

Arnd Hekermans

Dipl.-Inf. · System & SW Architect · Functional Safety

arnd@hekermans.de +49 (0) 172 78 33 249 www.hekermans.de 73207 Plochingen



System and software architecture for safety-critical embedded systems — from ISO 26262 to ASIL-D, from AUTOSAR to AI-assisted traceability.

In the automotive field since 1998 — in key roles on projects that went into series production. Focus: functional safety (ISO 26262 up to ASIL-D), system and SW architecture, AUTOSAR (Classic & Adaptive) and Automotive SPICE. Since November 2025 an additional focus on AI-assisted engineering tools: deterministic knowledge graphs with local LLMs for traceability, assessment preparation and test generation — auditable, not generative.

EXPERIENCE

in automotive since 1998

SPECIALTY

Functional safety up to ASIL-D

CURRENT FOCUS

AI-assisted safety engineering (since 11/2025)

BASED IN

Plochingen, Germany

01 Core Competencies

Functional Safety (ISO 26262)

From the functional safety concept through the technical safety concept to the safety architecture. Signal and control-flow analyses, freedom from interference, timing protection, partitioning/decomposition and assessment of integrity violations — demonstrated up to ASIL-D, all the way to series release.

System & SW Architecture

Deriving safe architectures from the safety concept, layered and hierarchical, with high cohesion and low coupling. Reverse engineering and documentation of existing systems, load balancing and reuse — end-to-end traceability from system level down to unit design.

AUTOSAR Classic & Adaptive

Deep experience at requirements and implementation level: diagnostics (UDS/DCM), memory services (NVM, FEE, FLS), operating system (OSEK/MICROSAR), Ethernet stack (TCP/IP, SOME/IP, DoIP), flash bootloader, BSW (SecOC, E2E, WdgM) and MCAL on Infineon AURIX.

Automotive SPICE & Process

ASPICE v3/v4 in safety assessments, coaching of projects and definition of processes. Applying the base practices from SYS.2/ SYS.3 and SWE.1 through SWE.6 — including setting up requirements engineering, golden samples and training entire teams.

AI-assisted Engineering

Since 11/2025: deterministic knowledge graphs combined with local LLMs (air-gapped, no cloud). Applications: auditable traceability, ASPICE assessment preparation, test derivation from AST/call graph and SIL validation — the AI proposes, the engine validates deterministically.

Team & Project Leadership

Technical steering and coaching of distributed teams (up to ~30 people), work-package and release planning, supplier management and customer communication — repeatedly took over and restructured running projects through to release.

02 Skills

Functional Safety EXPERT LEVEL

- ISO 26262 (up to ASIL-D, FailSilent & FailOperational)
- Functional & Technical Safety Concept
- Signal/control-flow analysis, critical path
- Freedom from Interference, Timing Protection
- Partitioning & decomposition
- SOTIF (ISO 21448), cybersecurity (ISO 21434)
- FMEA / FMEDA, safety assessments

SW Architecture & Method EXPERT LEVEL

- Safety architecture derived from the TSC
- Design patterns, high cohesion / low coupling
- MBSE: SysML / UML, RFLP approach
- Reverse engineering & architecture documentation
- Load balancing (thread/core), reuse
- Traceability from system to unit design

AUTOSAR & Basic Software EXPERT LEVEL

- Diagnostics (UDS, DCM), DEM fault memory
- Memory services: NVM, FEE, FLS (FEE patent share)
- Operating system (OSEK, MICROSAR), multi-core/-ECU
- Ethernet: TCP/IP, UDP, SOME/IP, DoIP, HTTP
- Flash bootloader (FBL), SIP integration & merge
- BSW: SecOC, E2E, EcuM, CAN, WdgM, RTE/VFB
- Hypervisor (ETAS, HCP4) — integration & debugging

Platforms & Languages

- Infineon AURIX TC4x / TC3x / TC27x / TC29x
- Texas Instruments TDA4x, Qualcomm
- C, C++ (C++14/17, MISRA)
- Python, Rust, TypeScript, Swift
- Build/Test: Bazel, CMake, GoogleTest
- Virtualization: QEMU, crosvm, QNX

AI & Knowledge Graph

- Local LLMs (Qwen) via Ollama / MLX / Metal
- Deterministic knowledge graphs, RAG
- AST/IR analysis (libclang, LLVM)
- Vision/VLM (YOLOv8, image analysis)
- ROS2 (Humble), CARLA / OpenSCENARIO (SIL)
- Air-gapped, on-premise, no cloud

ALM & Tools

- Polarion, Codebeamer, Jama, DOORS (NG)
- Enterprise Architect (Sparx), MagicDraw, Rhapsody
- PreeVision, PlantUML, Confluence, Jira
- Vector DaVinci Configurator/Developer, CANoe, vFlash
- vTestStudio, eSys (BMW), Monaco (Daimler)

03 Project Experience

since 11/2025

Own R&D / sensified

AI-assisted Safety Engineering

current

Knowledge Graph · Local LLMs · Compliance

ROLE

Architect & Developer

CONTRIBUTION

Building a family of tools that connect engineering artifacts (requirements, tests, source code, norms) in a deterministic knowledge graph and enrich them with local LLMs — auditable, reproducible and fully air-gapped. The AI proposes links, the engine validates them deterministically; no LLM runs in the evidence path.

ACTIVITIES

> Deterministic traceability engine (norm clause → requirement → element → test → code)

> Local LLM pipelines (Qwen via Ollama/MLX/Metal), RAG without cloud

> Source-code analysis via libclang AST and LLVM IR (code-to-requirement linking)

> ASPICE v4 assessment workbench (CL2 preparation), gap detection

> SIL validation of safety-relevant AI sensing (CARLA/ROS2, ISO 10218-2)

Result: Deterministic gap reports and traceability in minutes instead of weeks — auditable, not generative.

Knowledge Graph

Qwen / Ollama / MLX

libclang / LLVM

Python

Rust

TypeScript

ROS2 / CARLA

ISO 26262 / 21434 / ASPICE

since 2025 **Joynext** · RTCU – ASPICE Assessment & Test Generation

Client: Stellantis

ASPICE CL2 · SWE.4/SWE.5 · AUTOSAR integration

ROLE

ASPICE / Engineering Consultant & Tool Developer

CONTRIBUTION

Tool-assisted preparation of the ASPICE Capability Level 2 assessment and deterministic generation of SWE.4/SWE.5 test cases from AST and architecture — no LLM in the evidence path. In parallel, SW integration at MCU level.

ACTIVITIES

- › ASPICE v4 assessment preparation (CL2) with an in-house tool (PROVE/SOLVE)
- › Deterministic SWE.4 (unit) / SWE.5 (integration) test-case generation from AST/architecture
- › Integration of ALM sources (Polarion, DOORS NG, Jira) and traceability/coverage reports
- › AUTOSAR integration on AURIX MCU (Vector stack), tooling: CANoe, A2L

ASPICE v4 (CL2)

SWE.4 / SWE.5

AST test generation

Knowledge Graph

Polarion / DOORS NG

Vector AUTOSAR / AURIX

CANoe

since 2025 **BMW** · HIP – Hardware-in-the-Loop / SIL & ASPICE **ASIL-D**

Automated Driving / AAOS · SIL · ASPICE SWE.1–SWE.6

ROLE

SW Architect & Safety / ASPICE Consultant

CONTRIBUTION

Built a SIL/simulation environment and an end-to-end ASPICE implementation (SWE.1–SWE.6) including automatic generation of the Enterprise Architect models and an SWE.6 DoIP server; functional-safety coaching up to ASIL-D in the RFQ context.

ACTIVITIES

- › SIL/simulation environment (QEMU/AAOS/QNX, OpenSCENARIO scenarios)
- › ASPICE SWE.1–SWE.6 implementation incl. test and coverage reports
- › Automatic generation of the Enterprise Architect / MagicDraw models (EA generator)
- › SWE.6 DoIP server for the qualification tests
- › Functional-safety coaching (ISO 26262 up to ASIL-D), interface reviews, test planning

ISO 26262

ASPICE (SWE.1–SWE.6)

SIL / QEMU / AAOS / QNX

OpenSCENARIO

Enterprise Architect / MagicDraw

DoIP

Adaptive AUTOSAR

Python



Driving scenario of the SIL environment — basis for OpenSCENARIO replay and HiL/SiL validation.

2025 NEURA Robotics · OmniSensor – SIL Validation

Cognitive robotics · safety sensing · SIL

ROLE

SIL / Safety Engineer

CONTRIBUTION

Built a software-in-the-loop test system for an AI-based safety sensor (person detection) — deterministic, reproducible validation in a photorealistic factory environment to close the audit evidence gap.

ACTIVITIES

- › SIL test system based on CARLA + ROS2 (Humble)
- › Scenario-based validation of person detection (reaction time, occlusion)
- › Auditable SIL test reports (open instead of black box)

ISO 10218-2

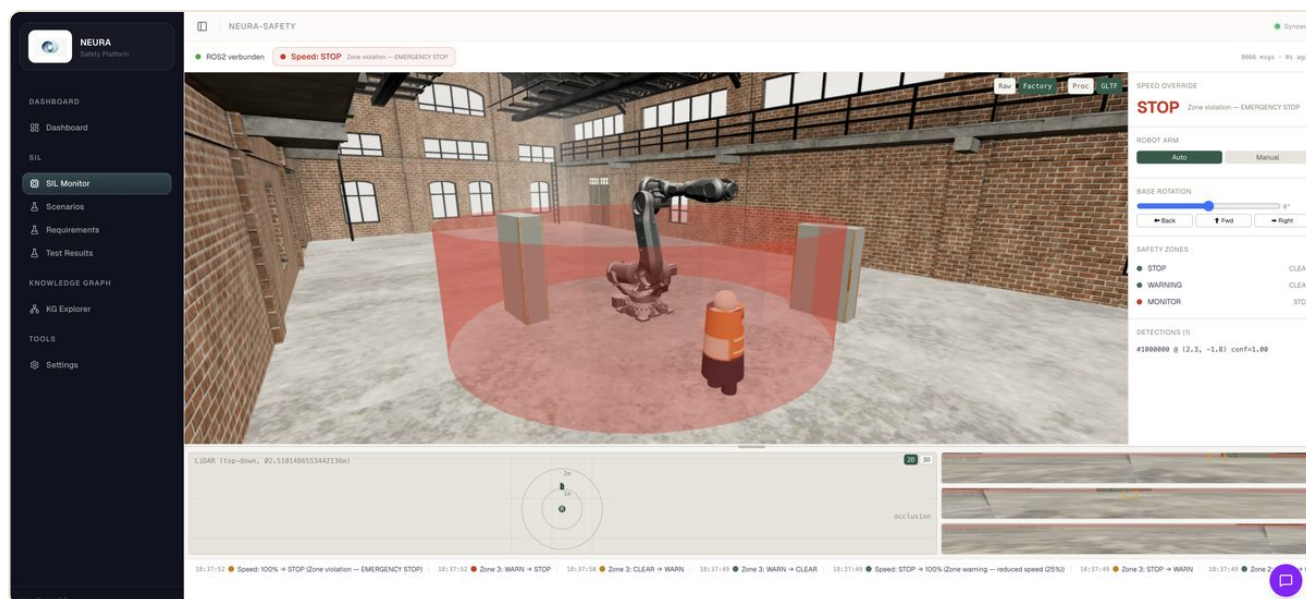
ROS2 (Humble)

CARLA

YOLOv8 / VLM

Python

Knowledge Graph



SIL monitor: safety zones, top-down LiDAR and person detection in a photorealistic factory (CARLA + ROS2).

2025 Brusa · H7 / ICS2P

Power electronics (inverter/charger) – SW-FMEA

ROLE

SW Safety Analyst / Architecture

CONTRIBUTION

Software FMEA and architecture analysis of the power-electronics software based on the EA architecture model.

ACTIVITIES

- › Conducting the SW-FMEA (Loss of Diagnostic / LOD)
- › Analysis of the SW architecture (Enterprise Architect)

SW-FMEA

Enterprise Architect (Sparx)

ISO 26262

2025 **BMW** · PeCU / DC/DC (PenthouseECU)

DC/DC converter – safety & SW requirements

ROLE

Safety / SW Requirements Engineer

CONTRIBUTION

Authoring of SW requirements (system/module level) as well as safety concept and safety analysis for a DC/DC / Penthouse ECU.

ACTIVITIES

- › Definition of SW requirements (system/module)
- › Safety concept and safety analysis
- › Documentation tooling (Markdown/HTML export)

ISO 26262

SW requirements

Safety analysis

2024 – 2025 **BMW** · IP Fahren – Sheer Driving Pleasure **ASIL-D (FailOperational)**

Automated Driving

ROLE

Coaching & Program Management (team ~10 FTE)

CONTRIBUTION

Technical guidance of the project team in ASPICE, SysML/UML and SW architecture, plus responsibility for functional safety (SEooC/Item, system and SW architecture).

ACTIVITIES

- › Analysis of system and SW requirements
- › Review of the technical safety concept
- › Reverse engineering of system and SW architecture from development artifacts
- › Program management of a team of domain experts

ISO 26262

ASPICE

SysML / UML

Codebeamer

MagicDraw

Enterprise Architect

C / C++ / Python

2024 **BMW** · IKS 25 – Interior Camera System **ASIL-B (FailSilent)**

Interior camera / SOTIF

ROLE

System & SW Architect

CONTRIBUTION

Definition of an ASIL-B compliant system and SW architecture for an interior camera system, including SOTIF considerations and coaching on requirements authoring.

ACTIVITIES

- › Definition of the ASIL-B system and SW architecture
- › Review of requirements, architecture and plans (ASPICE)
- › Coaching on requirements authoring at SYS.x / SWE.x
- › SOTIF — definition and requirements

ISO 26262

SOTIF (ISO 21448)

ASPICE

SysML / UML

Enterprise Architect

2024 **Porsche** · BMS 12 V ASIL-C (FailSilent)

Battery management

ROLE

SW Architect & Team Lead (5 architects)

CONTRIBUTION

Support of the SW architecture and definition of the logical program flow for application and BSW on Infineon AURIX TC3xx; process work at the intersection of Agile and ASPICE.

ACTIVITIES

- › Definition of the logical program flow (application & BSW)
- › Technical leadership of 5 architects
- › Architecture and safety work on AURIX TC3xx

ISO 26262

AURIX TC3xx

ASPICE / Agile

Enterprise Architect

2023 – 2024 **BMW** · IP Next – ADAS ASIL-D (FailOperational)

Driver assistance

ROLE

Coaching, Functional Safety & Requirements

CONTRIBUTION

Support of the project team in system/SW architecture and functional safety (SEooC/Item, system engineering), authoring the technical safety concept; reference SW development in Adaptive AUTOSAR.

ACTIVITIES

- › Analysis of system and SW requirements
- › Authoring the technical safety concept
- › Support in ASPICE, SysML, UML and SW architecture
- › Requirements engineering incl. assumptions of use (Codebeamer)

ISO 26262

SOTIF

Adaptive AUTOSAR

C++14 / MISRA

Bazel

GoogleTest

Codebeamer

QNX

2023 **Delta Electronics** · OneBox – On-Board Charger

Charging / power distribution – SW architecture

ROLE

SW Architect

CONTRIBUTION

Conception and documentation of the SW architecture of the OneBox platform (safe compute / safe storage / safe communication) via MBSE.

ACTIVITIES

- › Definition and documentation of the SW architecture (Enterprise Architect)
- › Preparation of features, system structure and system architecture

MBSE

Enterprise Architect (Sparx)

ISO 26262

2023 **Schaeffler** · OneBox – Cybersecurity

Cybersecurity (ISO 21434)

ROLE

Cybersecurity Engineer

CONTRIBUTION

Development of a cybersecurity work-package breakdown in the OneBox context.

ACTIVITIES

- › Definition and structuring of cybersecurity work packages

ISO 21434

Cybersecurity

2023 **Eberspächer** · PFC / 12V BMS – Program Flow Control

Functional safety / timing analysis

ROLE

Safety Analyst

CONTRIBUTION

Analysis of program flow control and timing of the SW architecture (functional-safety context) based on the EA model.

ACTIVITIES

- › Program-flow and timing analysis
- › Architecture analysis (Enterprise Architect)

ISO 26262

Enterprise Architect (Sparx)

Timing analysis

2023 **Valeo** · PDC – Park Distance Control Client: PPE / PPC

ADAS / parking – system architecture & diagnostics

ROLE

System / SW Architect

CONTRIBUTION

Preparation of the system architecture and requirements mapping as well as consideration of self-test diagnostics.

ACTIVITIES

- › System architecture (Enterprise Architect)
- › Requirements mapping (customer/system)
- › Self-test / diagnostics consideration

Enterprise Architect (Sparx)

DOORS

ISO 26262

2023 **Hella** · FHEV – Battery Management System Client: Ford

Battery management safety

ROLE

BMS SW / Safety Architect

CONTRIBUTION

Preparation of the BMS feature and component architecture (ASIL-C/A/QM partitioning) via MBSE.

ACTIVITIES

- › Architecture of the BMS features and components
- › Structuring by ASIL classes (C / A / QM)

ISO 26262

MBSE / PlantUML

AUTOSAR

2024 **Cariad** · Active Safety – MBSE Method

Method / single source of truth

ROLE

MBSE / Method Consultant

CONTRIBUTION

Development of an MBSE method (RFLP approach, ASPICE, single source of truth) for active-safety development.

ACTIVITIES

- › Method for system design and integration (ASPICE)
- › RFLP approach (Requirements–Functional–Logical–Physical)
- › Single-source-of-truth concept (PreeVision / ArchE / Cameo)

ASPICE

MBSE

SysML / UML

PreeVision

Cameo

2021 – 2023 **Continental** · ADC500 – ADAS Platform **ASIL-D (FailSilent)**

ADAS / universal SW platform

ROLE

SW (Safety) Architect & Team Lead

CONTRIBUTION

Conception and definition of the SW architecture for a universal platform that can be used generically across various internal and external application projects.

ACTIVITIES

- › Communication with system stakeholders
- › Analysis of system and SW requirements
- › Authoring of SW requirements and SW architecture
- › Platform evaluation TI TDA4x / J721E (Edge-AI / Linux SDK)

ISO 26262

DOORS NG

Enterprise Architect (SysML/UML)

Rhapsody

PTC Integrity

Adaptive AUTOSAR

QNX

TI TDA4x / J721E

C / C++

2020 – 2021 **Daimler / Mercedes-Benz** · BEA-II / BEA-III – Battery Management **ASIL-C (FailSilent)**

Battery management safety

ROLE

SW (Safety) Architect & Team Lead

CONTRIBUTION

Conception and definition of the safety SW architecture of a battery management system through to series readiness of several HW variants, plus the concept for upgrading from ASIL-B to ASIL-C.

ACTIVITIES

- › Analysis of system and SW requirements
- › Definition of SW safety mechanisms
- › Identification of gaps in system requirements
- › Authoring the technical safety concept (ASIL-B → ASIL-C)

Result: EQS variant produced in series.

ISO 26262

DOORS

Enterprise Architect (UML)

2018 – 2020 **BMW** · iBMU – Battery Management Unit Client: PIDEU ASIL-C (FailSilent)

Battery management safety

ROLE

SW Safety Architect (team ~20)

CONTRIBUTION

Took over a running project from the predecessor supplier with incomplete documentation. Rebuilt the process landscape per ISO 26262, set up requirements engineering and the safety architecture. Identified and resolved several potential show-stoppers.

ACTIVITIES

- › Technical steering of a team of 4 architects
- › Definition of the safety architecture and level-3 safety monitors
- › Signal-flow analyses incl. golden sample, timing protection, FFI
- › Provision of ASIL-C for Infineon MCAL
- › Definition & rollout of all ISO 26262 work products, team training

Result: Level-3 and level-4 release for the production start (G08) achieved successfully.

ISO 26262 Enterprise Architect (UML) AURIX / Infineon MCAL Jira / Jama / Confluence CANoe
DaVinci Configurator / Developer

2019 – 2020 **Daimler / Mercedes-Benz** · HV DC/DC Converter Client: PIDEU ASIL-C (FailSilent)

Battery management safety

ROLE

SW (Safety) Architect & Team Lead

CONTRIBUTION

Upgrading the ASIL level from B to C: defining the approach, identifying all affected SW components based on requirements and signal-flow analyses, and implementing the necessary changes.

ACTIVITIES

- › Definition of the safety architecture and level-3 safety monitors
- › Timing protection, program-flow/alive/deadline supervision, FFI
- › Partitioning of OS applications, ASIL-C for Infineon MCAL
- › SW integration tests (vTestStudio), SWE.4/SWE.5 documentation
- › Reworking the OS scheduling (non-preemptive → preemptive), load balancing

Result: Release successfully delivered to the client and deployed at the customer.

ISO 26262 Enterprise Architect (UML) AURIX / Infineon MCAL CANoe DaVinci Configurator / Developer
vTestStudio

2018 Audi · HCP4 / ELVIS – Flash Bootloader

Client: Bosch

Hypervisor & bootloader integration

ROLE

SW Integrator

CONTRIBUTION

Commissioning an Ethernet flash bootloader (Vector SIP) from a non-functional baseline: fault analysis and fixes in the TCP/IP stack, diagnostics and the hypervisor; adapting the flash process to the hypervisor architecture.

ACTIVITIES

- › Commissioning & debugging of the ETAS hypervisor
- › Configuration of the bootloader modules (DaVinci Configurator)
- › Implementation of FBL APIs, FBL updater, DID handling
- › SBC/SPI and external watchdog, integration with the application

Result: On-time delivery to Audi, very well received in the presentation; follow-up project ELVIS commissioned successfully on new hardware.

Vector vFlash

Tasking Compiler

DaVinci Configurator

Bosch AE / RTE Configurator

Enterprise Architect

DOORS

2016 – 2017 Volkswagen · EPS Crafter – Steering

Client: Bosch

ISO 26262 (Level 3)

Technical safety concept / safety architecture

ROLE

SW (Safety) Architect & Team Lead (7 developers)

CONTRIBUTION

Took over the project from the predecessor supplier with incomplete documentation. Defined processes for requirements, implementation and test; documented the code base via reverse engineering and qualified it through signal/control-flow analysis.

ACTIVITIES

- › Definition of the approach, training and execution
- › Definition of the safety architecture and safety monitors
- › Assessment of integrity violations
- › Coordination of a team of 7 developers (requirements, FuSa, test, diagnostics)

Result: Level-3 release per ISO 26262 achieved in a safety assessment; system deployed in the MQB platform.

ISO 26262

AUTOSAR

RTE / OSEK

DOORS

Enterprise Architect

ClearCase / ClearQuest

2015 Audi · zFAS – central driver assistance

Client: Valeo

ASIL-B

Technical safety concept / safety architecture

ROLE

SW Safety Architect

CONTRIBUTION

Authoring the technical safety concept together with the functional safety manager: analysis of system interrelations, assessment against safety criteria and building the safety architecture.

ACTIVITIES

- › Authoring and analysis of the safety architecture per ISO 26262

ISO 26262

AUTOSAR

RTE / OSEK

DOORS

Enterprise Architect

2014 – 2015 Toyota / VW · Park4You – Parking Assistance

Client: Valeo

ASIL-B

Driver assistance

ROLE

Team Lead & SW Safety Architect

CONTRIBUTION

Authoring the SW architecture per ISO 26262 (ASIL-B), assessing and resolving integrity violations, customer communication and ensuring product availability; ensuring series readiness in the VW context.

ACTIVITIES

- › Coaching and coordination of a team of 6 developers
- › Integration of the Toyota CAN stack, E2E protection, watchdog integration
- › Resource planning, ticket assessment and customer communication

Result: Product deployed successfully in platforms 560A, 488B, 795A as well as MQB / MLB-Evo B.

ISO 26262

AUTOSAR

RTE / OSEK

CANoe

DOORS

MISRA / QAC

Flexray / CAN

2010 – 2017 Daimler / Mercedes-Benz · Parkman / Scala 2 – Parking & Laser Scanner

Client: Valeo

Driver assistance / AUTOSAR integration

ROLE

Lead Integrator, SW Architect & Sub-project Lead

CONTRIBUTION

Ensured series readiness for Parkman as lead integrator and architect; later sub-project lead of the AUTOSAR V4 integration (Scala 2) for an internationally distributed team of ~30 developers and product release management.

ACTIVITIES

- › Definition and implementation of the SW architecture, bug-fixing around load issues
- › Review/rework of requirements and SW components
- › Supplier steering, release planning and documentation
- › Integration of SIPs, K-matrices, diagnostic updates and security topics

Result: Several releases delivered successfully to Daimler; systems deployed in platforms BR222, BR212, BR213.

ISO 26262

AUTOSAR

RTE / OSEK

CANoe

DOORS

MISRA / QAC

Flexray / CAN

2006 – 2010 Daimler / VW / Bentley · Instrument Cluster & Head-up Display

Client: Bosch

Display & HMI systems

ROLE

Architect, Designer & Developer

CONTRIBUTION

Concept, architecture and implementation of a data-driven menu description language as an AUTOSAR component to minimize the effort for changes and extensions; used worldwide to implement customer requirements.

ACTIVITIES

- › Conception, architecture and implementation of the system
- › Definition of the tool landscape and process chain
- › Windows tool to manage and generate embedded resources
- › Application modules: ACC, lane departure warning, diagnostics, head-up display simulation

Result: Daimler KIG1 successfully went into series production (sports line).

C / C++

AUTOSAR

RTE / OSEK

CANoe

ClearCase

DOORS

MISRA / QAC

MFC / Win32

For confidentiality reasons no project-internal details (people, confidential specifics) are disclosed. End customers and project codenames are stated where permitted.