Failure Diagnosis and Prognosis for Automotive Systems

Tom Fuhrman

General Motors R&D

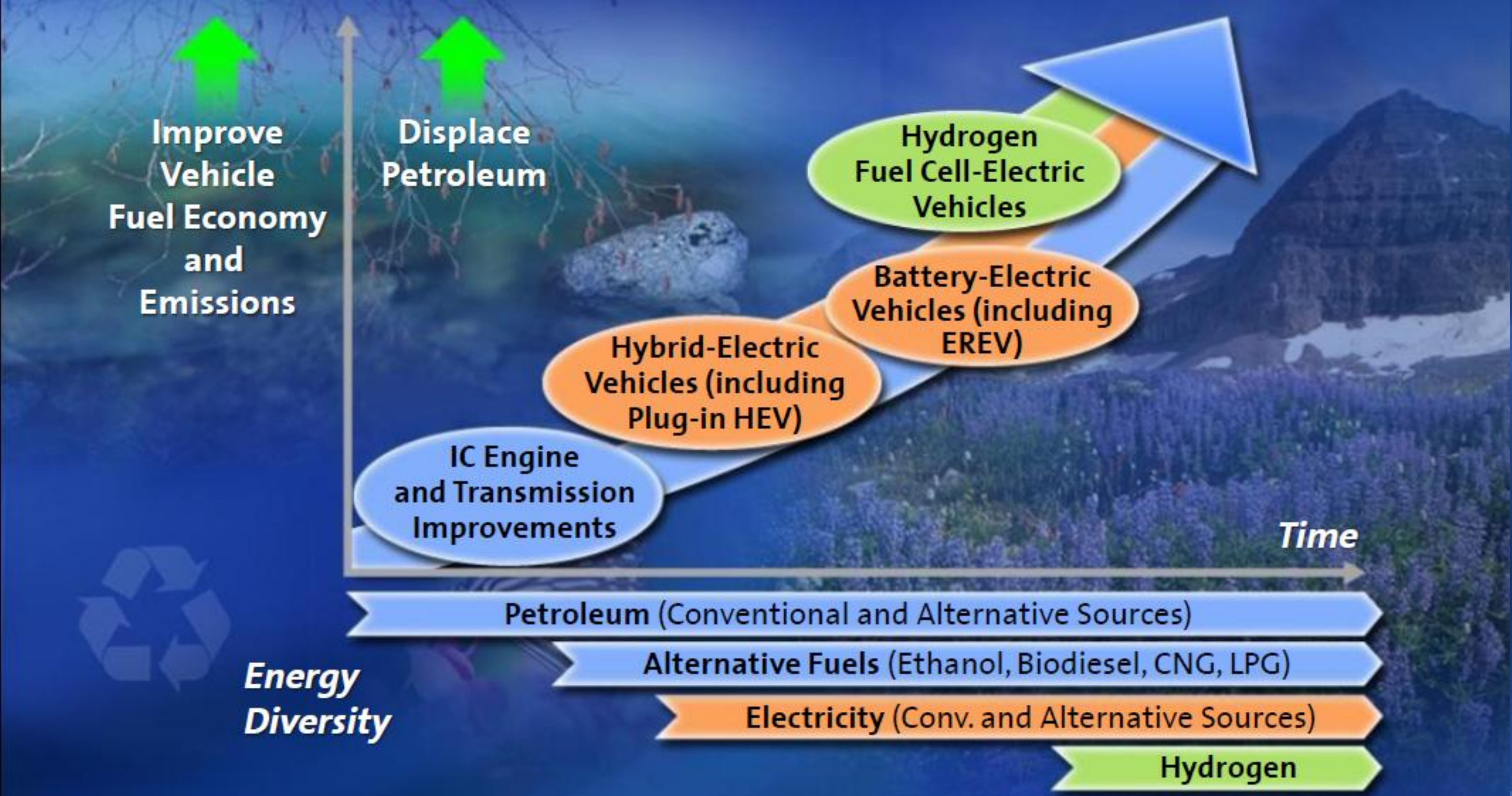
IFIP Workshop

June 25-27, 2010

Automotive Challenges and Goals

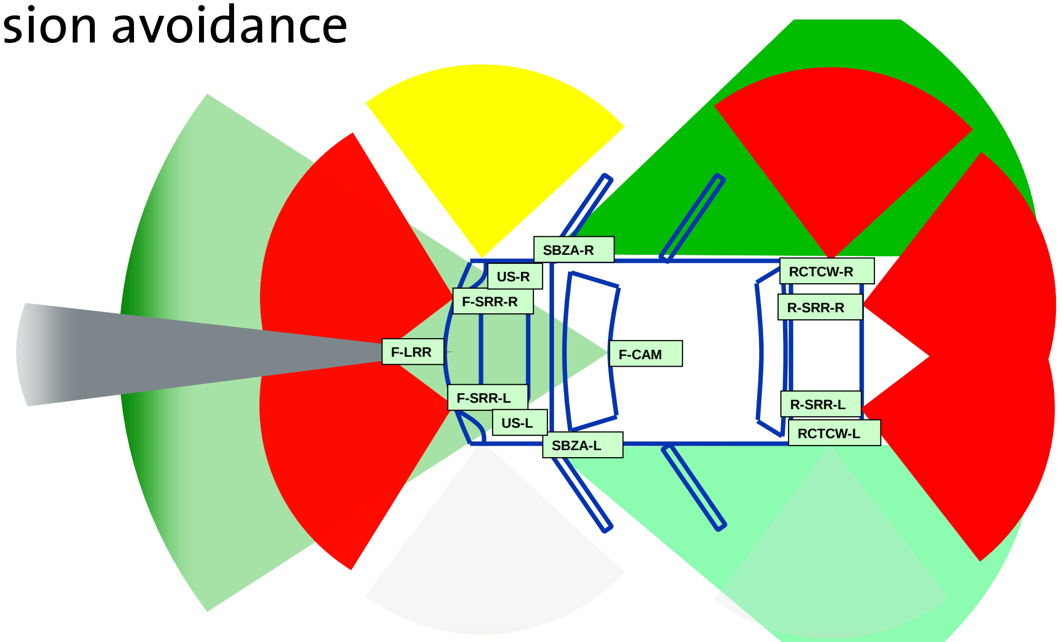
Driver	Challenges	Goals
Energy	• Rising cost of petroleum fuels • Non-renewability of fossil fuels • Increasing gov't regulations for fuel economy	• Reduce fuel consumption • Zero dependency on fossil fuels
Environment	• Impact of greenhouse gas emissions on the environment • Increasing gov't regulations for emissions	• Zero greenhouse gas emissions
Safety	• 40K traffic fatalities annually in the US	• Zero traffic fatalities
Connectivity	• Demand for connectivity to personal electronics devices • Worsening traffic congestion	• Zero traffic congestion • Safer roadways

FUEL ECONOMY AND EMISSIONS



Example Active Safety Systems

- Adaptive cruise control
- Forward collision warning
- Curve speed control
- Side blind zone alert
- Lane keeping / lane centering control
- Cross traffic collision avoidance



ROADMAP TO AUTONOMOUS DRIVING

Functionality

Driver Assist/ Warning

- Lane Departure Warning
- Side Blind-Zone Alert

Semi-Autonomous Driving

Distributed control between vehicle and driver

- Lane Centering

On-Demand Autonomous Driving

Vehicle performs autonomously "on-demand" for limited travel

- Highway-Only Autonomous Driving

Autonomous Driving

Vehicle drives itself for an entire travel journey

- Vehicle as Chauffeur

Today → **Future**

Where does failure diagnosis fit in?

Two main use cases:

- Off-line servicing / maintenance of the vehicle
- On-line safety architecture

Failure Diagnosis in Maintenance

- Well-established, mature area (since 1970's)
- Current practice
  - Diagnostic Trouble Codes (DTC) and Parameter IDs (PID) are generated by and stored within Electronic Control Units (ECUs)
    - Some are required and standardized by government regulations, for emissions equipment, these are called OBD (On Board Diagnostics)
  - Service tools plug into the Diagnostic Link Connector (DLC) and read out these codes (can also upload new calibrations and software code)
  - Diagnostic procedures (flow charts) indicate additional tests and probes to troubleshoot a particular customer concern
- Far from perfect, needs to be continuously improved

Failure Diagnosis in Maintenance

- Customer satisfaction goals
  - Never stranded ("walk-home")
  - Fix it right the first time (no repeat visits!)
- Warranty cost reduction
  - Reduce "No Trouble Founds" (NTF)
  - Focus on highest cost IPTV (Incidents Per Thousand Vehicles) and CPV (Cost Per Vehicle)
    - Batteries
    - Wiring harnesses and connectors
    - Certain Electronic Control Units

Failure Prognosis in Maintenance

- Predict the remaining useful life of components that wear out (in progress)
  - Batteries
  - Brake pads
- Predict the failure of electronic components (future)

Failure diagnosis in the run-time safety architecture

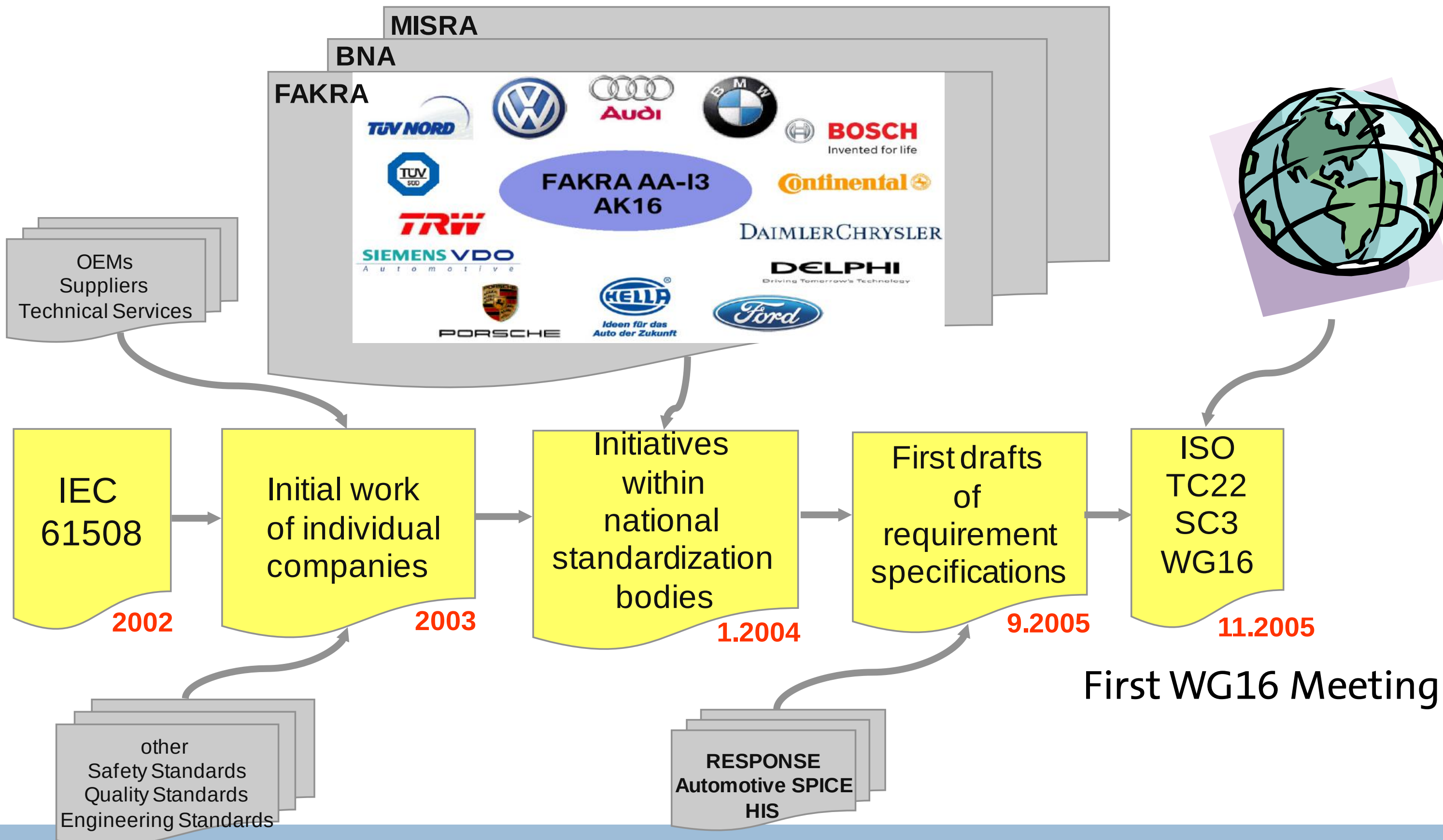
- Process considerations
  - Based on ISO 26262
- Architecture considerations
  - Fault detection and fault mitigation

Failure diagnosis in the run-time safety architecture

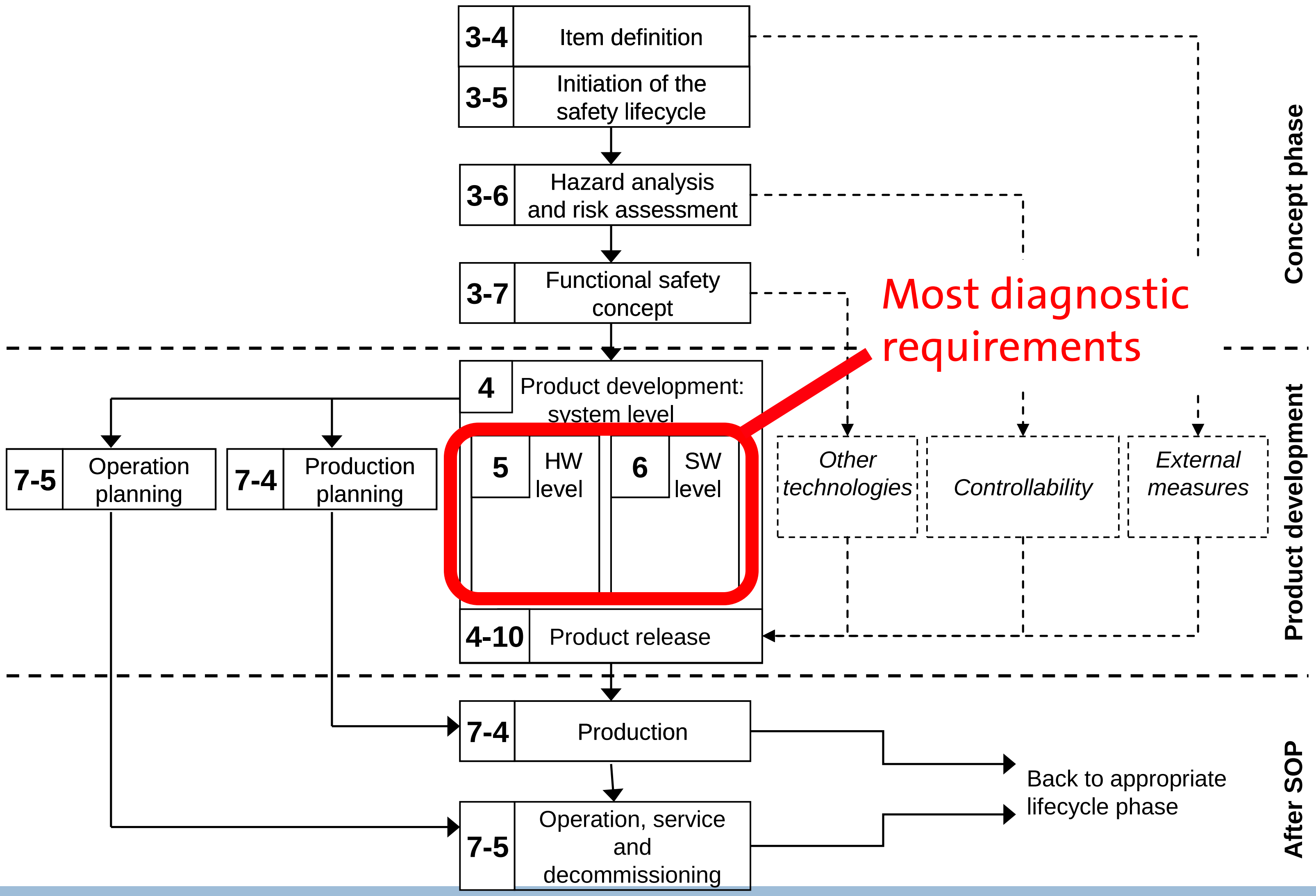
- Process considerations
  - Based on ISO 26262
- Architecture considerations
  - Fault detection and fault mitigation

ISO 26262 and the Functional Safety Process

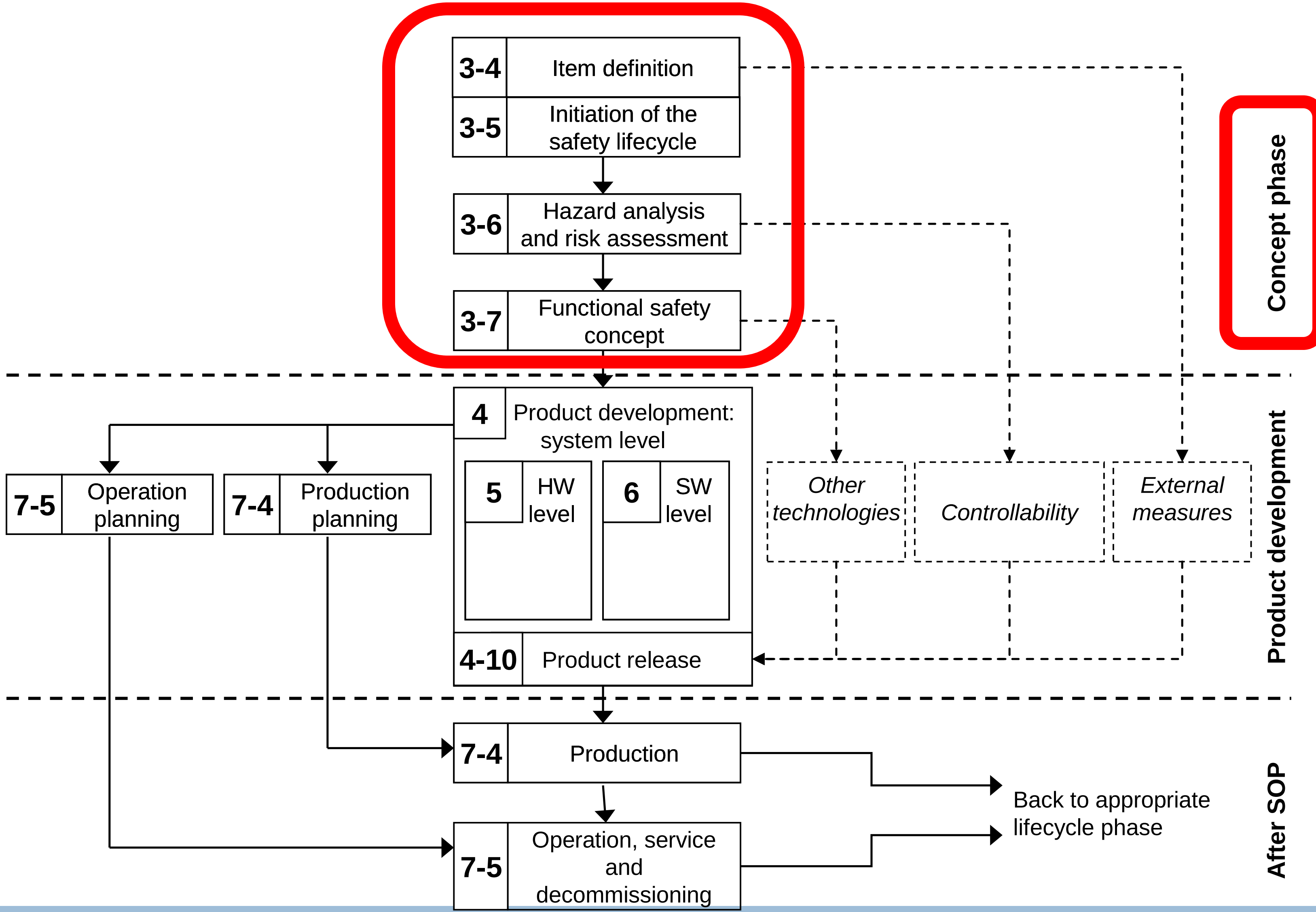
- ISO 26262 is the automotive specialization of IEC 61508



ISO 26262 Process Overview



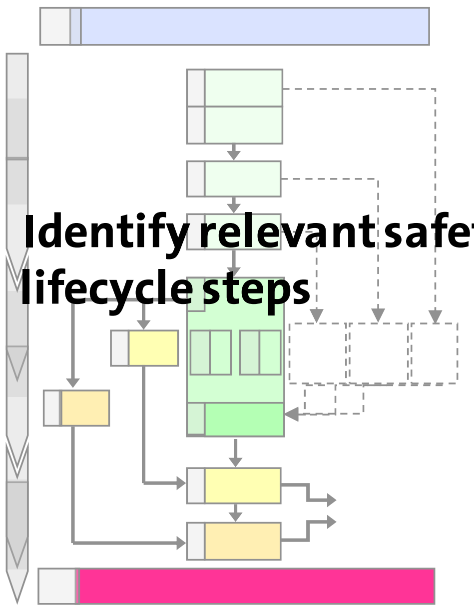
ISO 26262 Process Overview



GM

ISO 26262 Concept Phase

For a given Product "Item":

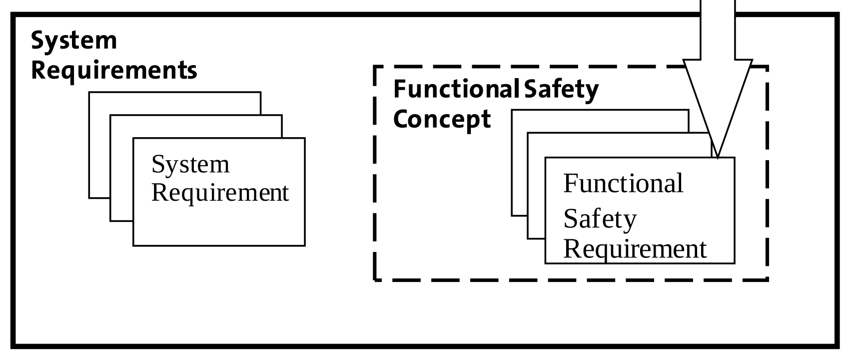


1) Identify relevant safety lifecycle steps

2) Perform a Hazard Analysis Determine ASIL

3) Identify Safety Goals

4) Identify Functional Safety Concept



ISO 26262 Hazard Analysis and Determination of ASIL (Automotive Safety Integrity Level)

Severity

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

Exposure

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

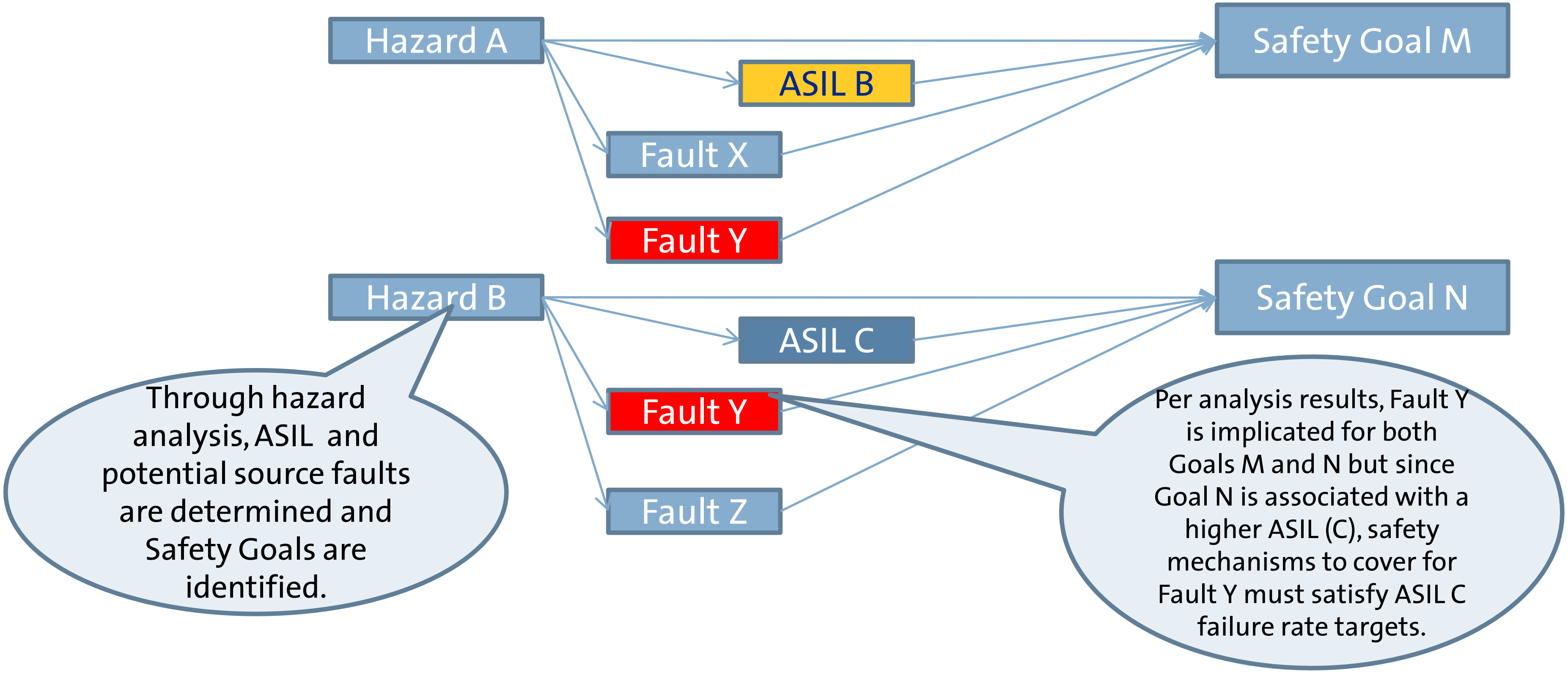
Controllability

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

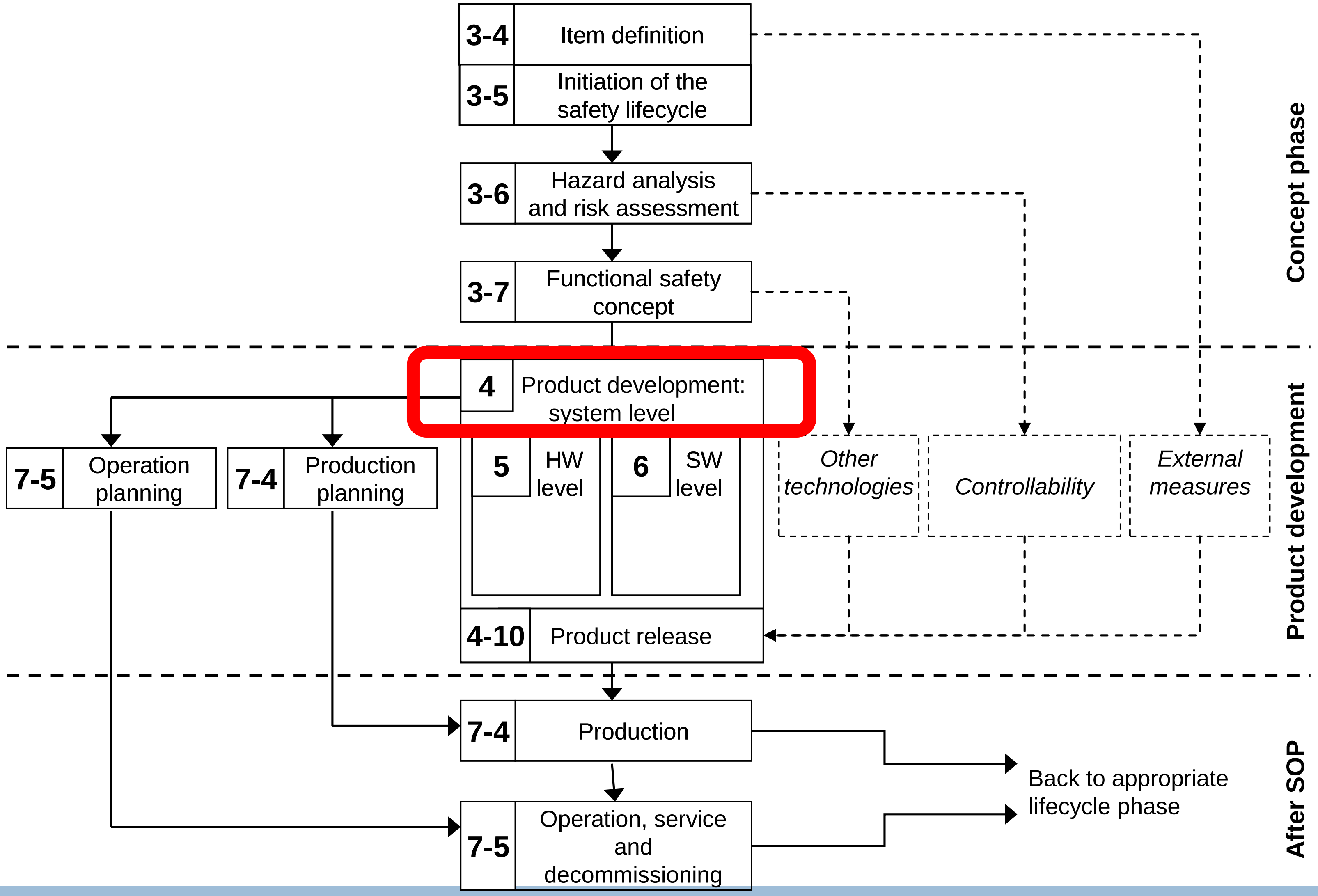
ISO 26262 Hazard Analysis and Determination of ASIL (Automotive Safety Integrity Level)

		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
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

ISO 26262 Identification of Safety Goals



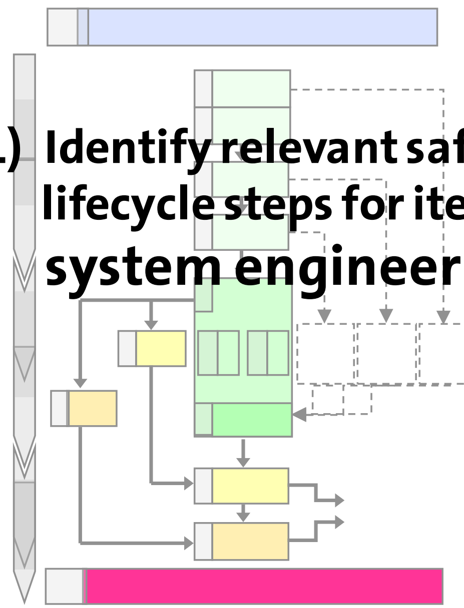
ISO 26262 Process Overview



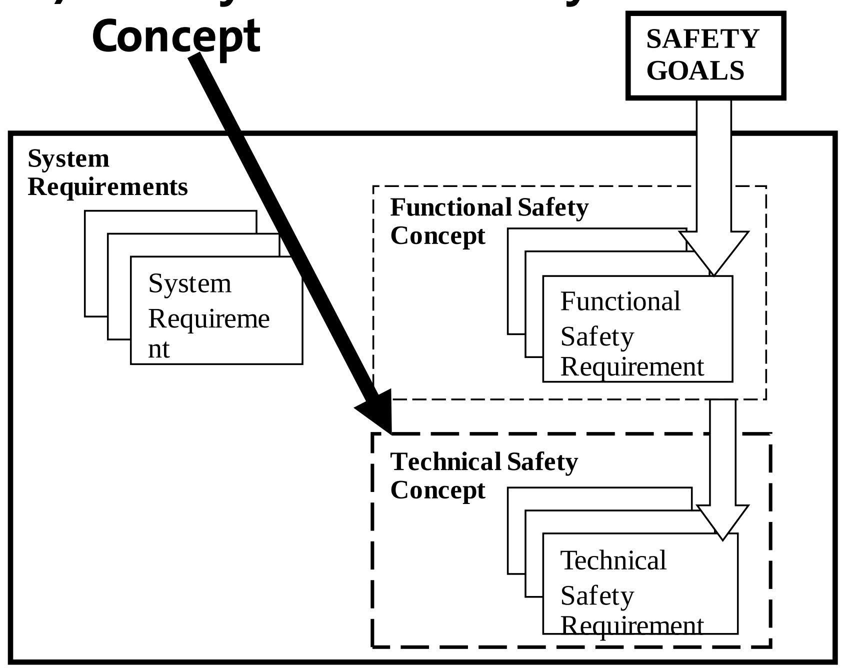
ISO 26262 System Level

For a given Product "Item":

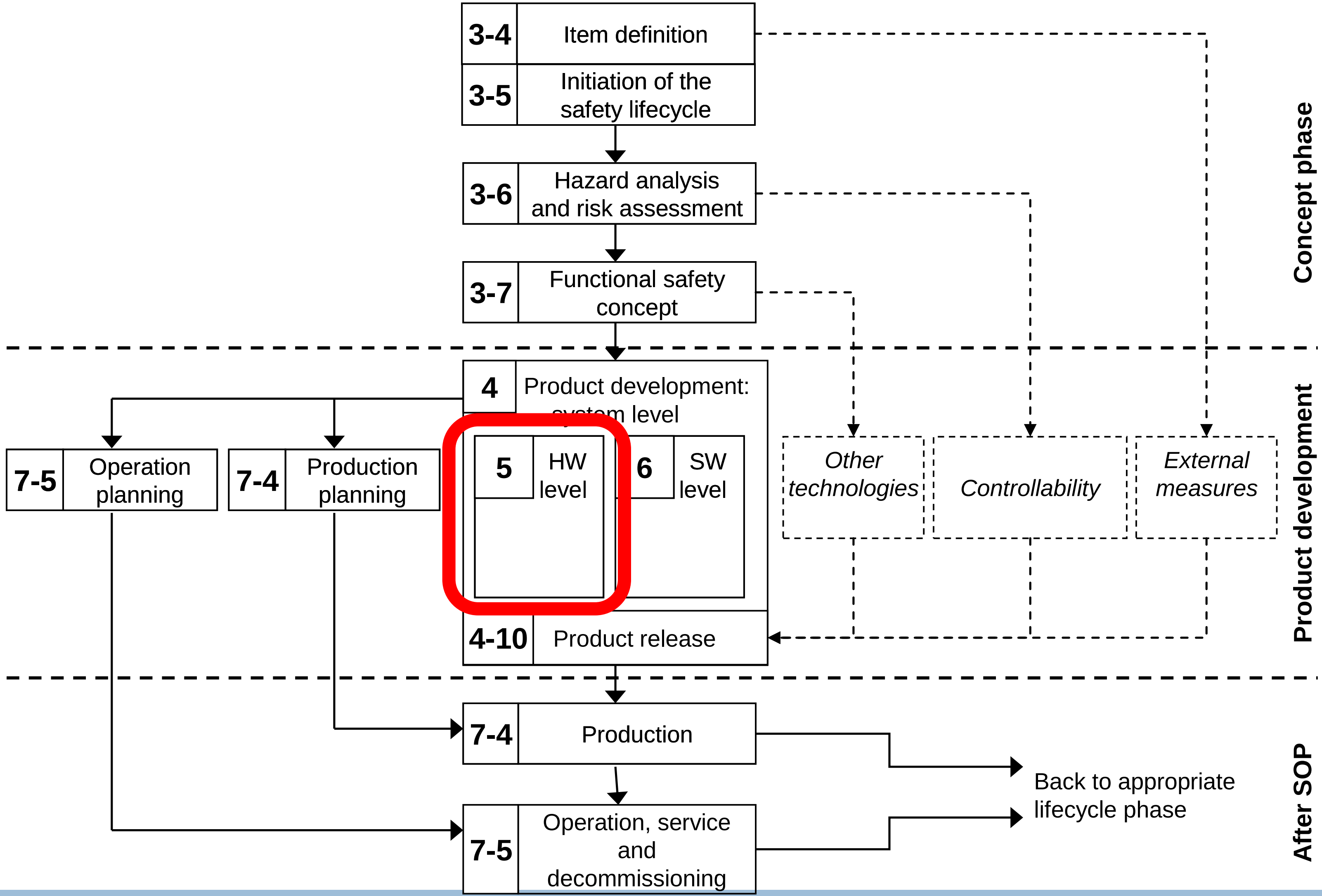
1) Identify relevant safety lifecycle steps for item system engineering



2) Identify Technical Safety Concept

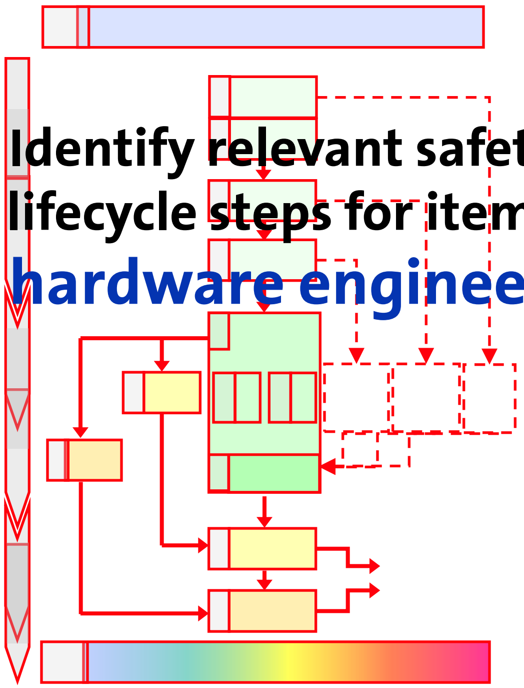


ISO 26262 Process Overview



ISO 26262 Hardware Design

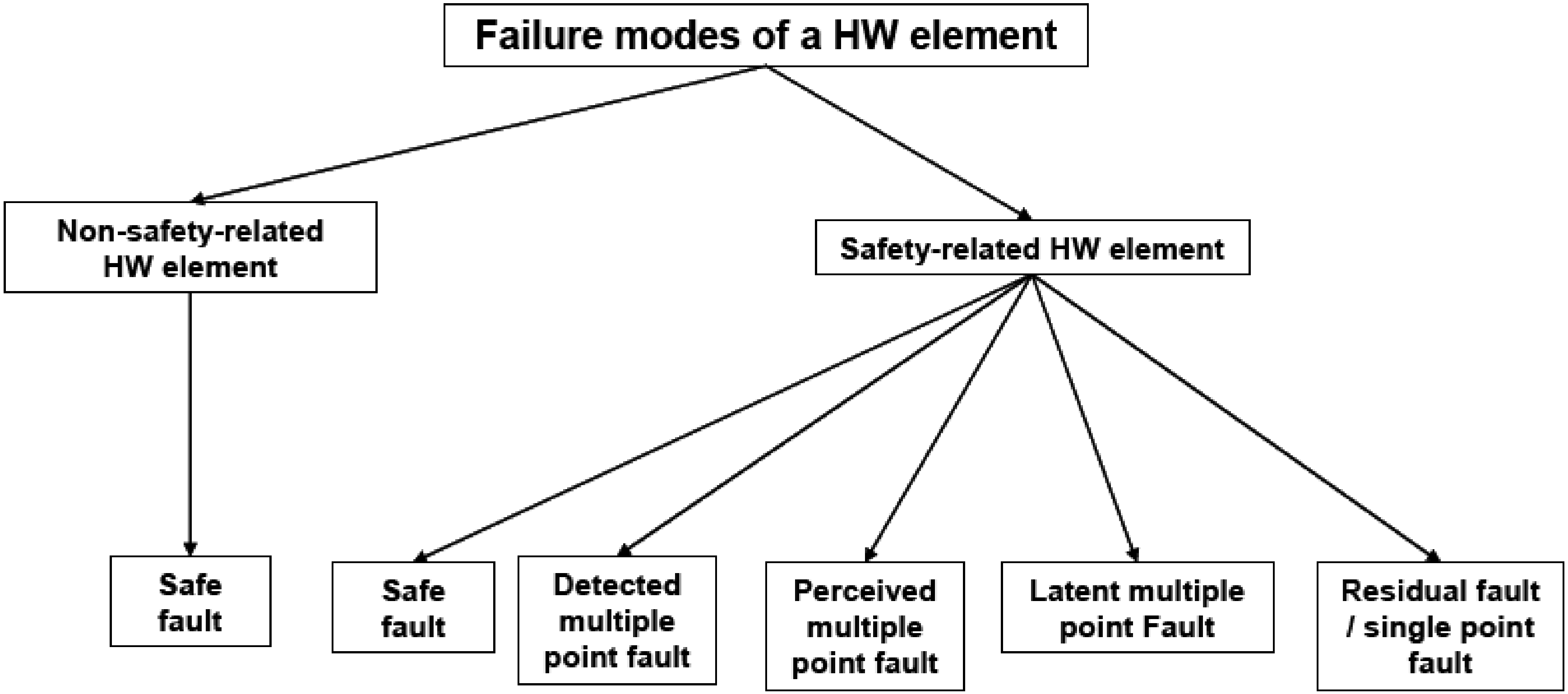
For a given Hardware "Item":



1) **Identify relevant safety lifecycle steps for item** **hardware engineering**

2) **Identify Hardware safety requirements**
3) **Design hardware, protecting for safety concerns**
4) **Evaluate hardware mechanisms for fault handling**
5) **Assess residual, single and dual point faults for residual risk and violation of safety goals**
6) **Plan for Hardware safety integration and test**
7) **Define requirements for Hw/Sw interface to support Technical Safety Concept**

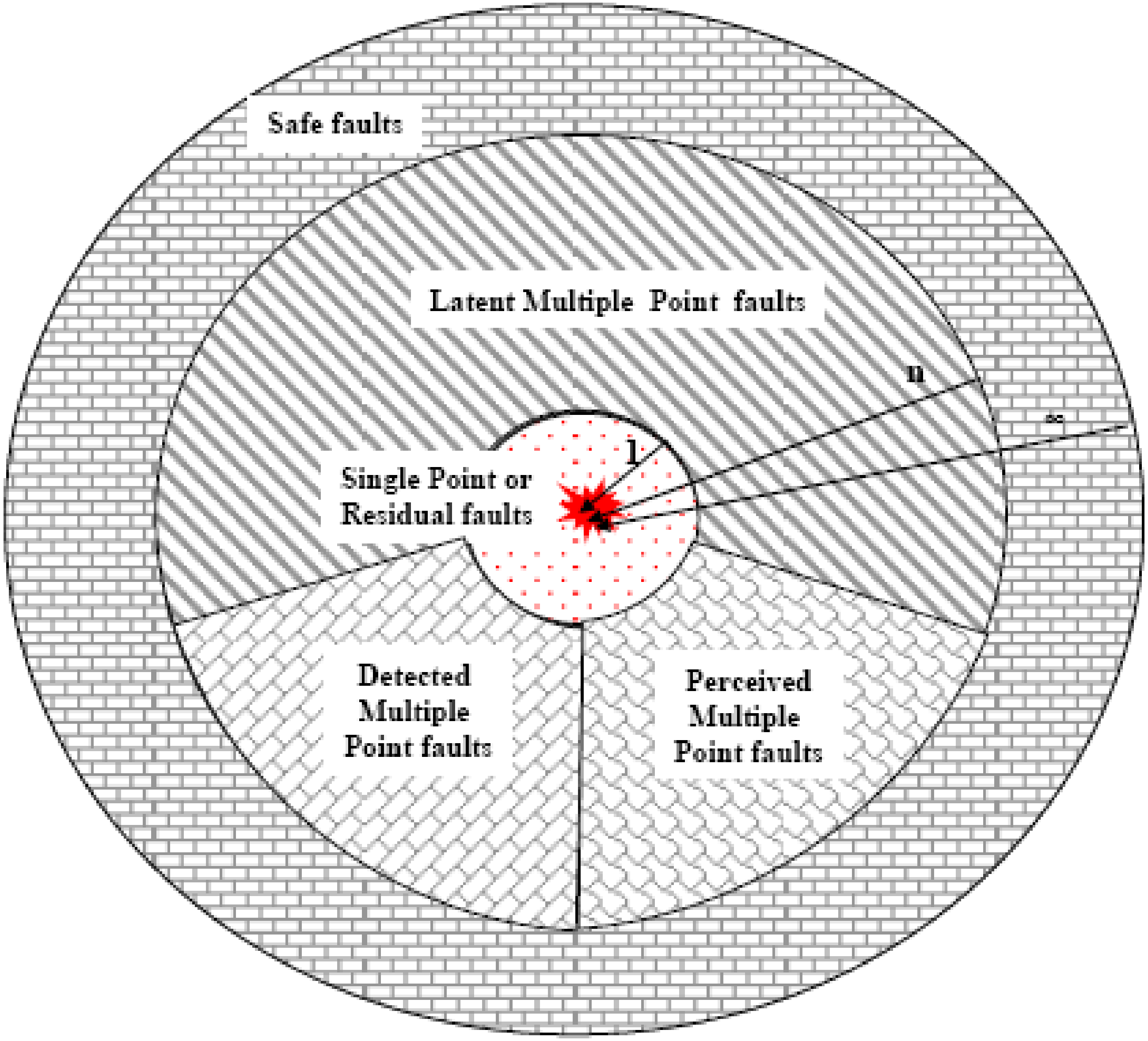
ISO 26262 Hardware Design: Fault Model



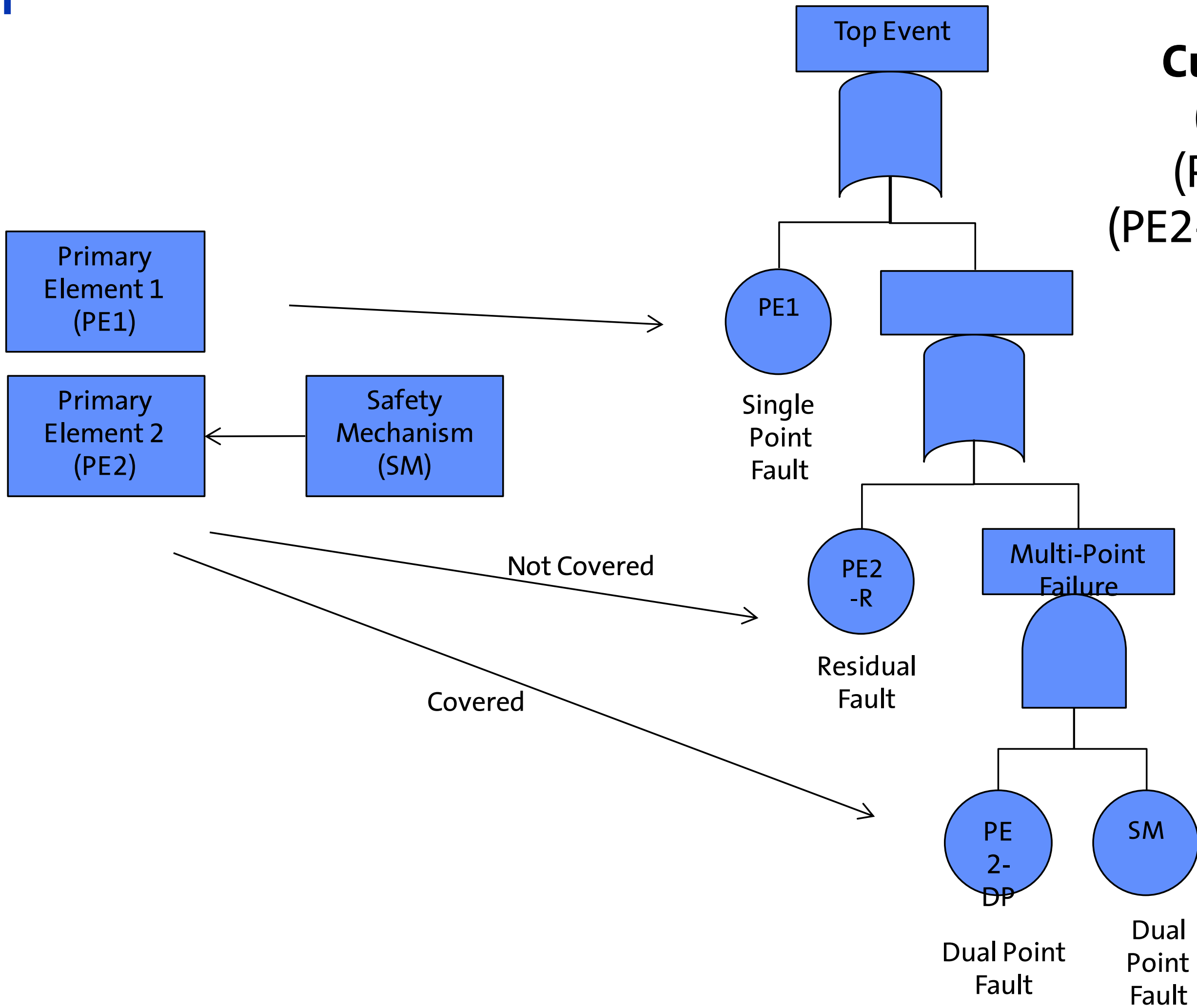
ISO 26262 Hardware Design: Fault Definitions

- **Safe fault**: fault whose occurrence will not significantly increase the probability of violation of a safety goal
- **Single point fault**: fault in an element which is not covered by a safety mechanism and where the fault leads directly to the violation of a safety goal
- **Residual fault**: portion of a fault which by itself leads to the violation of a safety goal, occurring in a hardware element, where that portion of the fault is not covered by existing safety mechanisms
- **Multiple point fault**: one fault of several independent faults that in combination, leads to a multiple point failure (either detected, perceived, or latent)
- **Latent fault**: multiple point fault whose presence is not detected by a safety mechanism nor perceived by the driver

ISO 26262 Hardware Design: Fault Model



ISO 26262 Hardware Design: Fault Tree Representation



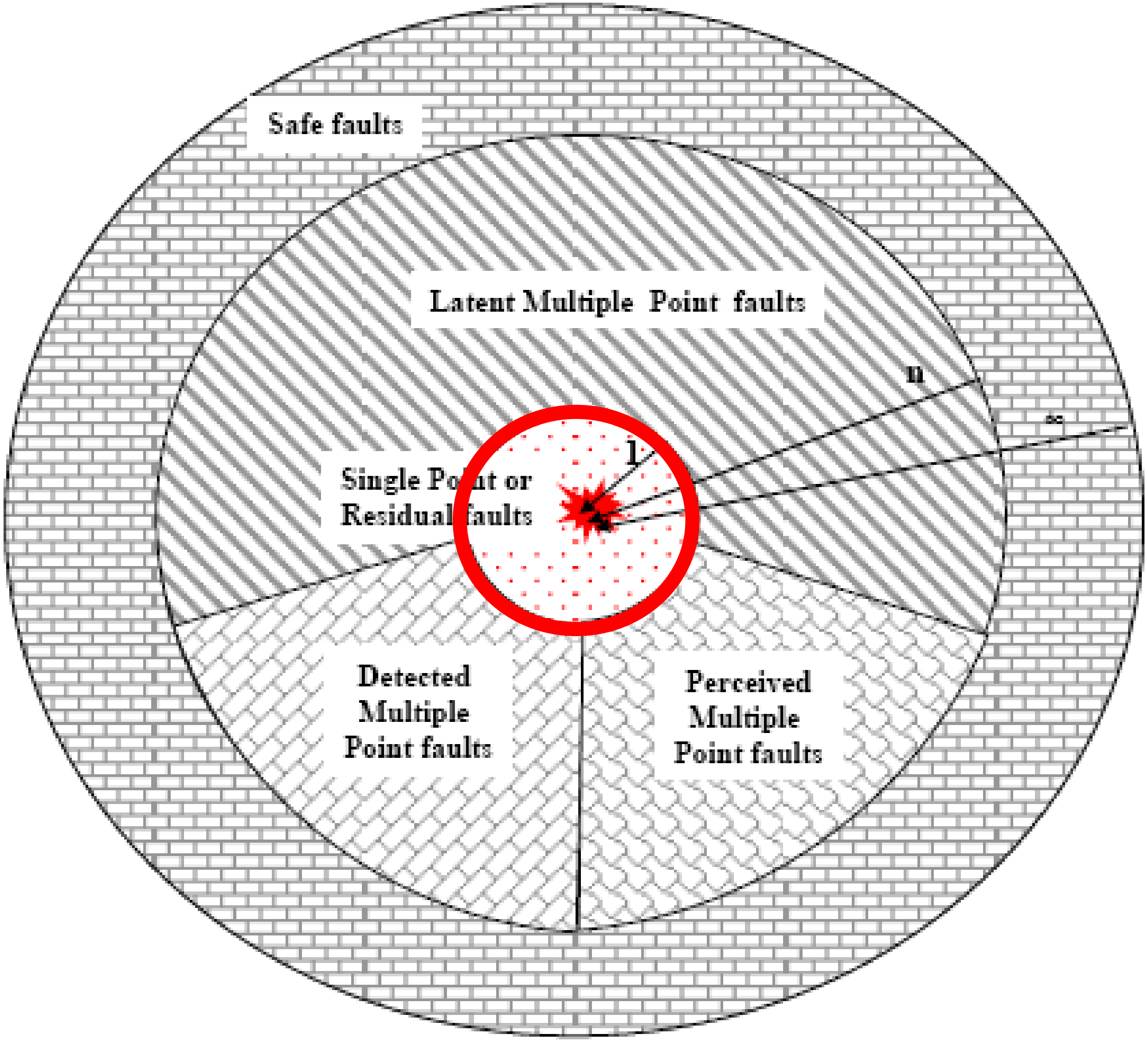
Cut Sets

(PE1)

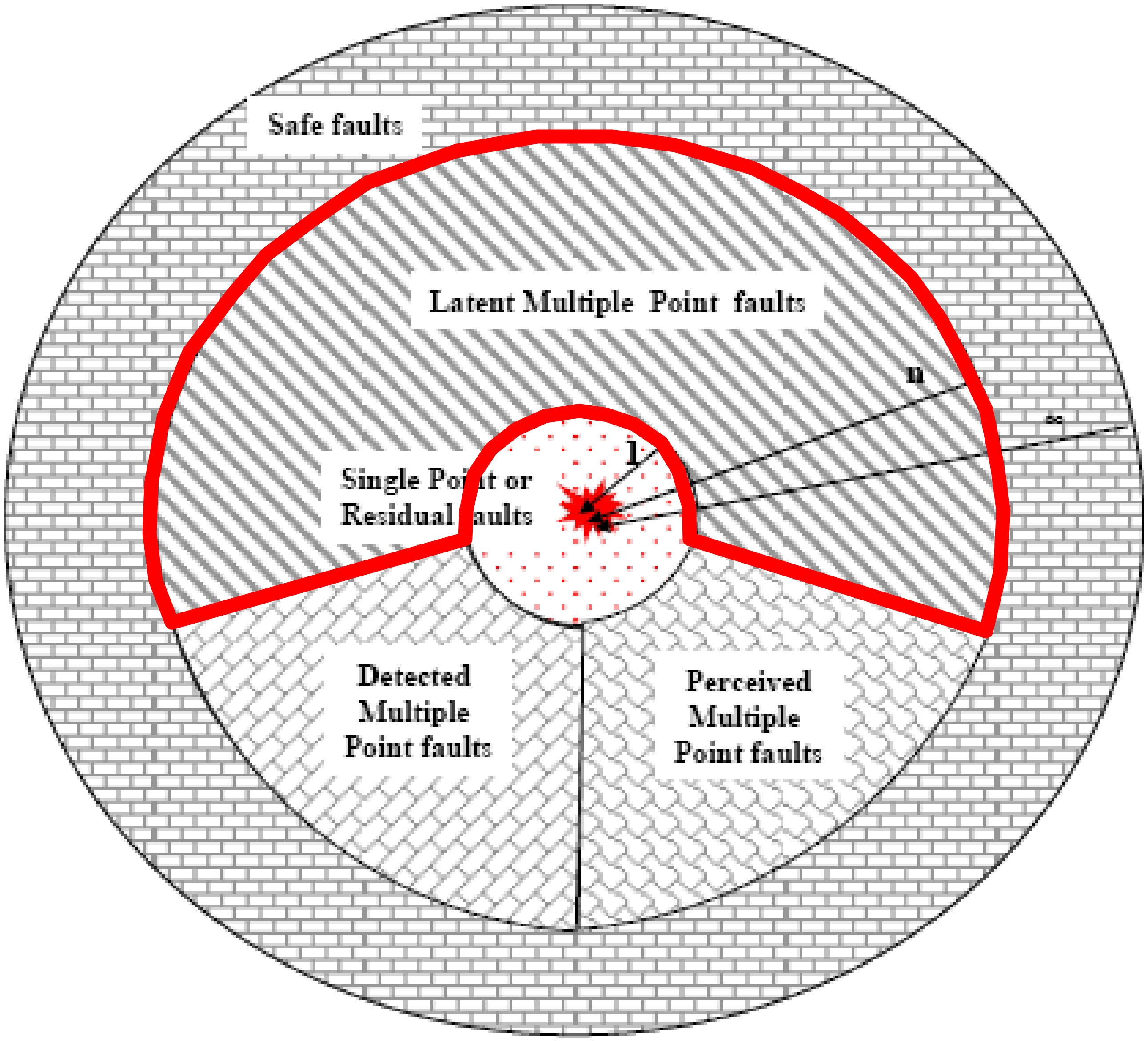
(PE2-R)

(PE2-DP&SM)

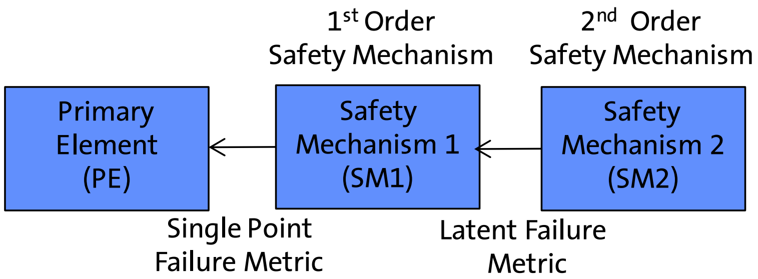
ISO 26262 Hardware Design: Fault Model



ISO 26262 Hardware Design: Fault Model

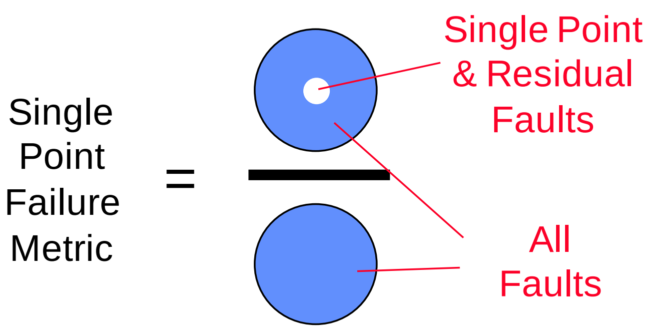


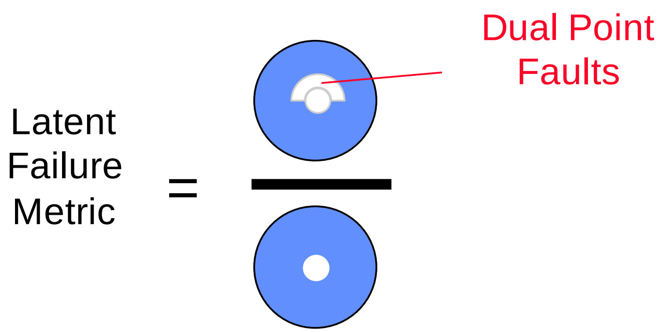
ISO 26262 Hardware Design: Diagnostic Coverage Metrics



Evaluates level of diagnostic coverage and safe faults vs. undetected faults

Based on safety goal ASIL





Based on Failure Rates of Faults that may lead to a violation of a safety goal

Table E.1 — Single point faults metric and latent faults metric target values

	ASIL B	ASIL C	ASIL D
Single point faults metric	> 90 %	> 97 %	> 99 %
Latent faults metric	> 60 %	> 80 %	> 90 %

ISO 26262 Hardware Design: Diagnostic Coverage Metrics (Part 5 Annex D)

Provides diagnostic coverage levels for typical diagnostics

Can be used as basis for assessment of diagnostic coverage

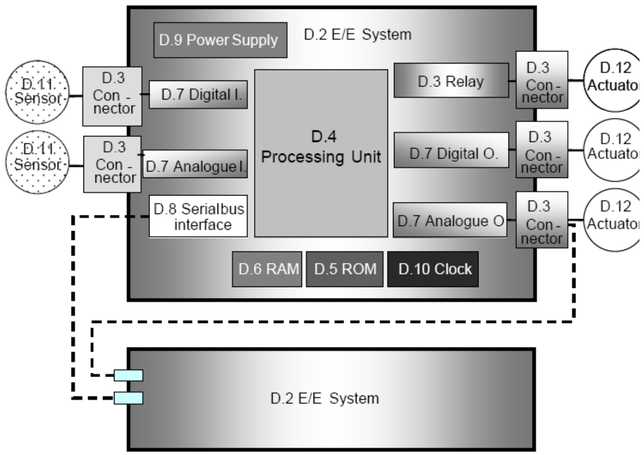


Figure D.1 — Generic hardware of a system

General Model Of A System

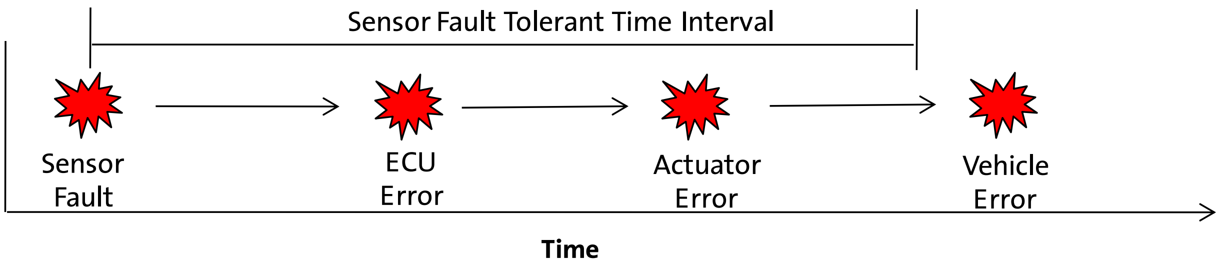
Table D.5 — Invariable memory ranges

Diagnostic technique/measure	See overview of techniques	Maximum diagnostic coverage considered achievable	Notes
Parity bit	-	Low	
Detection of memory data failures with error-detection-correction codes (EDC)	D.2.4.1	High	The effectiveness depends on the number of redundant bits.
Modified checksum	D.2.4.2	Low	-
Signature of one byte (8-bit) (CRC)	D.2.4.3	Medium	The effectiveness of the signature depends on the polynomial in relation to the block length of the information to be protected.
Signature of a double byte (16-bit) (CRC)	D.2.4.4	High	The effectiveness of the signature depends on the polynomial in relation to the block length of the information to be protected.
Block replication	D.2.4.5	High	-

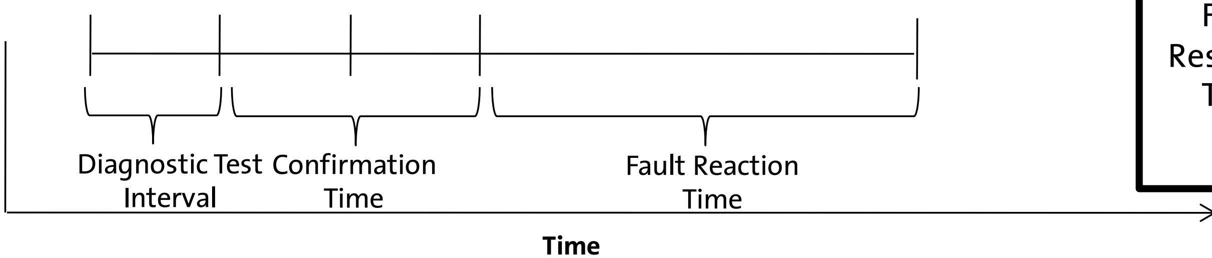
Example Diagnostics & Their Coverage Levels

ISO 26262 Hardware Design: Fault Response Time

Fault Tolerant Time Interval



Safety Mechanism Fault Response Time



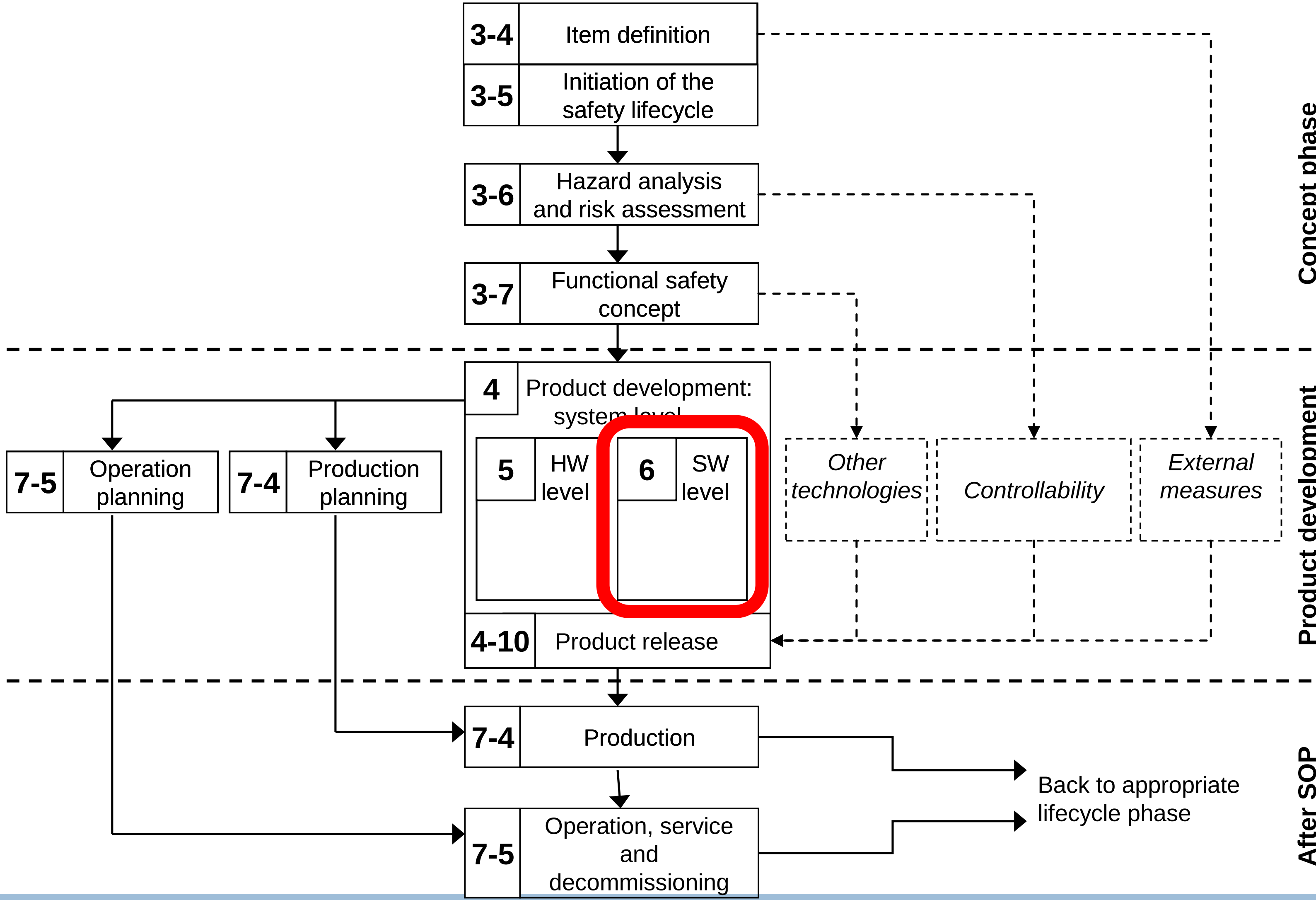
Fault Response Time $\overset{?}{\leq}$ Fault Tolerant Time Interval

Also

Multiple point fault detection interval - time span to detect multiple point fault (1.77) before it may contribute to a multiple point failure

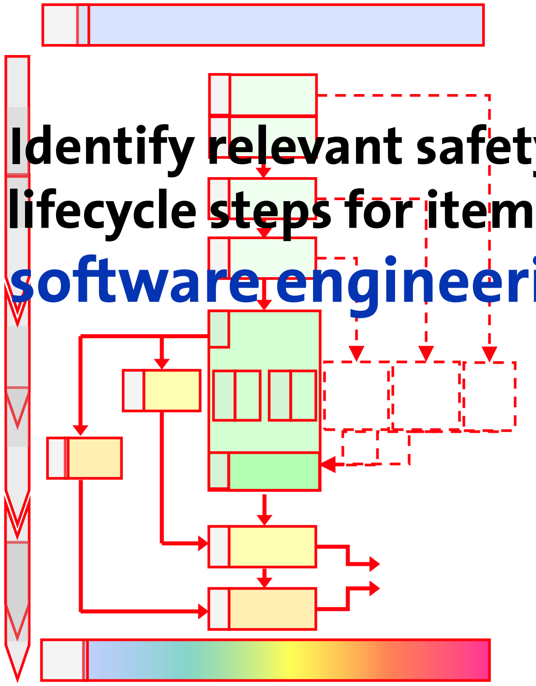
Typically one to several driving cycles (power up / power down)

ISO 26262 Process Overview



ISO 26262 Software Design

For a given Software "Item":



1) Identify relevant safety lifecycle steps for item

software engineering

2) Identify software safety requirements

3) Design software architecture, protecting for safety concerns

4) Design software units, protecting for safety concerns

5) Plan and conduct software unit testing

6) Plan and conduct software integration testing

7) Plan and conduct software safety verification testing

ISO 26262 Software Design

Table 5 — Mechanisms for error detection at the software architectural level

Methods		ASIL A	ASIL B	ASIL C	ASIL D
1a	Plausibility check[a]	++	++	++	++
1b	Detection of data errors[b]	+	+	+	+
1c	External monitoring facility	o	+	+	++
1d	Control flow monitoring	o	+	++	++
1e	Diverse software design[c]	o	o	+	++

a Plausibility checks include assertion checks. Complex plausibility checks can be realised by using a reference model of the desired behaviour.

b Types of methods that may be used to detect data errors include error detecting codes and multiple data storage.

c Diverse software design is not intended to imply n-version programming.

ISO 26262 Software Design

Table 6 — Mechanisms for error handling at the software architectural level

Methods		ASIL A	ASIL B	ASIL C	ASIL D
1a	Static recovery mechanism[a]	+	+	+	+
1b	Graceful degradation[b]	+	+	++	++
1c	Independent parallel redundancy[c]	o	o	+	++
1d	Correcting codes for data	+	+	+	+

[a] Static recovery mechanisms can be realised by recovery blocks, backward recovery, forward recovery and recovery through repetition.

[b] Graceful degradation at the software level refers to prioritising functions to minimise the adverse effects of potential failures on functional safety.

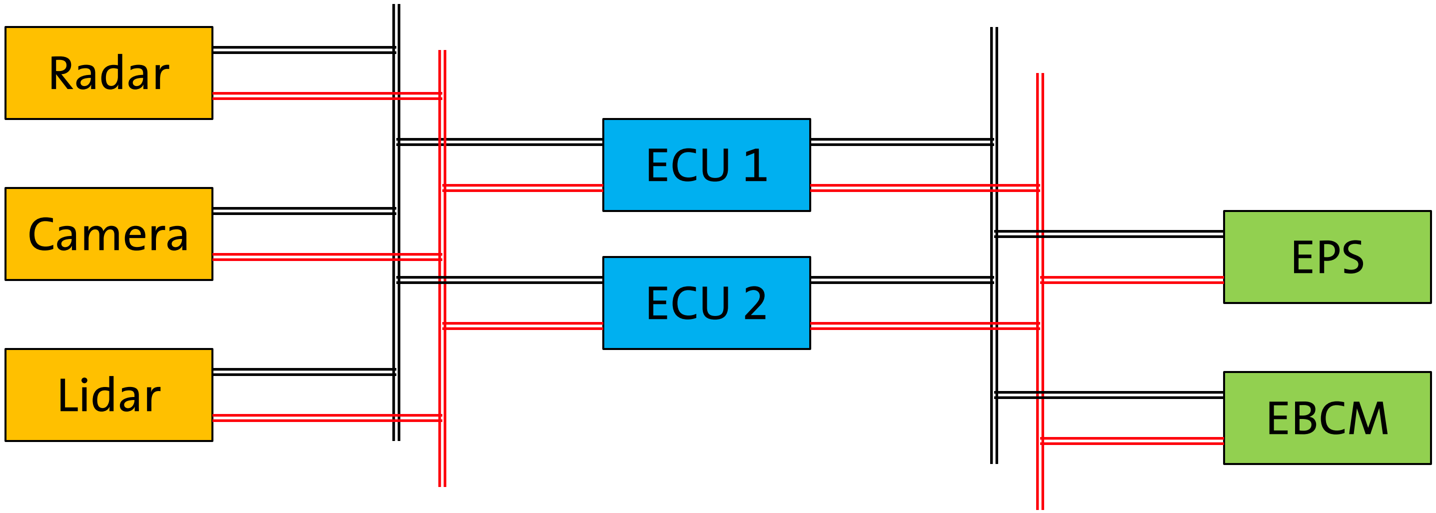
[c] For parallel redundancy to be independent there has to be dissimilar software in each parallel path.

Failure diagnosis in the run-time safety architecture

- Process considerations
  - Based on ISO 26262
- Architecture considerations
  - Fault detection and fault mitigation

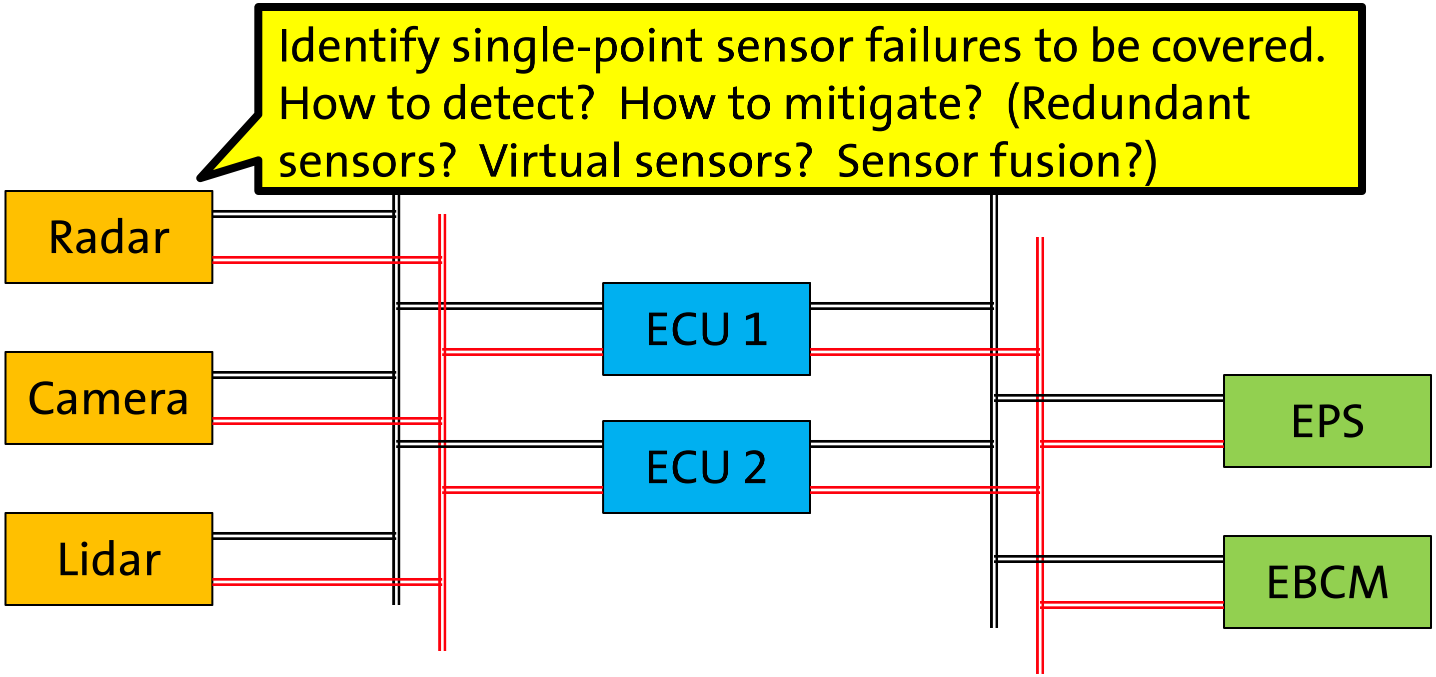
Architecture Considerations

For an imaginary autonomous steering & braking system



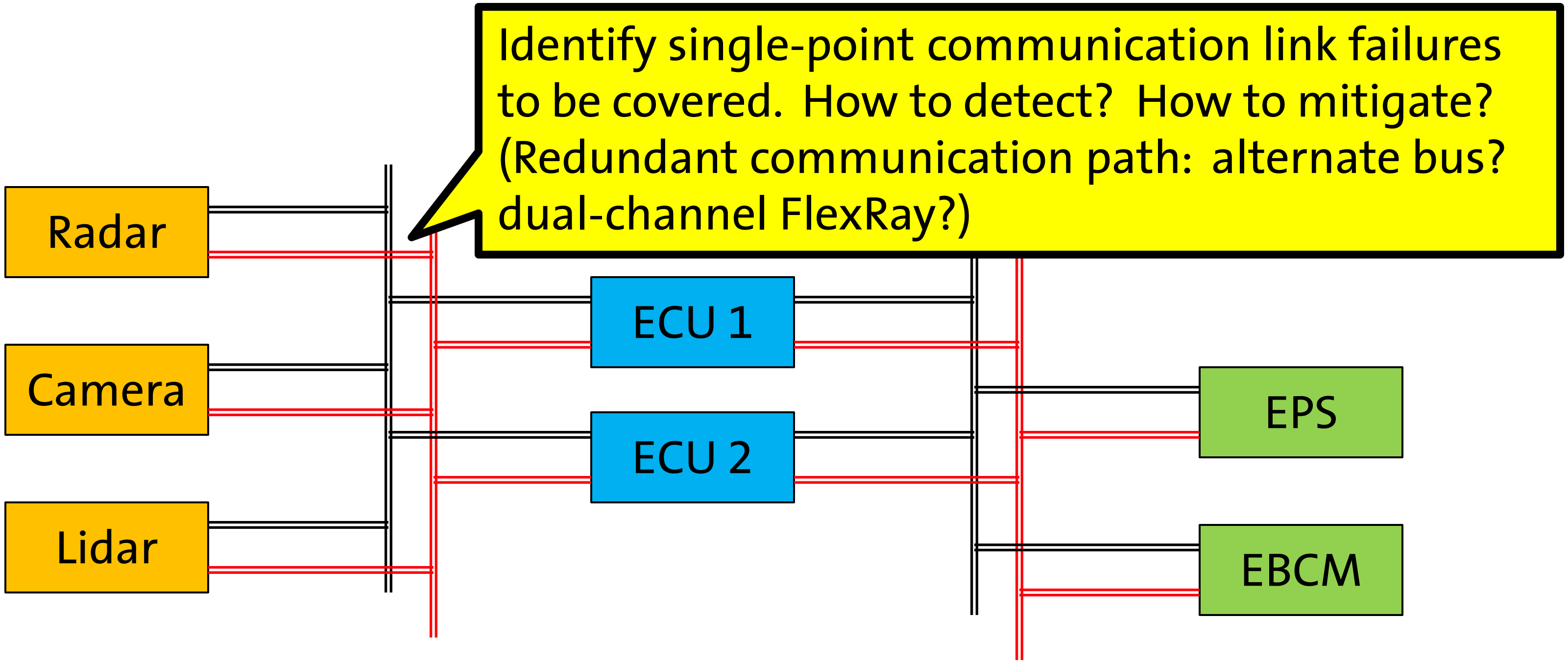
ECU = Electronic Control Unit
EPS = Electric Power Steering
EBCM = Electronic Brake Control Module

Architecture Considerations



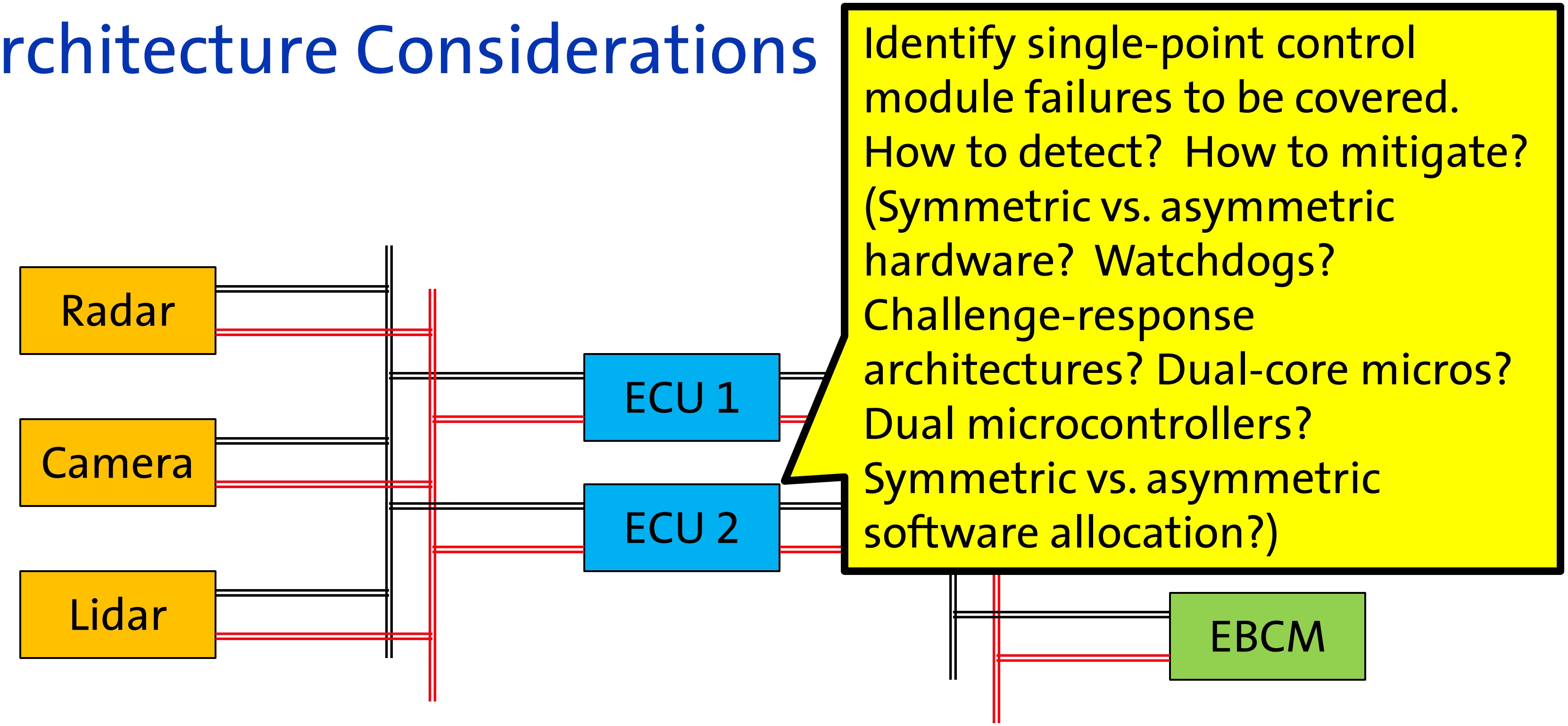
ECU = Electronic Control Unit
EPS = Electric Power Steering
EBCM = Electronic Brake Control Module

Architecture Considerations



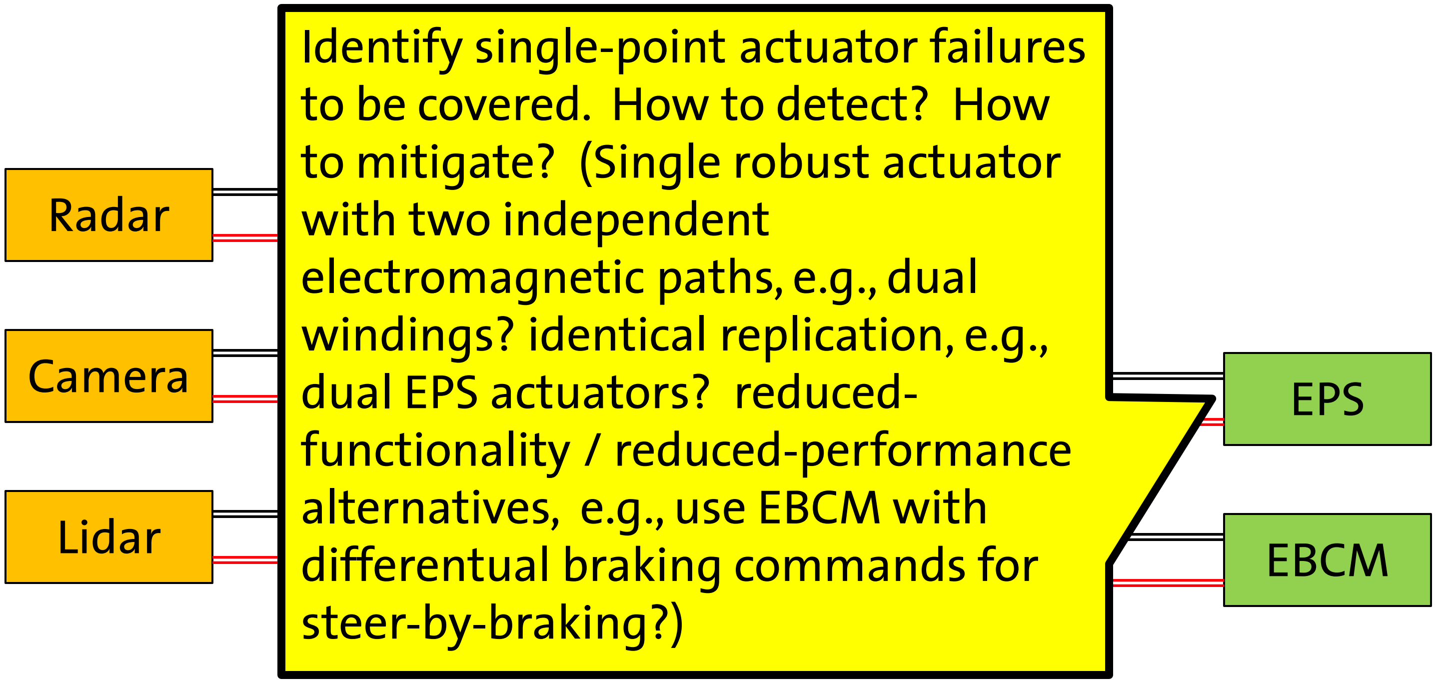
ECU = Electronic Control Unit
EPS = Electric Power Steering
EBCM = Electronic Brake Control Module

Architecture Considerations



ECU = Electronic Control Unit
EPS = Electric Power Steering
EBCM = Electronic Brake Control Module

Architecture Considerations



ECU = Electronic Control Unit
EPS = Electric Power Steering
EBCM = Electronic Brake Control Module

Architecture Considerations

- Identify fail-safe vs. fail-operational requirements (per ISO)
  - Identify faults to be considered (random hardware? software design?)
  - Identify fault detection and fault mitigation approaches
- Conduct single-element fault analysis
- Evaluate alternative fault-tolerance strategies
  - "Redundancies" for fault detection (watchdogs, etc.)
  - Application-specific vs. generic/systematic approaches
  - Physical vs. logical redundancies (model-based diagnosis)
  - Symmetric vs. asymmetric redundancy
  - Distributed vs. localized redundancy
  - Fail operational patterns (dual-duplex? triple modular redundancy?)

Summary and Conclusions

- High level automotive challenges
  - Energy
  - Environment
  - Safety
  - Connectivity
- Role of failure diagnosis in
  - Service / Maintenance
  - Run-time safety
- Importance of fault metrics for detection coverage per ISO 26262
  - Single-point fault metric
  - Latent fault metric
- Challenges
  - Warranty cost and NTF
  - Safety goal analysis for active safety and autonomous vehicle systems, in the presence of uncertainties in road conditions, traffic conditions, weather conditions, driver skill level, vehicle state of health

Thank-you for your attention!

- Questions?