Are you an OEM and you need to define a new fault-tolerant communication concept and architecture for L3/L4/L5 systems?

Are you switching to zonal architectures?

Are you switching to Ethernet?

Are you using high-performance platforms and intelligent gateways?

Are you having an interconnected vehicle, with V2x?

Do you want to simplify your system to use less of different network protocols and stacks?

DE0212 Safety communication in fail-safe and fail-operational systems up to SAE Level 5

Standards like ISO 26262 provide some guidance on communication protection. Detection of communication errors is a very basic knowledge that is state-of-the-art in automotive.

However, in advent of fault-tolerant systems required for L3/L4/L5 systems, the communication network does not only need to detect errors (and go to safe state), but most importantly it needs to be tolerant against failures of elements and ensure that even in case of a failure of one link, node or SoC, the automated vehicle functions (environment perception, route determination and lateral/longitudinal control) can still operate.

General approach:

The *exida* approach is to describe both fail-safe and fault-tolerant safety concepts. It starts top-down, relation of communication to item definition, HARA, safety goals, then it provides a system and software safety concepts for communication.

www.exida.eu

DE0212 Safety communication in fail-safe and fail-operational systems up to SAE Level 5

Who should attend?

- System Safety Engineers
- Software Safety Engineers
- Software Safety Architects
- Product Owners
- Software Developers

Duration:	8 hours split as two 4-hours sessions
Language:	English
Location:	online
Certificate:	Each participant gets a letter of attendance.

For more information, please contact:
Kerstin Tietel
+49 89 44118232
kerstin.tietel@exida.com

DE0212 Safety communication in fail-safe and fail-operational systems up to SAE Level 5

Agenda and Content

- Item Definition
  - Description of how fail-safe communication and fault-tolerant communication is needed by various item functions in a vehicle
- HARA and Safety goals
  - Summary/classification safety goals in view of their impact on safe communication
- Introduction to safe communication
  - Failure modes, fault definitions, safety protocols
  - Network layers, network stacks, E2E protection
  - Recommended E2E profiles
- Elements of a safe protocol:
  - Ingredients/mechanisms of each safety protocol, what is sufficient
- Configuration of communication
- Recommendation for new projects:
  - Recommended topologies, architectures, E2E protection profiles
- Communication and functional safety concept
- Communication and technical safety concept
- Communication and SW safety concept / SW architecture