How to build fail-operational systems for autonomous driving
Key learning objectives

Highly automated driving use cases require high levels of technological autonomy and rely on the heavy data-traffic from the perception layer. Learn how to conquer the resulting complexity and safety challenges.

Learn about the opportunities offered by the centralized, software-defined safety platform that ensures the safe execution of tasks and reliable communication with real-time guarantees in a highly heterogenous environment.

How to build a fail-operational system derived from principles found in the aerospace and space industry and to tailor it to automotive use cases in a cost-efficient manner.

How to propose an architectural design for an AD platform that fulfills the highest safety requirements according to the ISO 26262 standard, while proactively tackling the possible weak links.
The automotive industry is evolving at high speed

<table>
<thead>
<tr>
<th>Change #1</th>
<th>Change #2</th>
<th>Change #3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>From one-function appliances to a software platform</strong></td>
<td><strong>Sourcing best-in-class solution elements</strong></td>
<td><strong>Faster innovation cycles</strong></td>
</tr>
<tr>
<td>Move away from one-function hardware appliances to a software-defined architecture</td>
<td>Brings freedom to OEMs or Tier1s to select the best-in-class solution elements</td>
<td>With the decoupling of application software from hardware, faster innovation cycles are enabled</td>
</tr>
<tr>
<td>Highly modular, converged, centralized, service-oriented platform is needed</td>
<td>High transparency is achieved, as opposed to the old approach with sourcing a complete closed-box system</td>
<td>Serving as a competitive advantage</td>
</tr>
<tr>
<td>Built on generic high-performance computing hardware enabling software function re-use</td>
<td>Maximizes solution efficiency and value</td>
<td></td>
</tr>
</tbody>
</table>

Software functions serving as a differentiator for OEM's car brands
The automotive industry is evolving at high speed

**YESTERDAY & TODAY**

- **Distributed E/E architecture**
  - 1 ECU: 1 function

**2020 – 2025**

- **Domain E/E architecture**
  - 5-7 ECUs: n functions grouped by functional domains

**2025 +**

- **Centralized E/E architecture**
  - 2 ECUs: n functions

Service-oriented architecture with real time guarantees
The journey continues towards conquering the highly automated driving use cases

Designing a sound safety approach is one of the most critical challenges in AD

Fail-operational capabilities need to be brought to the core of the design principles in order to reach HAD
Highly automated driving use cases create tremendous complexity

Diverse input from sensors (radars, cameras, LIDARs) are processed to identify elementary pieces of information about the vehicle surroundings.

This information then travels through the sensor pre-processing and the perception layer and is fed into a central fusion layer to compile a complete and consistent representation of the surrounding of the car and the trajectories of all objects in real-time.

High definition maps and a cloud connection to further expand the perception of the surroundings is required as well.

The clusters of applications from path planning, controlling and actuation are delivering the driving strategy, implementing the navigation and are controlling steering, braking and the drive train.
Challenges brought on by perception layer

There is no “one-size-fits-all” approach to the perception layer for autonomous cars.

Sensor fusion is essential in adverse weather conditions, delivering different information (blizzards, snow, fog, rain).

The fusion of all sensor data into one stream eliminate blind spots or inaccuracies of one sensor output.
Opportunities brought on by the new architecture approach
Seamless roadmap to full automation in the future

Achieve cost predictability

Manage development & deployment risks

OPPORTUNITIES

Boost return on investments

Accelerate time-to-market
Boost return on investments

- With a platform-centric approach, software components can be re-used in future highly automated driving projects

- Re-use possible across multiple SoCs, vehicles, models and lines, making the most out of your investment
Seamless roadmap to full automation in the future

- A well-structured software architecture enables scaling from L2 to L5
- A scalable software platform enables the re-use of software and contributes to emerging functionality in the future
Achieve cost predictability

- The platform approach enables customers to focus on the application development building upon a stable, state-of-the-art platform
- OEMs can base their cost calculation on a predictable licensing model
Customers can take complexity out of their development projects, when basing them on a stable software platform.

Safety and real-time requirements are covered by the software platform which reduces program risks through a controlled integration process.
Accelerate time-to-market

- Adopting a series-proven, platform-centric approach speeds up time to market
- Versatility and scalability of a platform-centric approach allows fast adaption to different hardware platforms, supports application software re-use and reduces validation and testing efforts
Seamless roadmap to full automation in the future

Achieve cost predictability

Manage development & deployment risks

Boost return on investments

Accelerate time-to-market
Challenges brought on by the industry evolution
### Challenges for the automotive industry

<table>
<thead>
<tr>
<th>Time-to-market</th>
<th>Safety</th>
<th>Fail-operational requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-time processing</td>
<td>Applications of different criticality levels need to be hosted safely and executed with a sufficient level of independence. Manual integration of apps cannot ensure that all essential safety-related tasks running on different SoCs are scheduled appropriately. This can negatively impact the ability of the system to react in real-time to ensure vehicle and driver safety.</td>
<td>Level 3+ automated driving systems require a fail-operational architecture design. The E/E system must continue operation under all circumstances - even in the presence of a fault. System redundancy with the highest possible availability of services is required. Balance needed between aerospace full-redundancy and automotive cost restrictions.</td>
</tr>
<tr>
<td>Scalability &amp; versatility</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guarantee of service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>High complexity</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Levels of automation classification by SAE

### Fail-silent (driver is the fallback)

<table>
<thead>
<tr>
<th>DRIVER ONLY</th>
<th>ASSISTED</th>
<th>PARTIAL AUTOMATION</th>
<th>CONDITIONAL AUTOMATION</th>
<th>HIGH AUTOMATION</th>
<th>FULL AUTOMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Driver continues to perform the longitudinal and lateral dynamic driving task.</td>
<td>Driver continuously performs the longitudinal or lateral dynamic driving task.</td>
<td>Driver must monitor the system at all times.</td>
<td>Driver does not need to monitor the system at all times. Driver must be capable of resuming dynamic driving task.</td>
<td>Driver is not required during defined use case*.</td>
<td>No driver required during entire journey.</td>
</tr>
<tr>
<td>No intervening vehicle system active</td>
<td>The other driving task is performed by the system.</td>
<td>System performs longitudinal and lateral driving task in a defined use case*.</td>
<td>System performs longitudinal and lateral driving task in all situations in a defined use case*.</td>
<td>System performs the entire dynamic driving task on all road types, speed ranges and environmental conditions.</td>
<td></td>
</tr>
</tbody>
</table>

### Fail-operational requirements

- **Level 0**: Driver continuously performs the longitudinal and lateral dynamic driving task.
- **Level 1**: Driver continuously performs the longitudinal or lateral dynamic driving task.
- **Level 2**: Driver must monitor the system at all times.
- **Level 3**: Driver does not need to monitor the system at all times. Driver must be capable of resuming dynamic driving task.
- **Level 4**: Driver is not required during defined use case*.
- **Level 5**: No driver required during entire journey.

*Use cases refer to road types, speed ranges and environmental conditions.*
# System architectures vs. levels of automation

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control</strong></td>
<td>Driver</td>
<td>Vehicle</td>
<td>Vehicle</td>
<td>Vehicle</td>
<td>Vehicle</td>
</tr>
<tr>
<td><strong>Monitoring</strong></td>
<td>Driver</td>
<td>Driver</td>
<td>Driver (after take-over time)</td>
<td>Vehicle</td>
<td>Vehicle</td>
</tr>
<tr>
<td><strong>Fallback</strong></td>
<td>Driver</td>
<td>Driver</td>
<td>Driver (after take-over time)</td>
<td>Vehicle (in defined use case)</td>
<td>Vehicle</td>
</tr>
</tbody>
</table>

### Fail-silent system designs

- Assumed system layouts and ASILs

### Fail-operational system designs

- Redundancy management is a complex task. System availability becomes a safety property.
The fail-operational requirement

<table>
<thead>
<tr>
<th>Level 3</th>
<th>System detects its limits and asks driver to take over in case of faults</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 4</td>
<td>System can handle all situations automatically in the specific application case</td>
</tr>
</tbody>
</table>

**Even in the case of component failures:**
- Continue operation and request driver to take over (~10s in Level 3 systems)
- If driver does not take over, then situation specific reaction e.g. controlled stop

| Change lanes and stop the car at safe position | Stop the car in lane (avoiding obstacles) |

| Level 5 | System has to continue driving until planned travel end point |
Currently, there is no accepted safety assurance approach for AI based on deep neural networks.

Availability becomes a safety property.

Redundant elements need to satisfy sufficient independence requirements.

New mindset needed for ASIL D + fail-operational instead of ASIL D via strict monitoring functions (only leading to shut-off).

Vehicle E/E architecture needs to consider common cause faults (e.g. power loss) which used to be acceptable - while relying on mechanical fallback.

Fail-operational architecture solutions required for L3, L4, L5.
Fail-operational requirements for L3+ automated driving

Minimum system safety reaction: stop in a safe area or let driver take over – requires > 10 seconds of intelligent and controlled operation (360 meters at highway speed!)

- Redundancy (active / fallback) to cope with HW and SW failures
- Make sensor set available to active system and fallback system
- Provide sufficient computation power also on fallback system
- Simultaneous failure of active and fallback must be prevented
Autonomous operation requires fail-operational systems

20+ years of excellence in designing, building and assuring fail-operational systems across safety-critical industries

Fail-silent

Off-highway
IEC 61508

Industrial
EN/ISO 13849

Automotive
ISO 26262

Aerospace
DO 178C / 254

Fail-operational
Solutions that are fit-for-purpose
Platform-centric approach brings fit-for-purpose solutions

<table>
<thead>
<tr>
<th>Challenges</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>High complexity</td>
<td>Open integration platform</td>
</tr>
<tr>
<td>Scalability</td>
<td>Modular platform architecture</td>
</tr>
<tr>
<td>Real-time processing</td>
<td>Real-time orchestration of applications</td>
</tr>
<tr>
<td>Open collaboration models</td>
<td>Safety by design</td>
</tr>
<tr>
<td>Software integration</td>
<td></td>
</tr>
</tbody>
</table>
Fit-for-purpose solution #1

Real-time orchestration of applications

- Deterministic behavior ensuring always available services with guaranteed latency
- Time-aware platform architecture
- Innovative global scheduling technologies for applications and communications
- End-to-end real-time guarantees across a highly heterogenous environment
- Real-time processing with deterministic scheduling of computation chains
- Achieve predictability of the resource consumption, runtime, data flow latencies and application task sequences
Fit-for-purpose solution #1

Real-time orchestration of applications

Global scheduling
(Applications and Networking)

End to end real-time guarantees

Deterministic behavior

FUNCTION 1

FUNCTION 2

SCHEDULING
FUNCTION 1

FUNCTION 2

COMMUNICATION BACKBONE

SAFETY SOFTWARE PLATFORM

IN

OUT

IN

OUT

Perf. host 1

Perf. hosts

Perf. hosts

Safety host
Seamlessly integrate, test and validate applications from third party providers

Platform-wide integrated automotive, development and support services

AUTOSAR classic & adaptive compliant APIs

Scalable architecture to support L2 – L5 ADAS/AD systems

Uniform APIs ensure portability of applications

Create Digital Twins and PC-based co-simulation with the Software-in-the-Loop feature
Fit-for-purpose solution #2

Open & modular integration platform

Harmonization layer:
- Open standardized APIs
- Globally available services
- Behavioral aspects: Execution and communication
Harmonization layer:
- Open standardized APIs
- Globally available services
- Behavioral aspects: Execution and communication

This type of architecture is supporting fault containment regions for the fail operational system design.
Fit-for-purpose solution #3

Safety by design

- Freedom from interference by encapsulating applications
- Introduce fail-operational capabilities by supporting redundant configuration
- Monitoring of safety related components
- ASIL D safety compliance according to ISO 26262
- Manage data traffic with different levels of criticality
- Error handling up to ASIL D
Fit-for-purpose solution #3
Safety by design

Safe execution platform enables mixed-criticality of software

Freedom from interference

Timing | Communication | Memory

ASIL: D D QM B QM B B B QM

SAFETY SOFTWARE PLATFORM

SAFETY HOST

Perf. host 1

Perf. hosts

Perf. host n

COMMUNICATION BACKBONE

SAFETY BY DESIGN
Unleash benefits with MotionWise safety software platform
MotionWise: safety software platform

- Efficient global scheduling and integration of applications
- Deploy and re-use applications across multiple vehicle models – both in single or multiple SoC environments
- Highly modular, scalable platform
- Integrate, orchestrate and validate software components from multiple suppliers
- ASIL D safety compliance
- Manage complexity of a highly heterogenous HW architecture
A reference automated driving system architecture

Centrally ECU

**Sensors**
- EGO
- HD map
- Cameras
- Radars
- LIDARs
- Ultrasonics

**Interfaces**
- CAN
- ETH
- LIN
- FR
- LVDS

**Data fusion**
- Object fusion
- Localization
- Road graph
- Grid fusion

**Path planning**
- Prediction
- Behavior
- Trajectory

**Control**
- HMI
- Motion control

**Actuators**
- Powertrain
- Brake
- Steering
- Cluster

**Communication Backbone**
AUTOSAR approach towards designing ECU architecture

- Project specific safety and services concepts
- Loads applications with glue code and adaptations
- Applications use different APIs on different hosts
- No real-time guarantees

Every host acts as an isolated "island", without global scheduling and synchronization capabilities.
OEM's specific extensions towards designing ECU architecture

- OEM specific adaption layer on performance host(s)
- Different APIs and glue code on safety host
- No real-time guarantees

![Diagram showing OEM's specific extensions](image-url)
Platform-centric approach towards designing ECU architecture

- Integrated communication and services layer
- Same APIs on all hosts
- Integrated safety and synchronization concept
- Real-time guarantees

MotionWise
Safety software-defined platform
delivering safety services, synchronization and real-time guarantees

- AUTOSAR Classic
- MCAL
- Safety Host
- RTE interface

- AUTOSAR Adaptive
- RTOS / BSP
- Performance Host
- ARA interface

Avoid siloed architecture and achieve end-to-end real-time guarantees.
MotionWise safety software platform

**MotionWise**

**Real-time orchestration**
- Time aware architecture
- Data synchronization layer
- Global scheduling

**Safety by design**
- Freedom from interference
- Error and health management
- Fail-operational requirements

**Open integration platform**
- Unified APIs
- Heterogeneous SoCs
- Platform services & tools

**Deterministic Ethernet**

**Processing**

**ACTUATORS**

**SENSORS**
MotionWise

HPC
High Performance Compute
HPC
High Performance Compute

Safety host
Performance host
Performance host

Deterministic Ethernet
PCle
MotionWise

HPC
High Performance Compute
MotionWise Core Services

Extensions

Scheduling services

Communication services

Time synchronisation services

Safety & health services

Tool suite

Core

HPC
High Performance Compute
MotionWise

Extensions

Core

Tool suite

HPC
High Performance Compute
MotionWise Tool suite

HPC
High Performance Compute

App
Core
MotionWise Creator

App
MotionWise SDK

App
Extensions
SIL Environment
How to introduce fail-operational capabilities to your AD system
Fail-operational mandates active redundancy

* with no redundancy

Not acceptable!
Redundancy management is not trivial

Both automated driving functions operate correctly. Both outputs have correct results. The 2 results are not identical. The vehicle cannot distinguish between:

- 2 correct, but different results
- 1 correct and 1 faulty result
Abstract fail-operational layout for autonomous driving

**Sensors**
- Diverse and redundant setup: Cameras + Lidars + Radars
- Main driving algorithms:
  - ASIL D / fail-silent: switches to silent state in case of internal failure
  - BACKUP implementation of driving algorithms:
    - Lower ASIL admissible (when used for limited time duration)

**ACTIVE**
- ASIL D Fail-silent

**FALLBACK**
- ASIL B

**Actuators**
- ACTIVE and FALLBACK may output different trajectories: all actuators need to consistently select the same input
- Select “1st valid“:
  - Take input from ACTIVE if available, otherwise take input from FALLBACK
Achieving ASIL D by ASIL decomposition

Symmetric approach

- 2 similar driving algorithms running side by side
- Compare outputs (trajectories)
- Switch off, if trajectories do not match

Showstopper

Even correct trajectories are not necessarily identical

Asymmetric approach with Safety Co-Pilot

- ACTIVE / Checker configuration
- Checks if trajectory is in safe driving area to avoid collisions
- Lower performance requirements and simpler algorithms than ACTIVE, easier to reach ASIL C
  - Allows ACTIVE algorithms with ASIL A
  - Enables agile function development for ACTIVE
  - ACTIVE may implement AI-based algorithms, while Safety Co-Pilot implements a more conservative approach
Fail-operational architecture

- Primary Node = ACTIVE + Checker
- Fallback Node
- Redundant power supplies
- Redundant communication networks
- Redundant sensors
- Redundant actuators
- Decision Maker + High Availability
  Communication support the redundancy
- Primary ADS is always checked

If a fault in the Primary ADS is detected → system silences Primary Node and switches to Fallback Node
MotionWise safety software platform and Safety Co-Pilot

Delivering an end-to-end safety approach in highly automated driving

Correct behavior of the active channel is achieved by checking the output of the primary automated driving system, using an independent checker called Safety Co-Pilot.
Seamless roadmap to full automation in the future with MotionWise and In-Car-Compute Platform
In-Car-Compute Platform within the E/E architecture

Deterministic Ethernet TSN / CAN

ECU's as smart I/O's

High-speed dual redundant backbone link

External communication

Internal communication
MotionWise and Safety Co-Pilot supporting fail-operational by design

Benefit #1
Multiple safety mechanisms with configuration options for suitable system reaction (different for primary node and fallback node)
Sophisticated redundancy management

Benefit #2
MotionWise developed for compliance to ISO 26262 ASIL D
Supports ASIL decomposition of applications, especially:
ASIL D = ASIL B(D) + ASIL B(D)

Benefit #3
Supports deterministic design based on time-triggered architecture
Provides composability
Provides stability and high availability
Provides observability (for high quality of testing)
Why partner with TTTech Auto for your automated driving projects?
T T T Tech Auto safety and robustness in production powered by MotionWise

First series-proven level 3 platform on the market to enable:

Parking pilot
Traffic jam pilot
Your partner for autonomous driving projects

**AD production program experience**
We have the first series-proven level 3 solution on the market. We have productized the key-principles into MotionWise safety software platform

**Automotive safety expert at your side**
Ensure the highest safety-criticality and performance of your solutions by partnering with an automotive safety-specialized expert

**Customer proximity**
We are working alongside our customers, we understand their technology needs, as well as regulatory specifics set by each country that they operate in

**Cross-industry experience**
20+ years of experience with highly innovative deterministic and disruptive technologies in aerospace and space industries

**Unparalleled system integration skills**
20+ years of experience with SI to implement innovative approaches in minimizing workloads, empowering customers to automate those efforts and easily integrate the apps themselves

**Vendor independence**
Whether HW, applications, or complete systems, our vendor-agnostic approach keeps you away from vendor lock-in, ensures flexibility and openness of your solutions with best-in-class elements
Key take-aways

How to build a future-ready driverless system
MotionWise helps organizations move away from a slow, costly, complex and iterative integration process to a platform approach.

This speeds up time-to-market for new functionalities, guarantees safety, and allows software investments to be reused for highly automated driving projects.

Resulting in a seamless roadmap to full automation in the future.

Paired with our Safety Co-Pilot, MotionWise delivers an end-to-end safety approach.

MotionWise is capable of evolving all the way to a software-defined In-Car Compute Platform in the future.

Accelerate your journey towards highly automated driving with MotionWise safety software platform and Safety Co-Pilot.