THE THIRD PHASE OF IoT:

CONNECTED

SMART

AUTONOMOUS

SOFTWARE DEFINED BY AI
AUTONOMOUS SYSTEMS: COMPUTING PLATFORM

Intelligent eyes
- Vision.

Intelligent & powerful brain
- Perception and fusion.
- Modeling and planning.
- Decision making.

We need high-performance computing, flexibility, and programmability.
AUTONOMOUS SYSTEMS: E2E

THINGS

GATEWAY

NETWORK INFRASTRUCTURE

DATA CENTER/ CLOUD

IN-VEHICLE

Autonomous Driving Functions
- Trajectory Enumeration,
- Path Planning, Path Selection,
- Driving Policy, Maneuvering

Real-Time Environment Modeling
- Localization

Sensor Processing and Fusion
- Object ID and Classification,
- Multimodal, Time-Synchronized

Deep Learning Scoring

COMMUNICATION

Data Annotation and Labeling

Over-the-Air Updates to Models, Maps

Data Store

Data Set Management

Anomalous Data

5G

ANOMALY DETECTION

Sneakernet Test Fleets

DATA CENTER

End Point Management
- Geographical Tracking, OTA Updates

Deep Learning

Big Data and Statistical Analytics

- Model Training
  - Multi-node/Intel®
  - Architecture-Optimized Frameworks
A FLOOD OF DATA...

<table>
<thead>
<tr>
<th>Average Internet User</th>
<th>~1.5 GB of Traffic per Day</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Hospital</td>
<td>3,000 GB per Day</td>
</tr>
<tr>
<td>Autonomous Vehicles</td>
<td>4,000 GB per Day... Each</td>
</tr>
<tr>
<td>Airplane Data</td>
<td>40,000 GB per Day</td>
</tr>
<tr>
<td>Smart Factory</td>
<td>1,000,000 GB per Day</td>
</tr>
</tbody>
</table>

- Technical Data
- Societal & Crowdsourced
- Personal Data
...BUT CAN WE TRUST AUTONOMOUS SYSTEMS?

H/W and S/W complexity is expected to growth at least by a factor 20 in the next few years, so higher risk of failures....

Connectivity brings security threats....

...and autonomous systems are expected to detect & control failures!

I'm sorry Dave. I'm afraid I CAN'T do that.
THE DESIGN SPACE OF AUTONOMOUS SYSTEMS

H/W and S/W complexity is expected to grow at least by a factor 20 in the next few years, so higher risk of **failures**....

Connectivity brings **security threats**....

...and autonomous systems are expected to detect & **control** failures!
THE PATH TO TRUST

Adaptive Learning

Multi-agent formal-based safety + SOTIF

Agent Independent Safety (FuSa) at element level

Anomaly detection and reaction

Security
WE NEED FUNCTIONAL SAFETY

The absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems

Systematic failures
(Bugs in S/W, H/W design and Tools)

Random H/W failures
(permanent faults, transient faults occurring while using the system)

Ruled by International Standards
setting the “state of art” (for liability)

IEC 61508
ISO 26262
Automotive
IEC 61511
Process Sector
IEC 61513
Nuclear Sector
IEC 61800-3
Electr. Drives
EN 50128
Railway applications
IEC 50156
Furnaces
ISO 62061
Machinery
EN 50128
Railway applications
.....etc.

IEC 61508
ISO 26261
Automotive
AUTOMOTIVE REQUIREMENTS (ISO 26262)

ASIL A
- e.g. 60% faults detected and controlled

ASIL B
- e.g. 90% faults detected and controlled, ≤ 100 FIT

ASIL C
- e.g. 97% faults detected and controlled, ≤ 100 FIT

ASIL D
- e.g. 99% faults detected and controlled, ≤ 10 FIT

ADAS, AD

S/W DEFINED COCKPIT, VISION, COM LINK

1 FIT = 1 «failure in time» = 1 failure in 1 billion of hours
NOT JUST AUTOMOTIVE.....

INDUSTRIAL
IT IS EXPECTED 70% OF S/W DEFINED INDUSTRIAL SYSTEMS WILL REQUIRE FUSA IN 2020

DRONES
FUSA IS A CONCERN FOR BOTH CONSUMER AND INDUSTRIAL DRONES

ROBOTICS
HUMAN ROBOTIC AS THE NEXT FRONTIER OF THE HUMAN-MACHINE INTERACTION
Intel® Xeon® Processor D-1529 for Industrial 61508 Certification Functional Safety Solution

Accelerate design of safety-certified applications with a tightly integrated development package from Intel, including hardware, software, test libraries, and documentation.

RUN MIXED CRITICALITY WORKLOADS
Run mixed—safe and nonsafe—workloads with built-in virtualization

IMPROVE OPERATIONAL INSIGHT
Provides high levels of traceability and verification

ADDRESS KEY INDUSTRIAL USE CASES
Supports robotics, security, control and automation systems, and more

OPTIMIZE DIAGNOSTICS
Offline and online software diagnostics, software validation, and fault injection

intel.com/industrial-functional-safety-d1529

© 2016 Intel Corporation. All rights reserved. Intel, the Intel logo, the Intel Inside logo, Intel Experience What’s Inside, Intel Inside, the Intel Inside logo, and Xeon are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.
Safety for high-performance high-safety systems

- **100% H/W-based FuSa** (e.g. Dual core lock step).
- **S/W-based redundancy** (e.g. Loosely coupled lock step).
- **Heterogeneous and reconfigurable systems supported by FuSa hooks in H/W.**

**Safety «island», i.e. central brain for FuSa (for error detection and control)**

**Time Sensitive Network**

**High performance cluster**
- **Specialized**
- **FPGA**
- **MCU (actuation)**
«Guidance for system development with safety-related availability requirements», i.e. fail operational systems including the possibility of degrading to a lower ASIL in case of a fault...
Time to detection and time to reaction are important characteristics of the safety architecture.
Trending toward an holistic H/W level view, from ECU down to System On Chip, e.g.:

- Identifying link between fault-error-failures.
- Performing fault injection at different level of abstractions (safe vs dangerous, soft errors vulnerability,...).
- Etc...

ISO 26262 2nd edition: >180 pages guideline on how to apply Fusa to semiconductors
ISO 26262-11 has a chapter dedicated to dependent failures of semiconductor devices.
Fault injection at different abstraction level...

ISO 26262-11, clause 4.8

4.8.2 Characteristics or variables of fault injection
With respect to fault injection, the following information can help the verification planning:
- the description and rationale about fault models, and related level of abstraction;
- type of safety mechanism including required confidence level;
- observation points and diagnostic points;
- fault site, fault list, and
- workload used during fault injection.

4.8.3 Fault injection results
Results of fault injection can be used to verify the safety concept and the underlying assumptions as listed in 4.8.1 (e.g. the effectiveness of the safety mechanism, the diagnostic coverage and amount of safe faults).

NOTE 1 Evidence of fault injection is maintained in the case of inspections during functional safety audits.

NOTE 2 An exact correspondence between the fault simulated and the fault identified in the safety analysis (e.g. for open faults) may not always exist. In such a case refinement of the safety analysis can be based on the results of other representative faults (e.g. N-detect testing as reported in 5.1.10.2).
Confidence in the use of software tools is crucial for autonomous systems.
SAFETY ARCHITECTURES TREND - SW LEVEL

- A full stack of S/W components from front-end to back-end...... + FuSa.
- Need to support multiple and heterogeneous programming models.
- Complex OS compliant with Functional Safety standards.
Trending toward a combination of different techniques to achieve Functional Safety of S/W components, e.g.:

- Failure mode and effects analysis (FMEA) at least at S/W architecture level.
- ASIL/SIL decomposition and/or sand-boxing (e.g. for legacy F/W).
- S/W statistical analysis.
- Etc...

Note: QM+QM cannot lead to ASIL
SAFETY OF INTENDED FUNCTIONALITY

Autonomous systems that rely on sensing, can miss their goal and cause safety violations in absence of H/W or S/W failure...

<table>
<thead>
<tr>
<th>Causal factor of hazard with example</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>System E/E System failures</td>
<td>ISO 26262</td>
</tr>
<tr>
<td>Unintended behaviour without fault or failure (including E/E System performance limit)</td>
<td>SOTIF guidance</td>
</tr>
<tr>
<td>Foreseeable user misuses</td>
<td>SOTIF Annex</td>
</tr>
</tbody>
</table>

**ISO WD PAS 21448 1**

Safety of Intended Functionality (SOTIF)

- **System**
  - E/E System failures
  - Unintended behaviour without fault or failure (including E/E System performance limit)
  - Foreseeable user misuses

- **External factor**
  - Security violation
  - Impact from active Infrastructure and/or vehicle to vehicle communication.
  - Impact from car surroundings (other users, “passive” infrastructure, environment: weather, EMC...)

**Scope**

- Mentioned as necessary to ensure a safe behaviour, but not addressed in this document (See ISO21434:XXXX or SAE J3061)
- Can be necessary for a safe behaviour but not fully addressed in this document (ISO 20077 can be considered)
- Included in SOTIF scope
ISO 26262 2nd Edition Hot Topics - SOTIF

Safety of Intended Functionality (SOTIF)

ISO WD PAS 21448

Advanced development

Production development

SOTIF process

ISO 26262 process
### ISO 26262 2nd Edition Hot Topics - SOTIF

**Scene:** snapshot of the environment including the scenery and dynamic elements, as well as all actors’ and observers’ self-representations, and the relationships among those entities.

<table>
<thead>
<tr>
<th>Dynamic elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic objects’ states and attributes</td>
</tr>
<tr>
<td>Dynamic model-incompliant information</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scenery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lane network (lanes, conflict areas, ...)</td>
</tr>
<tr>
<td>Stationary elements (obstacles, curbs, traffic signs, traffic light positions, model-incompliant information, ...)</td>
</tr>
<tr>
<td>Vertical elevation</td>
</tr>
<tr>
<td>Environment conditions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Self-representations of actors and observers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skills and abilities, e.g., field of view or occlusions</td>
</tr>
<tr>
<td>Actors/observers’ states and attributes</td>
</tr>
</tbody>
</table>

**Situation:** selection of an appropriate behaviour pattern at a particular point of time.

<table>
<thead>
<tr>
<th>Relevant dynamic elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic objects’ states and attributes</td>
</tr>
<tr>
<td>Dynamic model-incompliant information</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Relevant scenery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lane network (lanes, conflict areas, ...)</td>
</tr>
<tr>
<td>Stationary elements (obstacles, curbs, traffic signs, traffic lights, model-incompliant information, ...)</td>
</tr>
<tr>
<td>Vertical elevation</td>
</tr>
<tr>
<td>Environment conditions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Relevant self-representation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skills and abilities</td>
</tr>
<tr>
<td>Ego state and attributes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Relevant goals &amp; values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transient (mission, operator commands, ...)</td>
</tr>
<tr>
<td>Permanent (regulatory, societal, ...)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Relevant function-specific situation aspects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Situation assessment results</td>
</tr>
<tr>
<td>Behavior intentions and options</td>
</tr>
<tr>
<td>Behavior actions and events</td>
</tr>
</tbody>
</table>

**Example:** critical situation analysis
- Weather conditions
- Mechanical disturbance
- EMC disturbance
- Acoustic disturbance
- Bad reflection
ISO 26262 2ND EDITION HOT TOPICS - SOTIF

- The use cases in which it is activated;
- The sensing and arbitration concept and technologies;
- The level of authority over the vehicle dynamics; and
- The interfaces with the other systems and functions of the vehicle and the road infrastructure.

- Severity and controllability are considered to determine the scenario for which a credible harm can result from the situation misinterpretation. For controllability, a delayed reaction may need to be considered.

- System improvement to avoid or reduce the risk which leads to a safety violation as a result of encountering a critical operational situation
- Functional restriction to reduce or mitigate critical operational situation effects
- Handing over the authority from a system to a driver to improve the controllability of critical operational situation effects
- Reduction or mitigation of foreseeable misuse effects

---

**Figure:**

Diagram illustrating the process of identifying and evaluating SOTIF risks, including steps for functional and system specification, risk identification and evaluation, and decision-making processes involving controllability and severity.

**Key Points:**
- **SOTIF Risk Identification and Evaluation**
- **Severity or Controllability Accepted?**
- **Hazardous Use Case Identification**
- **Known Use Case Coverage Sufficient?**
- **Unknown Use Case Coverage Targets Fulfilled?**
- **SOTIF V&V Area 2 Required**
- **SOTIF V&V Area 3 Required**

---

Internet of Things Group

ICRI-CARS kick-off
ISO 26262 2\textsuperscript{nd} EDITION HOT TOPICS – SOTIF

ISO WD PAS 21448 1 Annex E

Purpose

Extract misuse scenario sufficiently.

Strategy

clarify points that should be consider when we derive the misuse scenario.

Scope

- Vehicle/System level
- Except failure scenario

Input for consideration

Action

1) Consider stakeholders.
   Ex) driver/passenger

2) Consider misuse causes.
   Ex) Do not understand /False recognition/ Mistake/misjudgment/Intentional

3) Consider interactions between driver and system/vehicle.
   Ex) Usage of the system/ Warning or Information from system/ Vehicle behavior

4) Consider environment condition.
   Ex) road condition/ weather/ traffic condition

General guide word list of misuse.

Hazard analysis which is consider the hazard factor in interacting function units.

Input for reference

General driving and environmental condition list.

Output

Table D.3 Example of misuse scenario table.
ISO 26262 2\textsuperscript{nd} Edition Hot Topics - SOTIF

ISO WD PAS 21448 1 clause 10.2

Table 4: Sensor verification and validation

<table>
<thead>
<tr>
<th>Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>1a Determination of standalone sensor characteristics (e.g. Range, precision, resolution, timing constraints, bandwidth, signal-to-noise ratio, etc.)</td>
</tr>
<tr>
<td>1b Verification of the implementation of requirements</td>
</tr>
<tr>
<td>1c Determination of sensor characteristics, when integrated in the vehicle environment</td>
</tr>
<tr>
<td>1d SIL / HIL testing on selected test cases (derived from a technical analysis and by error guessing)</td>
</tr>
<tr>
<td>1e Vehicle level testing on selected test cases (derived from a technical analysis and by error guessing)</td>
</tr>
</tbody>
</table>

4 In some cases it is possible to emulate an unexpected behaviour of the sensor by means of fault injection at the simulation level, e.g. in the case of image sensors randomly flipping multiple pixels in a sequence of images to emulate field noise. A rationale as to why the fault models are able to represent the tested phenomena should be provided. Outcomes of those simulations may be combined with results of safety analyses.

Table 5: Decision Algorithm verification and validation

<table>
<thead>
<tr>
<th>Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>1a Robustness to Signal-to-Noise Ratio degradation (for example by noise injection testing)</td>
</tr>
<tr>
<td>1b Verification of the architectural properties including independence, if applicable</td>
</tr>
<tr>
<td>1c SIL / HIL testing on selected test cases (derived from a technical analysis and by error guessing)</td>
</tr>
<tr>
<td>1d Vehicle level testing on selected test cases (derived from a technical analysis and by error guessing)</td>
</tr>
</tbody>
</table>

Table 6: Actuation verification and validation

<table>
<thead>
<tr>
<th>Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>1a Determination of standalone actuators characteristics (e.g. precision, resolution, timing constraints, bandwidth, etc.)</td>
</tr>
<tr>
<td>1b Verification of actuators characteristics, when integrated within the vehicle environment</td>
</tr>
<tr>
<td>1d SIL / HIL testing on selected test cases (derived from a technical analysis and by error guessing)</td>
</tr>
<tr>
<td>1e Vehicle level testing on selected test cases (derived from a technical analysis and by error guessing)</td>
</tr>
</tbody>
</table>

Table 7: Robustness and Controllability verification and validation

<table>
<thead>
<tr>
<th>Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>1a Robustness to Signal-to-Noise Ratio degradation (for example by noise injection testing)</td>
</tr>
<tr>
<td>1b SIL / HIL testing on selected test cases (derived from a technical analysis and by error guessing)</td>
</tr>
<tr>
<td>1c Randomized input tests including error injection*</td>
</tr>
<tr>
<td>1d Vehicle level testing on selected test cases (derived from a technical analysis and by error guessing)</td>
</tr>
<tr>
<td>1e Controllability tests</td>
</tr>
</tbody>
</table>
| * Error Injection is used to generate input tests including erroneous patterns e.g. in the case of image sensors adding flipped images, altered image patches etc.
WE NEED SECURITY

The prevention of risks related to malicious intrusions, through computer and/or communication networks

SAE J3101 - Requirements for Hardware-Protected Security for Ground Vehicle Applications

- Secure Boot.
- Secure Storage.
- Secure Execution Environment.
- OTA, authentication.
- ...

SAE J3061 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

- Attacks enumeration.
- Threat analysis.
- Reduction of attacks surface.
- Security testing.
- ...

We need security: The prevention of risks related to malicious intrusions, through computer and/or communication networks.
ISO 26262 2\textsuperscript{nd} Edition Hot Topics - Safety & Security

- Security threats affecting FuSa
- Security measures helping FuSa
- FuSa measures as vulnerable points for security attacks
- FuSa measures helping security

Diagram:
- Hazard Analysis And Risk Assessment (HARA)
- Threat Analysis and Risk Assessment (TARA)
- Functional safety concept
- Safety concept review
- Fu..Sa. And Security Concepts defined
- Safety-Related Threats from TARA
- Threats and Safety Goals from HARA
- Cybersecurity concept
- Cybersecurity concept review

Source: Guidance on Potential Safety-Cybersecurity Interface Points (Informative Only)
ISO 26262-4:2018
Cybersecurity related changes

6.4.1 Specification of the technical safety requirements

a) the system configuration and calibration requirements.

NOTE 1 The ability to reconfigure a system for alternative applications is a strategy to reuse existing systems.

EXAMPLE 3 Calibration data (see ISO 26262-6:2018, Annex C) is frequently used to customise electronic engine control units for alternate vehicles.

NOTE 2 The cybersecurity concept (cybersecurity strategy and requirements), if applicable.

6.4.2 Safety mechanisms

...a) the safety mechanisms that enable the system's contribution to achieve or maintain the safe state of the item;

NOTE 4 This includes arbitration in the case of multiple control requests from safety mechanisms.

NOTE 5 Cybersecurity can be considered.
We need **self-adaptable systems**

Failure and threat **analytics**, combined with autonomous mission anomaly detection and control, are a great opportunity to build anomaly-aware and self-adaptable systems in cooperation with **Machine Learning** and **AI**.
Off-line Machine Learning Process Flow
CALL TO ACTION - KEY TOPICS FOR RESEARCH

H/W
- How to implement cost effective fault tolerant concepts tuned to new fault models

S/W
- How to make modern & complex S/W systems safe

SOTIF
- How to fill the gap between «ultimate» and «our» reality

Automation
- How to implement a Design for Safety & Security automated flow

AI
- How to use AI/DL/ML for mission anomaly detection
LEGAL NOTICES AND DISCLAIMERS

Intel technologies’ features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

© 2017 Intel Corporation