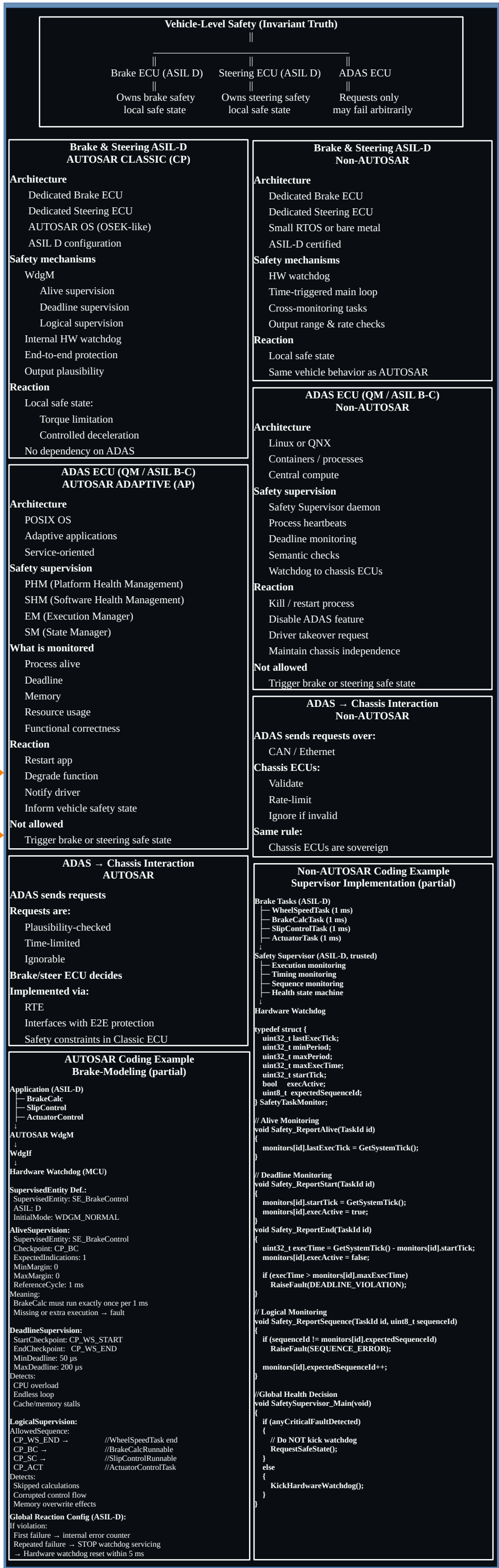
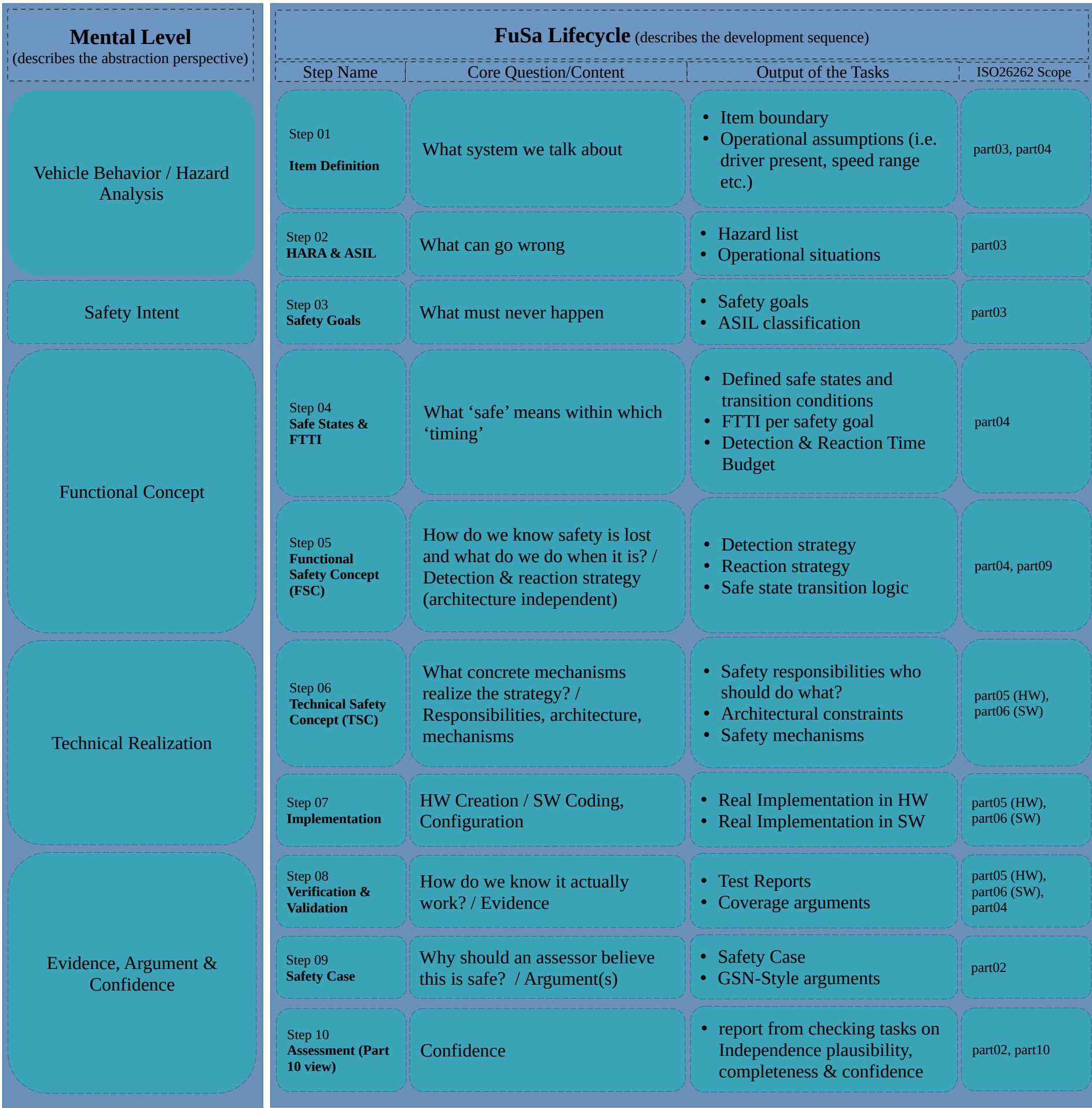


How Automotive Functional Safety really works: *a practical, ISO 26262:2018-Oriented Big Picture*

Version 1.0 ©Copyright by Yingtao WANG, Feb. 2026, Germany contact: Yingtao.Wang.de@gmail.com



How to Read This Big Picture

Purpose

This document explains how Automotive Functional Safety really works, from hazards to safe vehicle behavior, based on ISO 26262 principles.

1. Mental Model (What & Why)

Start here.

It defines hazards, safety goals, safe states, and timing — independent of AUTOSAR or implementation.

2. FuSa Lifecycle (When)

Follow the 10 steps top-down.

Each step answers one safety question and maps directly to ISO 26262 work products.

3. System Example (How)

The Brake + Steering + ADAS example shows how concepts are applied in real systems. AUTOSAR and non-AUTOSAR architectures realize the same safety intent.

4. GSN (Why believable)

The GSN tree structures the safety argument and supporting evidence on vehicle level.

5. Vocabulary & Roles

Terms and roles are used as defined here to avoid misunderstandings.

What this is NOT

Not a checklist, not a process manual, not a standard replacement.

Key Question to Remember

What is the hazard, what is the safe state, and who enforces it — within the allowed time?

Must-know FuSa Vocabulary

ISO 26262

Automotive functional safety standard addressing risks caused by systematic and random hardware failures in E/E systems.

Safety Item

A vehicle-level function or system under safety consideration, including its interactions and boundaries.

Hazard

A potential source of harm caused by malfunctioning behavior of the item.

Safety Goal (SG)

A top-level safety requirement defined to prevent or mitigate a hazardous event.

Safe State

A system state that eliminates or sufficiently reduces the risk associated with a hazard.

FTTI (Fault Tolerant Time Interval)

Maximum allowed time between fault occurrence and reaching the safe state.

ASIL (Automotive Safety Integrity Level)

A risk classification defining the required rigor of safety measures.

Derived from the risk matrix: S x E x C

S: Severity of harm / E: Exposure probability / C: Controllability by driver

QM (Quality Managed)

Function without unreasonable risk requiring ISO 26262 safety measures.

Functional Safety Concept (FSC)

Technology-independent definition of fault detection and reaction strategies to reach safe states.

Technical Safety Concept (TSC)

Concrete realization of the FSC through architecture, responsibility allocation, and safety mechanisms.

Freedom from Interference (FFI)

Assurance that one element does not adversely affect the safety of another.

ASIL Decomposition

Structured partitioning of a safety requirement into multiple elements with lower ASIL, while preserving safety.

Safety Case

A structured argument, supported by evidence, demonstrating that safety goals are achieved.

Advanced FuSa Vocabulary

GSN (Goal Structuring Notation)

Graphical or textual notation to express safety arguments explicitly.

Item out of Context (IoC)

Development of a safety element without full knowledge of its final vehicle integration.

Confirmation Measures

Independent reviews, audits, and assessments ensuring correctness and completeness of safety activities.

ISO 21448 – SOTIF

Addresses hazards caused by functional insufficiencies or performance limitations, not failures.

ISO 21434 – Cybersecurity

Addresses risks caused by malicious attacks, not accidental failures.

FuSa Roles

Functional Safety Manager (FSM / FuSa Manager)

Owns the functional safety process and ensures ISO 26262 compliance across the lifecycle.

Key resp.: define safety plan / ensure lifecycle completeness / coordinate confirmation measures / interface with assessor

Safety Requirements Engineer

Derives, manages, and traces safety requirements from HARA downstream.

Key resp.: safety goals / functional & technical safety requirements / traceability across lifecycle

Functional Safety Concept Designer (System Level)

Defines the detection and reaction strategies to reach safe states.

Key resp.: safe states / FTTI / FSC definition

Technical Safety Architect (HW / SW)

Realizes the FSC through architecture and responsibility allocation.

Key resp.: TSC / safety mechanisms / ASIL decomposition / freedom from interference

Functional Safety Developer (HW / SW)

Implements safety mechanisms according to the TSC.

Key resp.: watchdogs, monitors, diagnostics / fault reactions / timing guarantees

Base Software / Feature Developer

Implements functional behavior not directly related to safety mechanisms.

Safety Verification Engineer / Tester

Verifies that safety requirements and mechanisms behave as intended.

Key resp.: fault injection / timing verification / requirement-based testing

Safety Case Engineer

Builds and maintains the structured safety argument and evidence mapping.

Key resp.: GSN development / evidence consistency / argument completeness

Functional Safety Auditor

Verifies compliance of processes and work products with ISO 26262. Focus: process adherence

Functional Safety Assessor

Judges whether the safety concept and evidence are sufficient to claim safety.

Focus: safety sufficiency, not checklist compliance; Typically independent