 18, 2018

Tesla Fatal Crash- May 7, 2018

Uber Accident- March 18, 2018



https://www.youtube.com/watch?v=ywydaIBYhic

Tesla Fatal Crash- May 7, 2016

https://www.youtube.com/watch?v=uIV6sGHZo1U

Tesla Fatal Crash- May 7, 2016

Road:

- Divided highway

Trailer:

- White side of tractor trailer
- High ride height of the trailer

Sky:

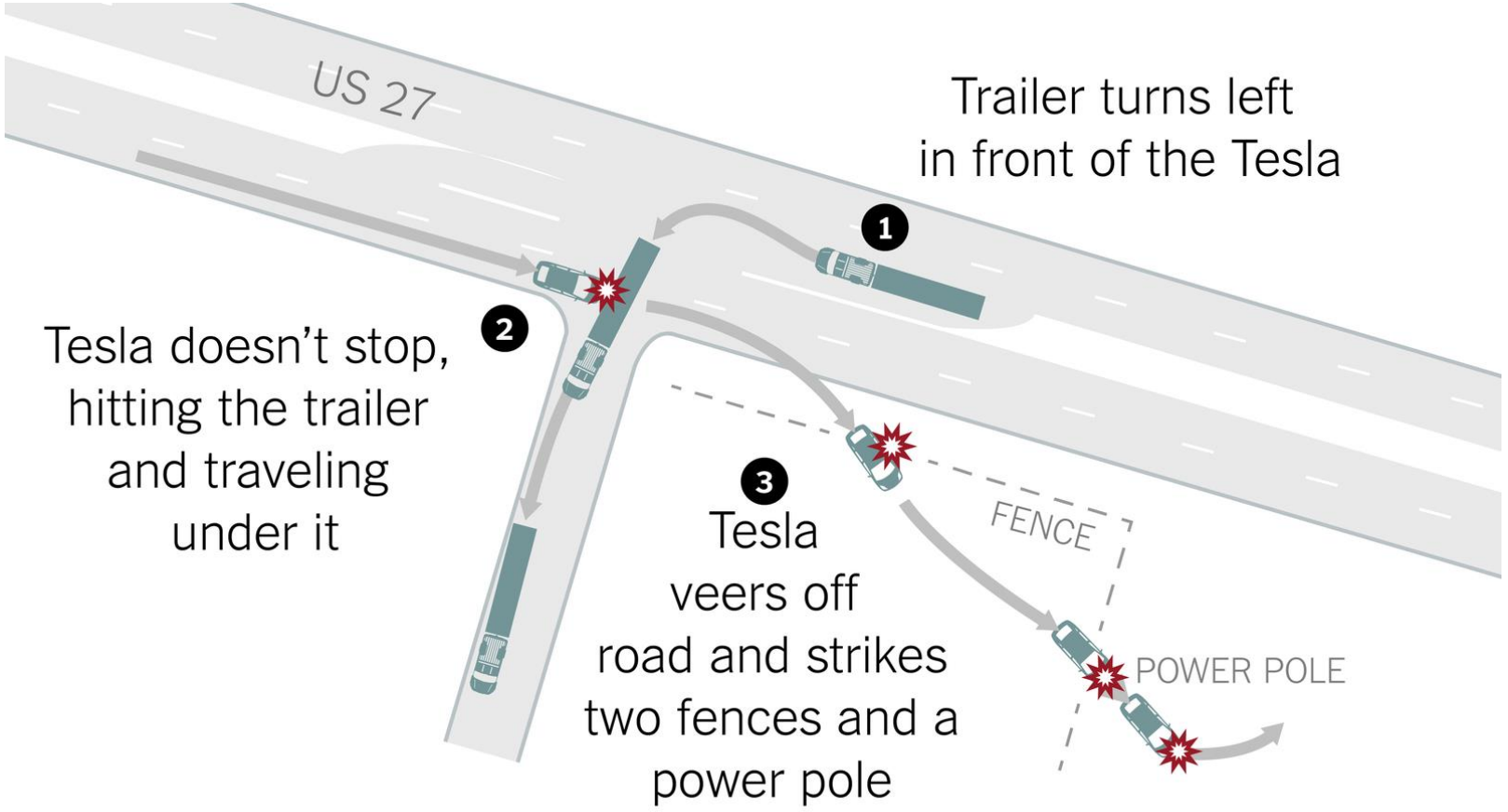
- Brightly lit sky

Vehicle:

- Autopilot Engaged
- Automatic Emergency Braking (AEB) was not activated
- Obstacle was not detected ~ Sensor Limitations

Driver:

- Driver could not see and react quickly enough ~ Human Factors
- Braking was not performed
- Watching a movie
- Incredible trust on the autonomous system



https://electrek.co/2016/07/01/understanding-fatal-tesla-accident-autopilot-nhtsa-probe/
https://www.nytimes.com/2016/07/13/business/tesla-autopilot-fatal-crash-investigation.html?_r=0

05.
Conclusion

Conclusion

- Functional safety is about **RISK** assessment, prevention, protection
- **SAFETY GOALS** and **ASIL** are defined by OEM and are related to a function
- Functional Safety for Automotive is covered by ISO 26262 (International Standard)
- Autonomous driving is the next big challenge for Safety
- Functional Safety applies to Industrial, Medical, Railway, Aeronautics, Nuclear, etc…

SECURE CONNECTIONS
FOR A SMARTER WORLD