An overview of TaaS reliability, security and functional safety challenges

Giovanni Sartori, IOTG ASPE FSS
Rebeca Delgado, TSS
Legal notices and disclaimers

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

This material may relate to the creation of end products used in safety-critical applications designed to comply with functional safety standards or requirements (“Safety-Critical Applications”). You agree and represents that you have all the necessary expertise to design, manage and ensure effective system-level safeguards to anticipate, monitor and control system failures in safety-critical applications. It is your sole responsibility to design, manage and assure system-level safeguards to anticipate, monitor and control system failures, and you agree that you are solely responsible for all applicable regulatory standards and safety-related requirements concerning your use of any material related to Safety Critical Applications. You agree to indemnify and hold Intel and its representatives harmless against any damages, costs, and expenses arising in any way out of your use of the material related to Safety-Critical Applications.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting: http://www.intel.com/design/literature.htm

Intel technologies’ features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at http://www.intel.com/ or from the OEM or retailer.

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.

Copyright © 2019, Intel Corporation. All rights reserved.
TAAS: what we need for its adoption

ISO 26262: Functional Safety
ISO 21448: Functional Safety Of Intended Functionality
SAE J3101, J3061: Cybersecurity and Safety

Scalable safe & secure architectures
Functional safety – iso 26262 2\textsuperscript{nd} edition

2\textsuperscript{nd} edition released in 2018

- HW random and systematic failures
- ASIL = Automotive Safety Integrity Level

Source: ISO 26262:2018 - Figure 1
Cybersecurity and functional safety

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.
SOTIF - Safety Of The Intended Functionality

Those systems relying on complex sensors and processing algorithms for getting proper situational awareness can experiment hazardous behaviors due to the intended functionality or to performance limitations in the fault-free system/elements.

Examples:

- Inability of the function to comprehend correctly the situation and operate safely,
- Insufficient robustness to inputs variation of sensors or environment conditions.

• SOTIF is the absence of unreasonable risk due hazardous behaviors related to such limitations.

• SOTIF it’s currently the ISO PAS 21448.
Contributors to Hazardous events

Faults

- HW random
- Transient fault
- Latent fault
- SW bug

System failure

ISO 26262

Triggering events

- Misuse
- Wrong detection

Simplified view!

System weakness

Scenario

Faults

- SW bug
- HW random
- Transient fault
- Latent fault

System failure

ISO 26262

Hazardous event

SOTIF

Internet of Things Group

Vector Congress North America 2019
Known-Unknown Scenario categories

<table>
<thead>
<tr>
<th>Area</th>
<th>System behavior</th>
<th>Scenario class</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Nominal behavior of the system</td>
<td>Known safe scenarios</td>
</tr>
<tr>
<td>2</td>
<td>Known system limitations</td>
<td>Known unsafe scenarios</td>
</tr>
<tr>
<td>3</td>
<td>Unexpected behavior of the system</td>
<td>Unknown unsafe scenarios</td>
</tr>
<tr>
<td>4</td>
<td>Robust system</td>
<td>Unknown safe scenarios</td>
</tr>
</tbody>
</table>

Source: ISO/PAS 21448, 2019 §4
POSSIBLE SYSTEM behavior IN DIFFERENT CONDITIONS

<table>
<thead>
<tr>
<th>Case</th>
<th>Behavior</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRUE POSITIVE</td>
<td>System activation as expected in a real critical condition</td>
<td>Presence of a real critical condition</td>
</tr>
<tr>
<td>FALSE POSITIVE</td>
<td>Unexpected system activation in non-critical condition (false alarm)</td>
<td>Absence of any real critical condition</td>
</tr>
<tr>
<td>TRUE NEGATIVE</td>
<td>System does not activate as expected since non critical condition</td>
<td>Absence of any real critical condition</td>
</tr>
<tr>
<td>FALSE NEGATIVE</td>
<td>System does not activate in a real critical condition</td>
<td>Presence of a real critical condition</td>
</tr>
</tbody>
</table>
# External/INTERNAL factors influencing sensors

<table>
<thead>
<tr>
<th>Sensor type</th>
<th>External factor</th>
<th>Effect on sensing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Camera</td>
<td>Heavy rain</td>
<td>Distorted image</td>
</tr>
<tr>
<td>Camera</td>
<td>Sunny day</td>
<td>Blindness</td>
</tr>
<tr>
<td>Radar</td>
<td>Snow</td>
<td>Reduced range</td>
</tr>
<tr>
<td>Radar</td>
<td>RF interference</td>
<td>Degraded detection</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sensor type</th>
<th>Internal factor</th>
<th>Effect on sensing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Camera</td>
<td>Low resolution/MP</td>
<td>Reduced detection distance</td>
</tr>
<tr>
<td>Radar</td>
<td>Poor range/angular accuracy</td>
<td>Reduced discrimination</td>
</tr>
</tbody>
</table>
SOTIF measures for risk reduction

• On sensors, previous internal and external factors act as triggering events
• For SOTIF adequate risk reduction measures are required
  – Example:

<table>
<thead>
<tr>
<th>Sensor type</th>
<th>Triggering event</th>
<th>Risk reduction measure(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Camera</td>
<td>Heavy rain</td>
<td>Limit system performance in case of severe weather condition</td>
</tr>
<tr>
<td>Radar</td>
<td>Poor range/angular accuracy</td>
<td>- Select sensors with adequate discrimination capabilities OR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Modify their architecture</td>
</tr>
</tbody>
</table>
FuSa architectures and trade-offs

System level safety based on Off The Shelf (OTS) components used as QM plus ASIL safety monitors

Diverse or homogenous combination of safety capable components

Single safety capable component plus fall back

Source: various, from the Web
FUSA Architecture trend

Source: various, from the Web