Elektrobit

Introduction to Functional Safety

Hurley Davis

Director of Engineering, U.S., Elektrobit

November 8, 2018

© Elektrobit (EB) 2018

What is Functional Safety?

ISO 26262 Definitions

Safety	Absence of unreasonable risk
Risk	Combination of Probability and Severity
Functional Safety	Absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems
E/E System	System of electrical and electronic components including software

© Elektrobit (EB) 2018

Elektrobit

ISO 26262 Functional Safety Standard

- Introduced in 2011
- Second addition expected late 2018
- Automotive safety lifecycle
- Automotive risk-based approach
- Requirements for validation and confirmation measures

© Elektrobit (EB) 2018

ISO 26262 Consists of Ten Parts

1) Vocabulary

2) Management of Functional Safety
- Overall Safety Management
- Safety Management during Item Development
- Safety Management after SOP

3) Concept Phase
- Item Definition
- Start Safety Lifecycle
- Hazard & Risk Analysis
- Functional Safety Concept

4) System Development
- System Dev. Initiation
- System Requirements
- System Design
- Release
- Validation & Safety Assessment
- Item Integration, Test

5) Hardware Development
- Initiation
- HW Safety Requirements
- HW Designe
- HW Architectural Metrics
- HW Failure Rate
- HW Integration and Testing

HSI

6) Software Development
- Initiation
- SW Safety Requirements
- SW Design
- SW Unit Design & Implementation
- SW Unit Testing
- SW Integration and Testing
- Verification of SW Safety Requirements

7) Production and Operation
- Production
- Service
- Observation

Safety Lifecycle

ISO 26262 has
- 10 parts
- 500 pages
- 43 Chapters
- 600 Requirements
- 100 Work Products
- 180 Methods

8) Supporting Processes
- Distributed Development
- Mgmt. of Safety Requirements
- Configuration Management
- Change Management
- Verification
- Documentation
- Qualification of SW Tools
- Qualification of SW Comp.
- Qualification of HW Comp.
- Proven in Use Argumentation

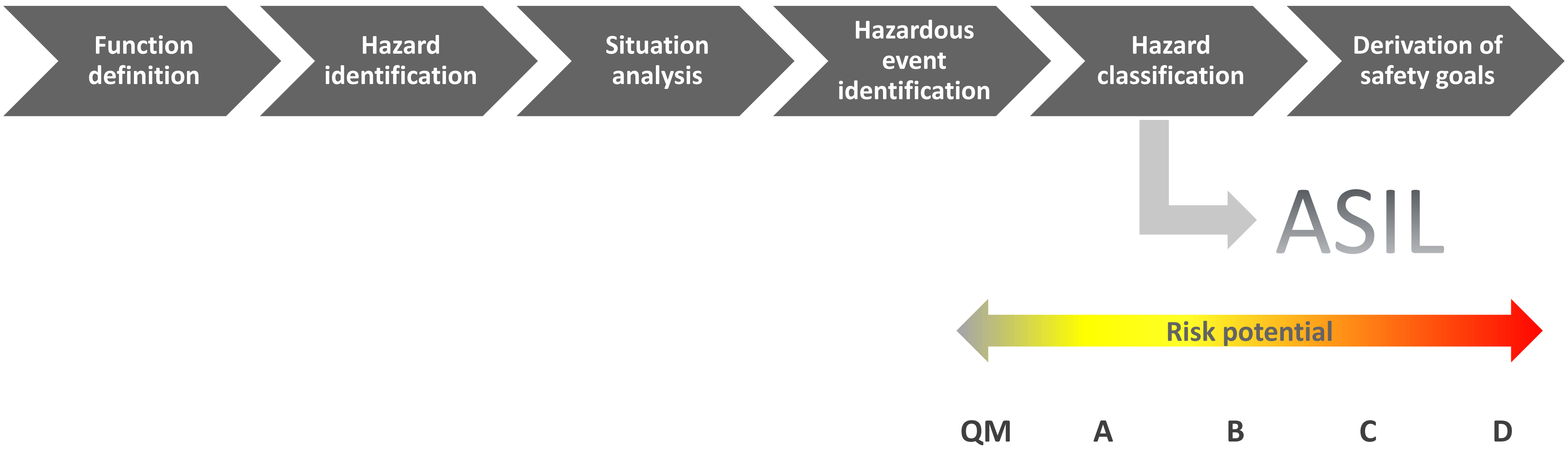
9) ASIL-Oriented and Safety-Oriented Analysis
- Requirement Decomposition
- Coexistence of Elements
- Safety Analysis
- Analysis of dependent Failures

10) Guide-line

© Elektrobit (EB) 2018

Automotive Safety Integrity Level (ASIL)

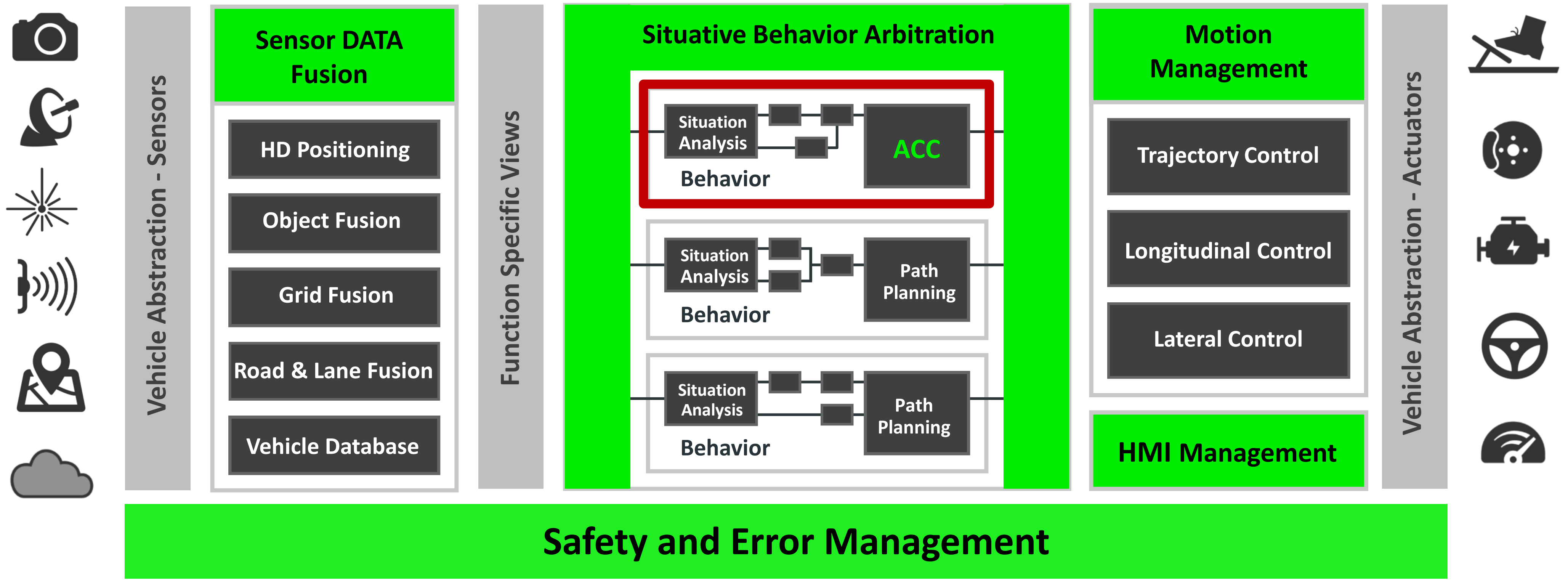
ISO 26262:2011, Part 3 – Section 7.1: Hazard Analysis and Risk Assessment (HARA)



HARA Workflow

Step 1 - Define the function to be analyzed

Example: Adaptive Cruise Control (ACC) with emergency braking

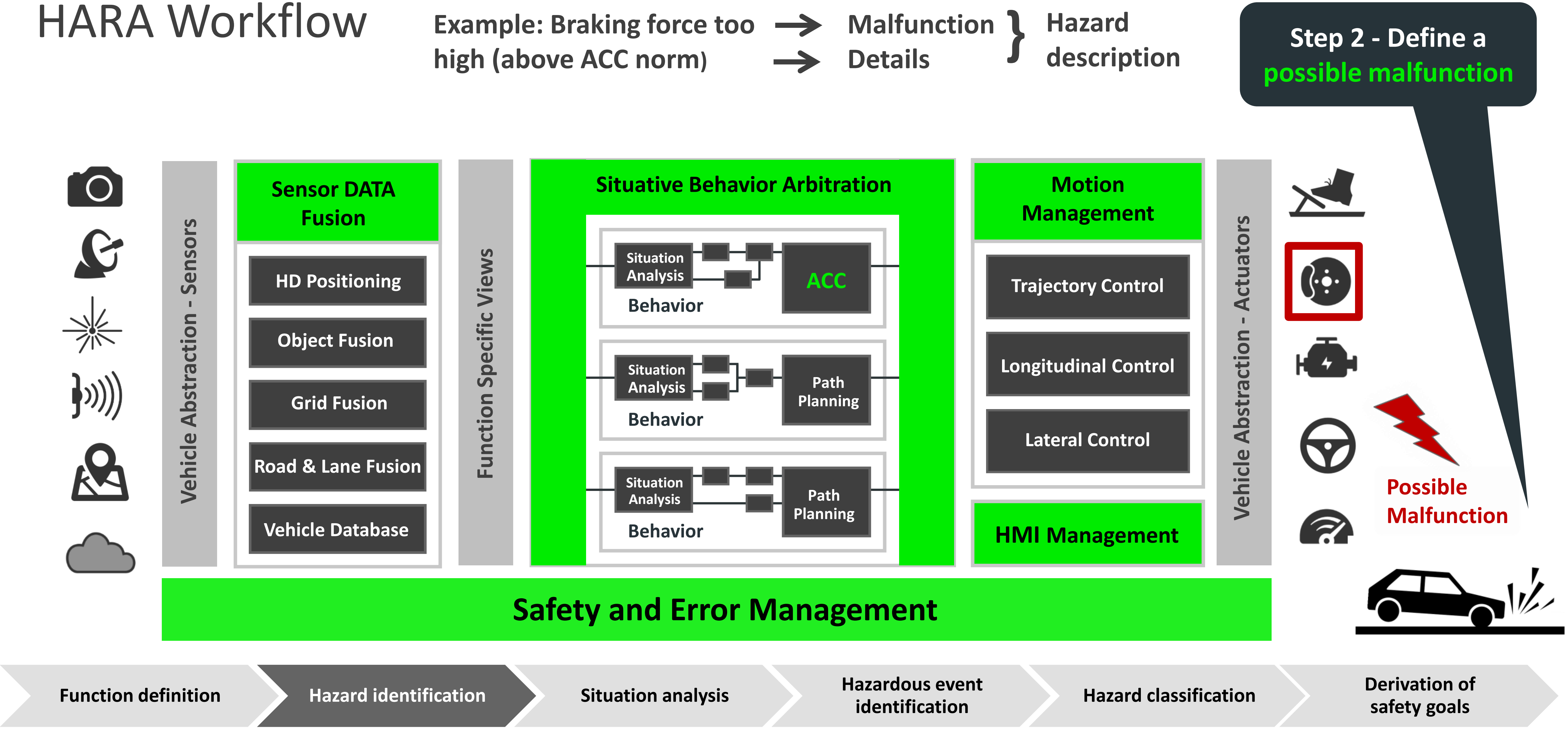


Function definition → Hazard identification → Situation analysis → Hazardous event identification → Hazard classification → Derivation of safety goals

© Elektrobit (EB) 2018

HARA Workflow

Example: Braking force too high (above ACC norm) → Malfunction Details } Hazard description



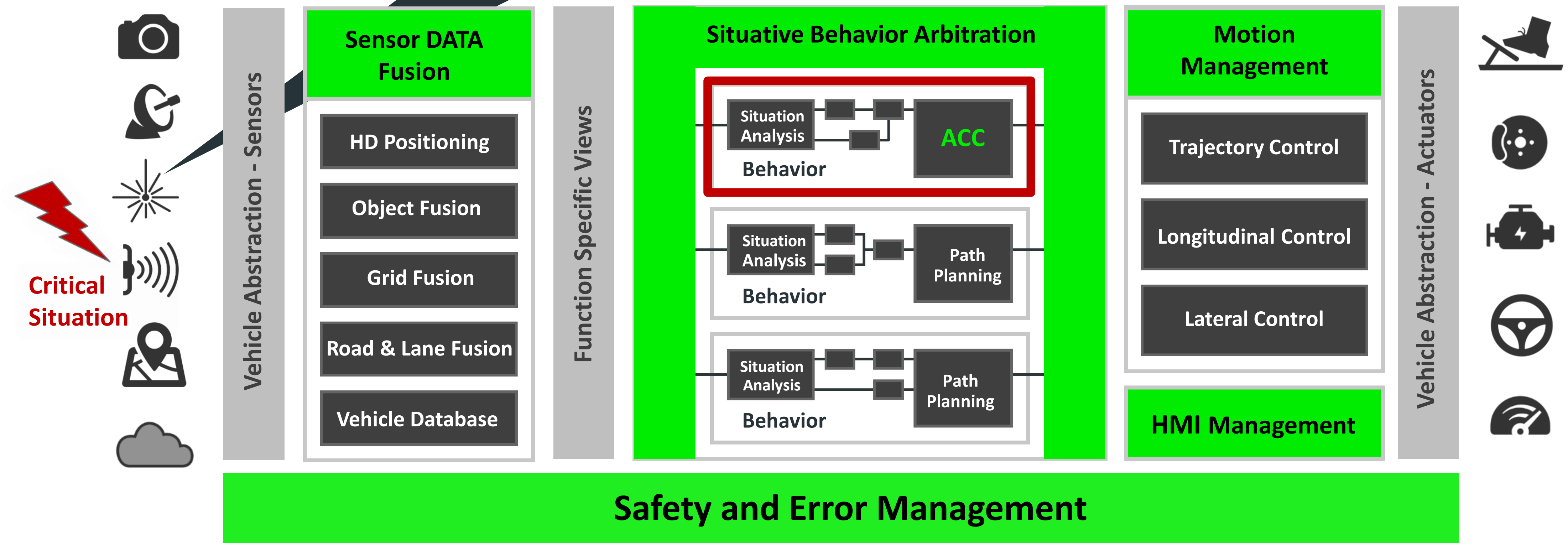
© Elektrobit (EB) 2018

HARA Workflow

Step 3 - Define a critical situation

Example:
Normal highway driving in fog (degraded view) with high speed (rear traffic near)

→ Operating mode
→ Operational situation
→ Environmental condition
Speed (details)



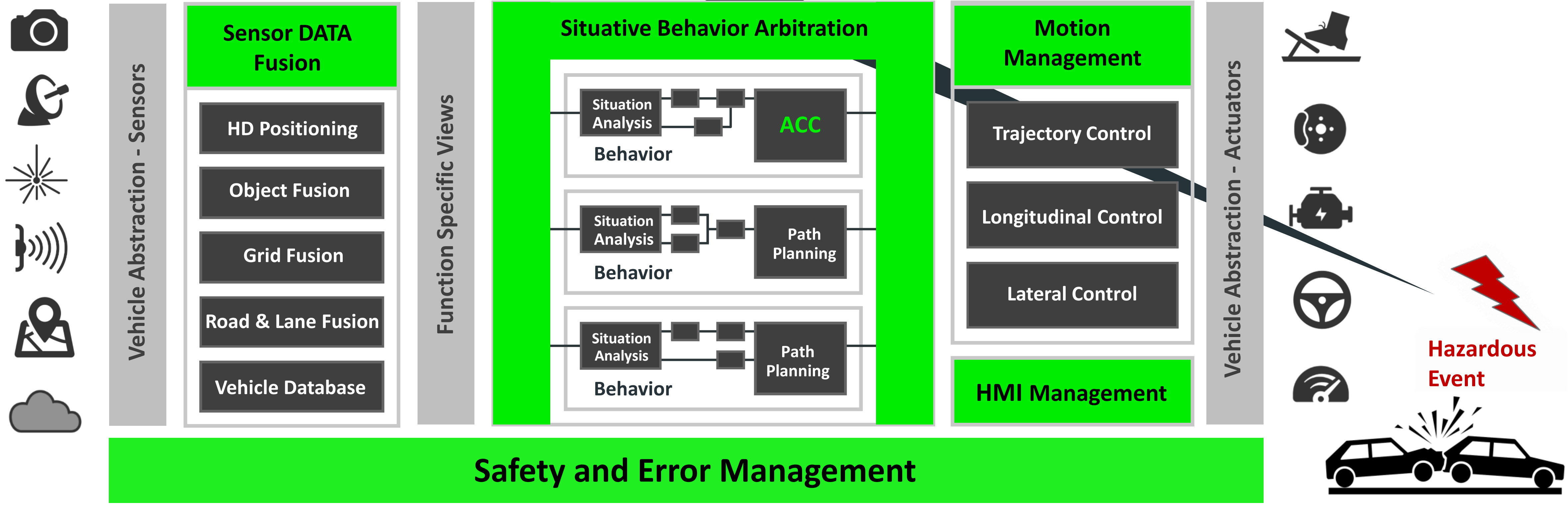
Function definition → Hazard identification → **Situation analysis** → Hazardous event identification → Hazard classification → Derivation of safety goals

© Elektrobit (EB) 2018

HARA Workflow

Step 4 - Evaluate consequences of the malfunction

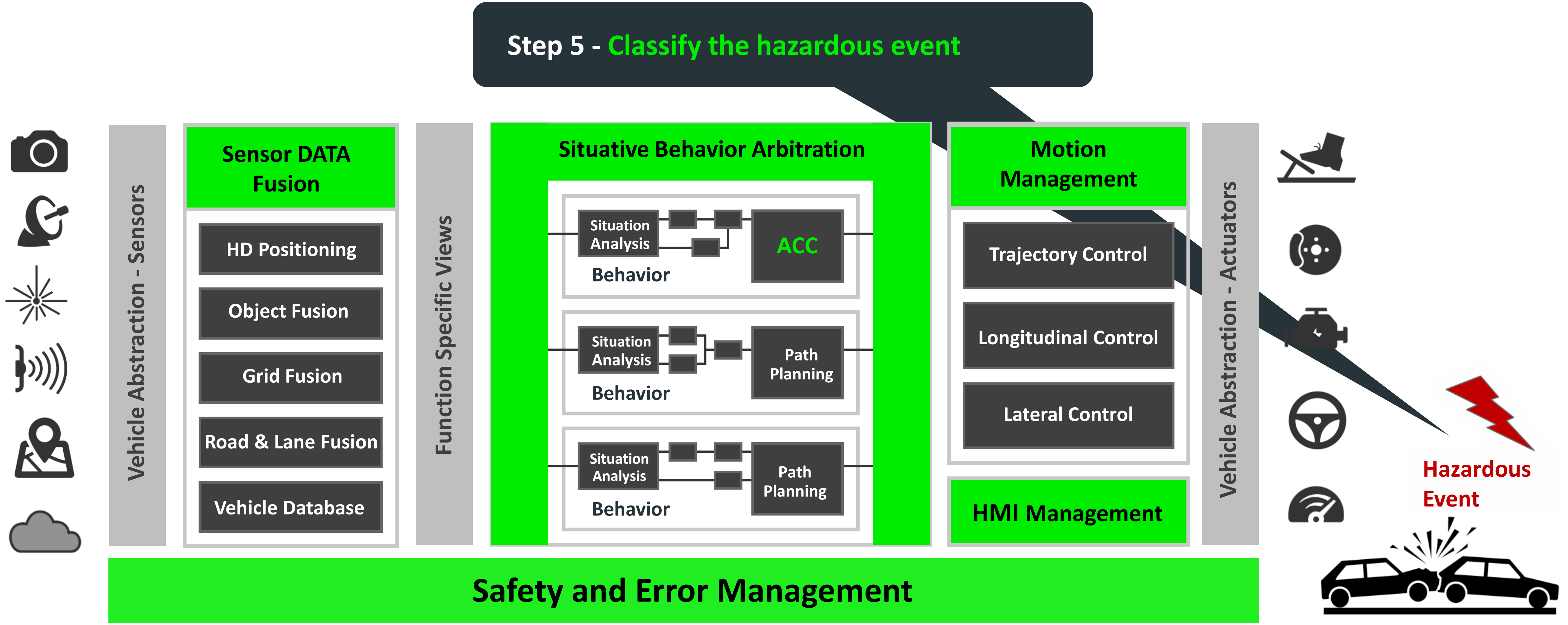
Rear-end collision with speed difference > 25 mph → Hazardous Event Details } Malfunction Effect



Function definition → Hazard identification → Situation analysis → **Hazardous event identification** → Hazard classification → Derivation of safety goals

© Elektrobit (EB) 2018

HARA Workflow



Function definition → Hazard identification → Situation analysis → Hazardous event identification → **Hazard classification** → Derivation of safety goals

© Elektrobit (EB) 2018

Hazard Classification

Severity, exposure and controllability

Severity (S)

Degree of potential harm to persons

- S0: No injuries
- S1: Light or moderate injuries
- S2: Severe and life threatening injuries
- S3: Life threatening injuries fatal injuries

Exposure (E)

Probability of being in a situation

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

Controllability (C)

Ability to avoid harm through reaction of the persons involved

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

© Elektrobit (EB) 2018

Elektrobit

ASIL Level derived from

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

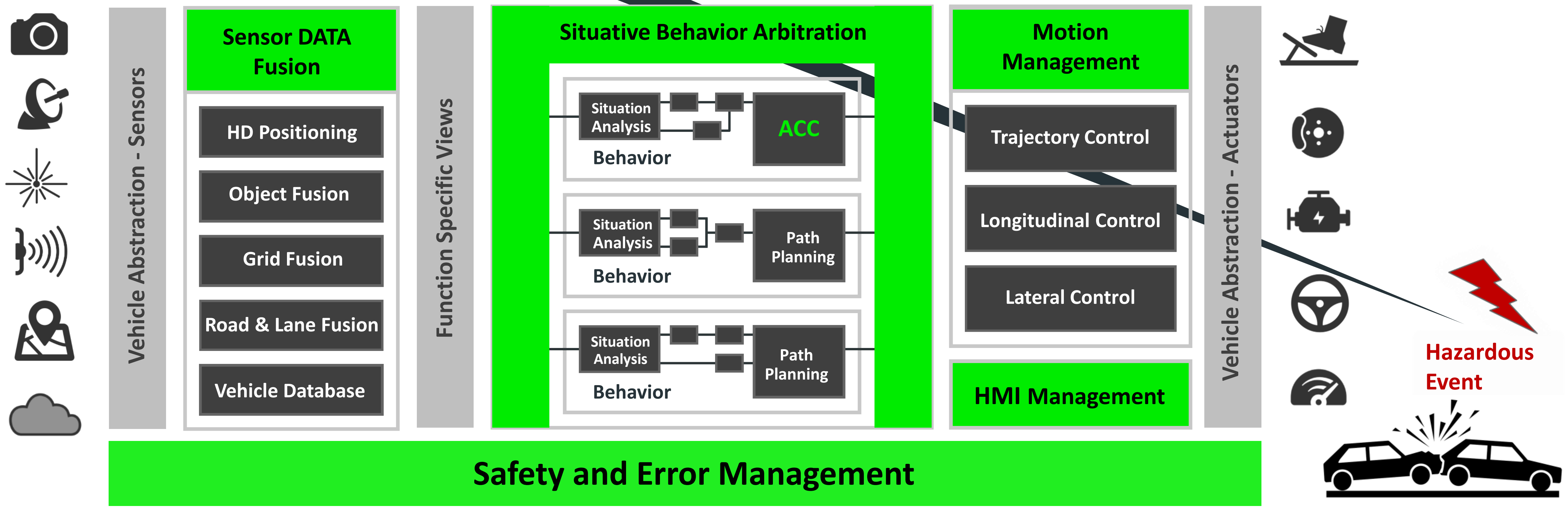
© Elektrobit (EB) 2018

HARA Workflow

Step 5 - Classify the hazardous event

EXAMPLE:

Severity (of potential harm)	Exposure (of situation)	Controllability (of hazardous event)	ASIL Determination
S3 - Life-threatening or fatal injuries	E3 - Medium probability	C3 - Difficult to control or uncontrollable	C



Function definition → Hazard identification → Situation analysis → Hazardous event identification → **Hazard classification** → Derivation of safety goals

© Elektrobit (EB) 2018

Elektrobit

Development Methods Dependent on ASIL Levels

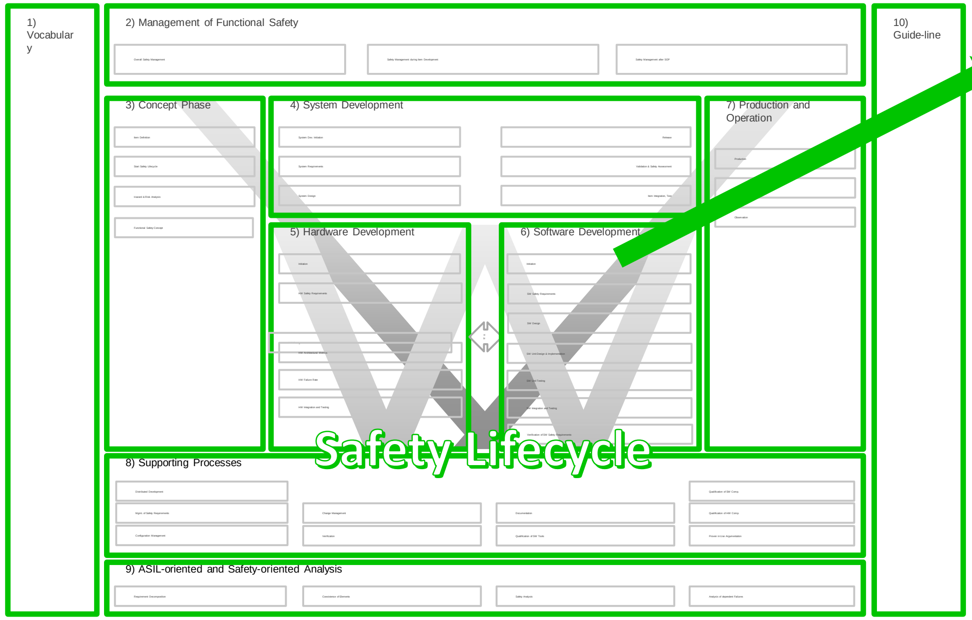


Table 15 — Methods for software integration testing

	Methods	ASIL			
		A	B	C	D
1a	Requirements-based test	++	++	++	++
1b	External interface test	++	++	++	++
1c	Fault injection test[a]	+	+	++	++
1d	Resource usage test[b, c]	+	+	+	++
1e	Back-to-back test between model and code, if applicable[d]	+	+	++	++

[a] This includes injection of arbitrary faults in order to test safety mechanisms (e.g. by corrupting software or hardware components)

[b] To ensure the fulfilment of requirements influenced by the hardware architectural design with sufficient tolerance, properties such as average and maximum processor performance, minimum or maximum execution times, storage usage (e.g. RAM for stack and heap, ROM for program and data) and the bandwidth of communication links (e.g. data busses) have to be determined.

[c] Some aspects of the resource usage test can only by evaluated properly when the software integration tests are executed on the target hardware or if the emulator for the target processor supports resource usage tests.

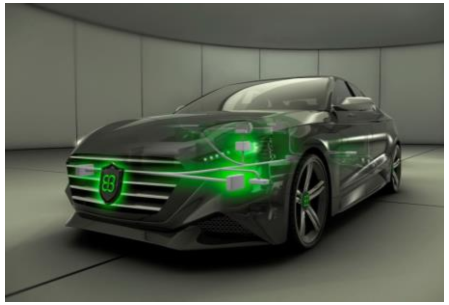
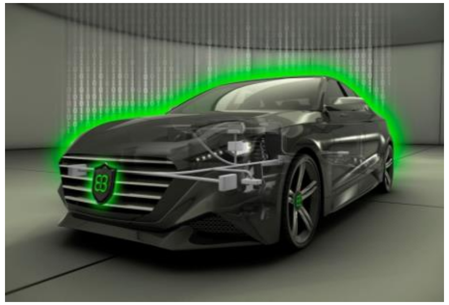
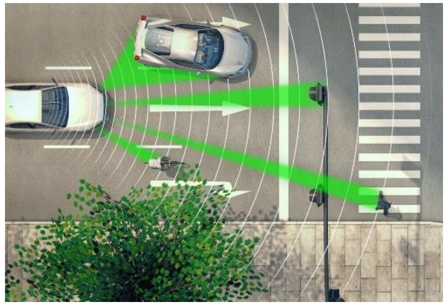
[d] This method requires a model that can simulate the functionality of the software components. Here, the model and code are stimulated in the same way and results compared with each other.

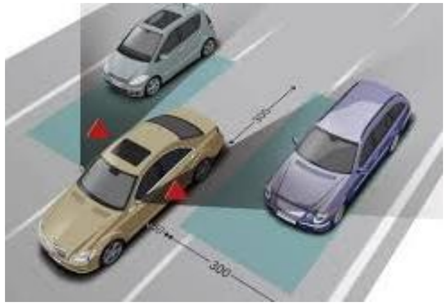
"++" The method is highly recommended for this ASIL.
"+" The method is recommended for this ASIL.
"o" The method has no recommendation for or against its usage for this ASIL.

© Elektrobit (EB) 2018

Elektrobit

Functional Safety Alone – Not Sufficient



Functional Safety	Security*	Safety of the Intended functionality (SOTIF)	Usage Safety	Active / Passive Safety
Protect from				
Hardware or software not working according to the specification	Unauthorized access or attack	Hazardous situation due to unspecified behavior	Poor usability induces risks	Accidents / accident impacts

* Issues can lead to safety hazards

© Elektrobit (EB) 2018

Elektrobit

Security Impacts Safety

Hacking vehicle steering

OTA/Wireless Capabilities

Unintended Access to Safety Functions

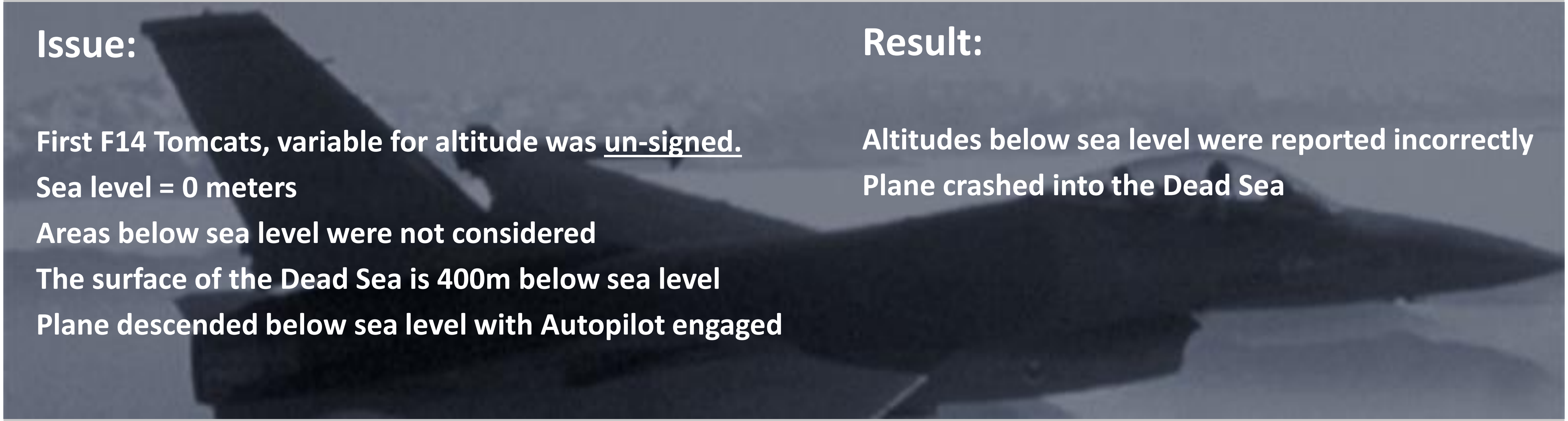
Hazards to Passengers

Security and Safety go hand-in-hand

© Elektrobit (EB) 2018

Safety of the Intended Functionality (SOTIF)

Airplane autopilot systems use the measured altitude to regulate horizontal tail.



Issue:

First F14 Tomcats, variable for altitude was <u>un-signed.</u>

Sea level = 0 meters

Areas below sea level were not considered

The surface of the Dead Sea is 400m below sea level

Plane descended below sea level with Autopilot engaged

Result:

Altitudes below sea level were reported incorrectly

Plane crashed into the Dead Sea

* Issues can lead to safety hazards

© Elektrobit (EB) 2018

Elektrobit

Safety of the Intended Functionality

Functional safety and nominal performance

- Bad weather conditions
- Hidden speed signs
- Assignment of traffic lights to lanes

Sensors can be functionally safe,
but is the performance sufficient?

© Elektrobit (EB) 2018

Elektrobit

Closing Remarks

- Technology – benefits and risks
- Laws are put into place to protect people
- State-of-the-art methods, processes and tools
- Internal Competence Development programs
- Professional Functional Safety Consulting
- We are committed to staying ahead of the technology curve and helping our customers, suppliers and partners do the same!

© Elektrobit (EB) 2018

Introduction to Functional Safety

Hurley Davis
Director of Engineering, U.S., Elektrobit
hurley.davis@elektrobit.com

© Elektrobit (EB) 2018