Functional Safety Architectural Challenges for Autonomous Drive

Ritesh Tyagi: August 2018
Topics

- Market Forces
- Functional Safety Overview
- Deeper Look
- Fail-Safe vs Fail-Operational
- Architectural Considerations
- Challenges
Megatrends shaping the automotive market

Automated Driving
- Enabling safety towards Vision Zero

eMobility
- Enabling CO₂ reduction

Connectivity
- Enabling the communication of cars

Advanced Security
- Enabling security in connected cars

Copyright © Infineon Technologies AG 2018. All rights reserved.
Socio-Economic Pressure

**Safet**
- 94% of U.S. crashes involve human error. [1]
- 1.2 million deaths worldwide due to vehicular crashes in 2018. [1]
- 37.461 road deaths in the U.S. in 2016 and 2.4 million injuries in 2015. [1]
- 2 out of 3 people will be involved in a drunk driving crash in their lifetime. [1]

**Society**
- $594 billion in harm from loss of life and injury each year. [1]
- $277 billion in annual economic costs. [1]
- $160 billion in gas burned and time lost each year. [1]

**Mobility and Quality of Life**
- 3 million Americans age 40 and older are blind or have low vision. [1]
- 79% of seniors age 65 and older living in car-dependent communities. [1]
- 42 hours wasted in traffic each year per person. [1]

Source: Waymo Safety Report
AD deployment can happen much earlier than we think

Miles accumulated by roadway vs a simulated virtual environment

Google's IRL self-driving cars
5 Million Miles traveled
Operated on public roads from inception to Feb 2018

Waymo
8 Million Miles traveled per day!
2.7 Billion virtual miles in 2017

What is Functional Safety (FuSa)
Does This Look Safe?

› Does redundancy help here?

› What could go wrong?
What is Functional Safety?

Example of railroad crossing – How much is the probability of collision?

Root causes of danger are completely removed.

By adding functional measures, acceptable level of safety is ensured.

Assessment of the "functional measures" (safety functions) and its numerical evaluation is the basis of Functional Safety.
Safety Concept: Holistic Approach

- **Functional Safety**
  - **ZERO** accidents by system failures
  - (ISO 26262)

- **Vehicle Safety**
  - **ZERO** accidents by human error
  - (ADAS & Safety of the intended functionality)

- **Device Reliability**
  - **ZERO** components failure
  - (Robust products)

- **Security**
  - **ZERO** accidents by systems hacks
  - (End-to-end Security)

Copyright © Infineon Technologies AG 2018. All rights reserved.
Functional Safety: Deeper Look
Vocabulary

**Item**
A system or array of systems which implements a safety related function e.g. steering, braking, transmission to which ISO26262 is applied

**System**
Consists of elements (sub-systems, components, HW, SW) and relates a sensor, controller and actuator with each other

**Component**
A none system level element which consists of more than one HW part or more than one SW unit

**Hardware (HW) Part**
Hardware which cannot be sub-divided

**Software (SW) Unit**
Atomic level of the SW architecture which can be tested as a standalone part of the SW
Functional Safety Standard: ISO 26262 Origin

Functional Safety Standards (based on IEC 61508)

- **IEC 61508**
  - Functional safety of electrical / electronic / programmable electronic safety-related systems

- **ISO 26262**
  - Functional safety in Automotive Electronics

- **IEC 60601-1**
  - Medical electrical equipment General requirements for basic safety and essential performance

- **EN 5012x / EN50129**
  - Rail Transport

- **IEC 60880-2**
  - Nuclear Power

- **Increased complexity of automotive systems**
  - Higher number of incidents due to system faults

- **Partial adaptation of IEC 61508 to automotive industry**

- **ISO 26262**
  - Introduction focused on possible hazards caused by malfunction of E/E safety related systems
## ISO26262 Coverage

<table>
<thead>
<tr>
<th>ISO 26262 <strong>DOES</strong> address</th>
<th>ISO 26262 <strong>DOES NOT</strong> address</th>
</tr>
</thead>
<tbody>
<tr>
<td>• E/E systems in mass production vehicles</td>
<td>• Hazards due to other factors (e.g.: smoke, fire), or technologies (unless directly caused by malfunctioning behavior of the E/E system)</td>
</tr>
<tr>
<td>• Possible hazards caused by malfunctioning E/E systems</td>
<td>• Performance of the E/E Systems</td>
</tr>
<tr>
<td></td>
<td>• Special purpose vehicles designed for drivers with disabilities</td>
</tr>
</tbody>
</table>

Copyright © Infineon Technologies AG 2018. All rights reserved.
Types of failures

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Process related</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.g.: Bugs in specifications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>– Product, test &amp; verification specification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software related</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.g.: Programming error at loop termination condition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>– Unwanted endless loop (leads to Watchdog-Reset)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware related</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.g.: Reuse of weak concepts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>– Insufficient EMC Immunity due to new environmental conditions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Random HW Failures</th>
<th>ISO Part 4</th>
<th>ISO Part 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware related</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.g.: Aging or Oxidation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>– Loss of contact or short circuit</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ISO 26262 Process Overview

- International standard for Road Vehicle Functional Safety providing the **management and process requirements** for the
  - Development
  - Production
  - Operation, maintenance and
  - Decommissioning
  of E/E Systems and components

- Approximately 500 pages long and very explicit
  - Over 1000 requirements defining what to do
  - Over 50 tables defining how to do it
  - Over 130 documents / files needed to show compliance

- Origin is the IEC61508 (Functional safety of electrical / electronic / programmable electronic safety-related systems)
- Process based on the V model
- Applicable to all products involved in Safety related systems
- Process requirements vary according to the ASIL.
Automotive Safety Integrity Levels (ASILs) Concept

- At the top-level, Safety goals are defined through the process of hazard analysis and risk assessment (HARA).
- Safety goals are written in terms of avoiding harm during some vehicle operational condition, with a corresponding Automotive Safety Integrity Level (ASIL).
- ASIL applies to individual safety goal, not overall system!
- ASIL defines the required degree of rigor in technical, organizational, and process activities.
- There are 5 ASIL levels QM, A, B, C & D.

<table>
<thead>
<tr>
<th>ASIL</th>
<th>Certainty that Safety Function is Correctly Performed</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>Very High</td>
</tr>
<tr>
<td>C</td>
<td>High</td>
</tr>
<tr>
<td>B</td>
<td>Medium</td>
</tr>
<tr>
<td>A</td>
<td>Low</td>
</tr>
<tr>
<td>QM</td>
<td>Quality Measures are Enough</td>
</tr>
</tbody>
</table>
Functional Safety is relevant for the whole car

- **Front View Camera System**
  - No valid video sensor data
  - ASIL B

- **Instrument Cluster**
  - Speedometer not available
  - ASIL B

- **Transmission**
  - Unwanted vehicle deceleration
  - ASIL C to D

- **Active Suspension**
  - Suspension oscillates
  - ASIL B to C

- **Smart Rear View Camera System**
  - No valid video sensor data
  - ASIL B

- **Rear Lights**
  - Failure on both sides
  - ASIL A

- **Airbag System**
  - Inadvertent Deployment
  - ASIL D

- **77GHz RADAR ACC**
  - Inadvertent Braking
  - ASIL C

- **Engine Management**
  - Unwanted vehicle acceleration
  - ASIL C to D

- **Electric Power Steering**
  - Self Steering
  - ASIL D

- **Braking and Stability Systems**
  - Unintended full power brake
  - ASIL D

- **Driving Lights**
  - Failure on both sides
  - ASIL B

- **Break Lights**
  - Loss of Brake Lights
  - ASIL B

- **Sensor Fusion ECU**
  - Don’t send incorrect commands
  - ASIL D

- **HMI**
  - Human Machine Interface

---

The safety goals may differ, depending on the OEM, vehicle type and region.
Paradigm shift: Fail-Safe to Fail-Operational
Fail-Operation : Foundation for AD

Level 0 – Level 5: SINGLE definition across the globe: NHTSA = VDA = SAE

- **Level 0**: Driver only
  - Driver task
  - No system
  - "Feet-off"
  - Driver completely in charge

- **Level 1**: Assisted
  - Driver in charge of longitudinal or lateral control
  - Vertical or lateral control
  - Vehicle takes charge of other functions

- **Level 2**: Partly automated
  - Vertical and lateral control
  - Vehicle runs both longitudinally and laterally in certain situations

- **Level 3**: Highly automated
  - "Eyes-off"
  - Driver needs to be ready to take over as a backup system

- **Level 4**: Autonomous
  - "Brain-off"
  - Driverless during defined use case
  - Autonomous

- **Level 5**: Driverless
  - No driver

**ADAS**
Advanced driver assistance systems

**AD**
Automated driving

Amendments of current regulations are necessary (e.g. Vienna StVO, ECE-R79)

**Fail Safe, driver fallback**

**Fail Operation, machine fallback**

Source: Barclays Research

Copyright © Infineon Technologies AG 2018. All rights reserved.
### Fail operational Response Time

<table>
<thead>
<tr>
<th>Level 3: Eyes-off</th>
<th>1 s – 10 s</th>
<th>driver takes over after warning</th>
</tr>
</thead>
<tbody>
<tr>
<td>e.g. driver sleeping</td>
<td>10 s – 20 s</td>
<td>repeat warning if no driver response, prepare for stop</td>
</tr>
<tr>
<td></td>
<td>20 s – 30 s</td>
<td>manage controlled and save stop</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level 4: Brain-off</th>
<th>1 min – 15 min</th>
<th>car stops at next rest area</th>
</tr>
</thead>
<tbody>
<tr>
<td>e.g. driver on rear seat</td>
<td>&gt;15 min</td>
<td>prepare and manage controlled and save parking stop</td>
</tr>
<tr>
<td></td>
<td>10 s – 20 s</td>
<td>stop in a controlled way at very severe failures</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level 5: Driver-off</th>
<th>1 h – 10 h</th>
<th>car is driving home</th>
</tr>
</thead>
<tbody>
<tr>
<td>e.g. no driver in car</td>
<td>&gt;10 h</td>
<td>car is driving to next partner service station</td>
</tr>
<tr>
<td></td>
<td>10 s – 20 s</td>
<td>stop in a controlled way at very severe failures</td>
</tr>
</tbody>
</table>
Driverless cars consist of many fail operating building blocks and systems.
AD demands high dependability across all systems

- Airbag
- ABS
- Adaptative Cruise Control
- Blindspot
- Lane Departure Warning
- Automated Parking
- Lane Keep Assist
- Autonomous Parking
- Highway assist
  - Stop&Go
  - Cruising (0-130 km/h)
- Blindspot
- Lane Departure Warning
- Automated Parking
- Lane Keep Assist
- Highway assist
  - Inter-urban
  - City Stop & Go
- AEB
- Parking Assist
- Automated driving
  - Stop&Go
  - Cruising (0-130 km/h)
- Driverless Cars
- Highway (Highly automated)

Fail Silent
Fail Safe with enhanced fault tolerance
Fail Operational
Architectural Considerations
Fail-Operational Architecture

**Diversity**
Same task with different algorithms,
Architectural implementation

**Redundancy**
2002 DFS architecture,
2003 Triplex Modular Redundancy with voting
Redundant architecture considerations

2oo2 DFS (Dual Fail Safe)

- 2oo2 can be derived from today’s Fail Safe systems
- Two redundant and robust channels with diagnostic monitor
- Implications of this architecture
  - Two systems with each being able to supply safe, secure, reliable and available Service
  - Two independent supply’s for each channel
  - Optional isolated inter processor communication

2oo3 TMR (Triple Modular Redundancy)

- 2oo3 is the reference architecture in aerospace and in several safety critical systems
- Concept = 3 different units whose results are compared using majority vote
- Implications of this architecture
  - Independent supply for each computing unit (3 supplies) and each voter
  - Need to compare results using a majority vote with voter
  - Voter Complexity might increase with data throughput
2oo2DFS Architecture
(Symmetric vs. Asymmetric)

Performance, Power Budget, and Software Re-use Will Drive Architecture

**Symmetric**

```
ADAS/AD
Sensor Set #1,2
Primary Compute (PC)
Secondary Compute (SC)
```

Attributes:
- Higher cost
- Higher power consumption
- Full functionality in case of failure

**Asymmetric**

```
ADAS/AD
Sensor Set #1
Switch #1
Primary Compute (PC)
Secondary Compute (SC)
Switch #2
Secondary Compute (SC)
```

Attributes:
- Lower cost
- Lower power consumption
- Limited functionality in case of failure

**PC:** High Computation ("Number Cruncher")

**SC:** Object-level Fusion and ASIL-D Controller
2oo2 DFS can be derived from today's Fail Safe systems

Two redundant and robust channels with diagnostic monitor

Implications of this architecture
• Two systems with each being able to supply safe, secure, reliable and available Service
• Two independent supply's for each channel
• Optional isolated inter processor communication
Challenges
Challenges in Fail Operation Systems

- Increase in hardware costs in cases of triple Redundancy systems
- Systems can’t be completely re-used because of diversity need
- Redundancy ≠ Fail Operation
- Increase in ASIL levels for most of the systems for Highly Automated Driving
- Challenges in Testing and Validation of Fail Operational Systems
- Non-Deterministic Machine Algorithms used in Highly Automated Driving
Fail-Operational Architecture Complexity

Fail-operational view

How much redundancy?

- Automated drive ECU main
- Automated drive ECU secondary

Drive Domain Controller
- Crash Protection
- xEV
- Combustion
- Braking main
- Braking secondary
- EPS main
- EPS secondary
- Transmission main
- Transmission Sec.

Body / comfort Domain Controller

Infotainment Domain Controller

- Ethernet
- CAN
- FlexRay
- LIN
- Other

Supply: supply1, supply2

Copyright © Infineon Technologies AG 2018. All rights reserved.
Challenges in FuSa for Neural Networks

Traditional Systems VS Neural Networks

ISO 26262

<table>
<thead>
<tr>
<th></th>
<th>Traditional Systems</th>
<th>Neural Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Included in 2nd Edition</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Process Defined</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Development Guidelines</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Safety Concept</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Software Tools</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>

Uncertainties & Unknowns in Neural Networks

1. Content and deterministic characteristic of software is uncertain as it learns over time
2. No existence of development standards or best practices
3. Unknown of what additional system measures are needed to argue/prove it’s safe
4. Uncertainty in how much training sets are needed to claim a “Predictable and Trusted” behavior
ISO26262 Limitations for ADAS/AD

- ISO26262 addresses the safety risk of a malfunctioning E/E in a vehicle.
- However:
  - In ADAS applications safety hazards (for driver, passengers, pedestrians, etc.) may come from a “fault-free” system:
    - Decision Algorithms (braking, steering).
    - Driving conditions (fog, snow, traffic, roadworks, etc.).
    - Environmental noise (EM, signal degradation, etc.).
- SOTIF: Safety of Intended Functionality (ISO/WD PAS 21448 – under development [https://www.iso.org/standard/70939.html]).

For SAE L3 or greater: ISO26262(2nd Edition) + SOTIF
Part of your life. Part of tomorrow.