FUNCTIONAL SAFETY FOR MULTI-CORE PROCESSOR BASED AVIONICS SYSTEMS

Jyotika Athavale, Principal Engineer, Senior Functional Safety Technologist
Riccardo Mariani, Intel Fellow, Chief Functional Safety Technologist
GROWING COMPLEXITY AND HIGHER RISK OF FAILURES

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**....
WHAT IS 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)
• Intel’s key role in FuSa standards:
  • Leading **ISO 26262 Part 11**, i.e. “Guideline on application of ISO 26262 to semiconductors”
  • Workgroup members in:
    – ISO 26262 (US, IT, and DE delegations)
    – ISO/NWIP 3568 (SOTIF)
    – SAE J2980 (ASIL Hazard Classification)
    – SAE J3061 (Cybersecurity)
    – IEC 61508 (industrial)
• Intel develops products intended to be used in functional safety application following a strict FuSa lifecycle compliant with functional safety standard such as ISO 26262, IEC 61508, ISO 13849 etc.

• More than 150 work products (including revisions)

• Final certification achieved in 2018
INTEL FUNCTIONAL SAFETY ACHIEVEMENTS

✔ FuSa LifeCycle 3.0 certified for ISO 26262:2018 (ASIL D) and IEC 61508:2010 (SIL 3) by TUEV: first Intel externally certified development process; paving the way for Intel products’ broad acceptance in the Automotive and Industrial markets.

✔ fRTools Suite 2018.1 Certification By TUEV Sued: The suite contemplates a set of tools used to perform functional safety analysis and metrics verification on Intel SoC in order to ensure the capability to reach the Safety Integrity Level required in IOTG key markets (i.e. Automotive, Industrial).
## FSLC WorkProducts

This is an example list of work products compliant to the FSLC --

<table>
<thead>
<tr>
<th>Calibration data</th>
<th>FuSaMatrix</th>
<th>Safety Post-Si VR</th>
<th>Supplier DIA – Accepted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calibration data specification</td>
<td>FuSaScopeEvaluation</td>
<td>Safety Report</td>
<td>SW coding standard</td>
</tr>
<tr>
<td>Change Management Plan</td>
<td>PSA</td>
<td>Selection report</td>
<td>Systematic Capability Appraisal</td>
</tr>
<tr>
<td>Change Management Report</td>
<td>Qualification of suppliers</td>
<td>Software Tool Chain evaluation</td>
<td>Target Reachability</td>
</tr>
<tr>
<td>Configuration data</td>
<td>Release to production notice</td>
<td>SOW</td>
<td>Tool application guidelines</td>
</tr>
<tr>
<td>Configuration data specification</td>
<td>Safety Analysis - DFA</td>
<td>SReq - HSI</td>
<td>User Guide</td>
</tr>
<tr>
<td>Configuration Management Plan</td>
<td>Safety Analysis - FFI</td>
<td>SReq - HW</td>
<td>V&amp;V Plan</td>
</tr>
<tr>
<td>Confirmation Measure - Review</td>
<td>Safety Analysis - FMEDA</td>
<td>SReq - SW</td>
<td>V&amp;V Report</td>
</tr>
<tr>
<td>DIA</td>
<td>Safety Case</td>
<td>SSAS</td>
<td>Safety Metric Verification Report</td>
</tr>
<tr>
<td>FI</td>
<td>Safety Concept</td>
<td>STL Code</td>
<td>Safety Package</td>
</tr>
<tr>
<td>FuSaLifecycle</td>
<td>Safety Manual</td>
<td>STL Pre-Si VP</td>
<td>Safety Plan</td>
</tr>
<tr>
<td></td>
<td>Safety Metric Verification Plan</td>
<td>STL Pre-Si VR</td>
<td>Safety Post-Si VP</td>
</tr>
</tbody>
</table>

IOTG Product and Technology Summit and Technical Exchange
Failure modes can be caused by permanent and transient random hardware faults.

Reliability prediction model (IEC62380), stress tests, wear out, field data, etc.

Soft error due to high energy neutrons, alpha particles, etc.
SOFT ERROR RATE DEFINITIONS

- **Soft Error** – a bit which is flipped by an alpha or neutron particle
  - Particles are naturally occurring and random events
  - There are more particle strikes at higher altitudes
  - Intel uses 900m for altitude (85% of the world population is below)

- **Benign Error** – a soft error that does not effect results
  - Bit never read, bit over-written, or corrected (ECC)

- **DUE** – Detected Uncorrectable Error
  - Bit upsets exceeding correction scheme and within detection regime
    - Parity protection scheme: no correction; Single Bit Upset (SBU) = detected error, double bit error = SDC
    - SECDED protection scheme: SBUs are corrected, double bit error = detected error
    - Typically results in a MCA event

- **SDC** – Silent Data Corruption
  - Represents potential for incorrect output at the pins of device, resulting in either:
    - System or application crash or hang,
    - Change in the output of application, or
    - May be masked altogether with no net effect
SOFT ERROR RATE MODELING

- SDC and DUE numbers represent Intel models
- Models built from analysis of test chips
  - Particle beam testing at Los Alamos
  - Confirmed with product testing
- Models tend to be conservative due to certain assumptions and inherent unknowns:
  - Use 900m elevation (>85% of population vs. average)
  - System utilization assumes one processor in 1 of 2 binary states:
    - Full utilization: 100% utilization
    - Sleep states: All cores in sleep state
    - Does not account for processor idle times in a multi-processor system
  - Software de-rating included for an average of various workloads
    - Robust OS and/or applications may result in further de-rating
- Individual products may vary

SER data are included in Safety Analysis
Soft errors induce the highest failure rate of all other reliability mechanisms combined.

Complying with Functional Safety requirements requires addressing several challenges for SER.
SOFT ERROR RATE: VULNERABILITY ANALYSIS

• Advanced flow to measure vulnerability of HW to soft-errors ($F_{safe}$ in ISO 26262)

$$SER^{derated} = \sum_{UCs} F_{UC} (V, f_{clk}) \cdot \sum_{circuits/nodes} SER^{nominal} \cdot TVF \cdot AVF \cdot PVF$$

3 vulnerability factors

- **AVF = Architectural Vulnerability Factor**
  - Function of micro-architecture & workload
  - Affects all logic – uArch structures, sequential state, static logic

- **TVF = Timing Vulnerability Factor**
  - Function of clocking, circuit behavior & workload
  - Affects primarily sequential state

- **PVF = Program Vulnerability Factor**
  - Function of final user observable program output
  - Intel can model PVF but does not generally take any benefit from it due to requirements for general purpose operation
  - For specific applications PVF can be modeled and accounted for

• We use a set of workloads covering a broad variety of both industry standard benchmarks as well as traces from actual workloads

• This trace-list is the same trace-list we use to profile our performance & power specs so we are consistent with regard to workload sets for all our specifications
PROBABILISTIC METRIC FOR HARDWARE FAILURES

ISO 26262 standard (automotive)

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

1 FIT = 1 «failure in time» = 1 failure in 1 billion of hours

Includes transient + perm failures

NOTE 2 In addition to these four ASILs, the class QM (quality management) denotes no requirement to comply with ISO 26262. Nevertheless, the corresponding hazardous event can have consequences with regards to safety and safety requirements can be formulated in this case. The classification QM indicates that quality processes are sufficient to manage the identified risk.
Functional Safety and in particular how to achieve compliance to transient reliability requirements is posing many challenges that need to be addressed to be successful in markets such as drones, robotics and autonomous vehicles.
SAFETY ANALYSES

• FMEA / FMEDA
  • Evaluates the mitigation measures (i.e. Safety mechanisms) in place and to be added in order to achieve the required safety integrity.
  • Compute (quantitative analysis) the safety metrics and failure rates (including SER).

• DFA and FFI
  • Dependent failure analysis to identify the single events or single causes that could bypass or invalidate a required independence or freedom from interference between given elements and violate a safety requirement.
  • Freedom From Interference (FFI) has been performed in case of coexistence within the same element or sub-elements with different or no ASIL allocated (e.g. SW running on IE).
H/W and S/W Safety Mechanisms tested for coverage and robustness
Intel Offers --

- High Performance
- High RAS
- Low Power
- Extended temp
- Extended life

FLIGHT SAFETY LANDSCAPE AND CHIP EVOLUTION

First Mover Advantage

- Increased complexity, increased functional integration.
- Shift to multicore processors; demand for higher performance.
- New failure modes.
- DO-254 DAL A certification needs.
DO-254 DESIGN ASSURANCE LEVELS / SAFETY CRITICAL SYSTEMS
The avionics safety standards do not describe specific requirements and work products needed for SOC components to achieve flight safety certification of systems. The focus is on avoidance of catastrophic events by ensuring correct execution (integrity) and continuous operation (availability) in critical situations.

By completing a gap analysis between the DO-254 and the Automotive ISO-26262, the proposed approach is to map the DO-254 Avionics safety requirements to corresponding artifacts from automotive ISO26262 certification, thereby leveraging certification efforts for automotive towards a flight safety evidence package.

The top-level safety processes between the two standards can be considered to be compatible although the terminology and resulting work products are different.

Work products, data items and lifecycles can be mapped between the two standards.

The safety approaches are generally equivalent.
FLIGHT SAFETY WORK PRODUCTS

- DO-254 requires certification of aircraft at the system level

- Work product examples (safety evidences) for DO-254 enablement are listed below

<table>
<thead>
<tr>
<th>WORK PRODUCT (EXAMPLES)</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electrical Data Sheets (EDS)</td>
<td>Datasheet including parameters and specifications</td>
</tr>
<tr>
<td>Product Reliability Qualification Reports (PRQ)</td>
<td>Data from stress tests and reliability prediction models</td>
</tr>
<tr>
<td>Manufacturing Validation (MV) Report</td>
<td>Data from DFX testing, test report, issues</td>
</tr>
<tr>
<td>C-Spec</td>
<td>Architecture Specification - Description of product and architectural features, block diagram usage model</td>
</tr>
<tr>
<td>Failure Mode Effects Analysis (FMEA) Reports</td>
<td>Quantitative analysis of safety metrics and failure rates; evaluate mitigation measures.</td>
</tr>
<tr>
<td>Platform Architectural Specification (PAS)</td>
<td>PAS contains block diagram, use cases, architectural features</td>
</tr>
</tbody>
</table>
SAFETY CONSIDERATIONS: REDUNDANCY AND DISSIMILARITY

• Redundancy
  • Dual Modular Redundancy (DMR) required for all systems
  • DAL A systems (flight controls, engine controls) need Triple Modular Redundancy (TMR)

• A redundant and dissimilar architecture is desired for safety critical systems. Dissimilarity is about absence/detection of common cause failures (CCF) due to:
  – HW random failures
  – HW/FW systematic failures
  – SW systematic failures
**DETERMINISTIC SYSTEM**

- A system in which no randomness is involved in the development of future states of the system. A deterministic model will thus always produce the same output from a given starting condition or initial state.

- FuSa can addresses some sources of “Randomness”
  - Atmospheric Neutrons flipping a bit etc.

**TEMPORAL DETERMINISM A.K.A REAL-TIME**

- The system completes the calculation in a deterministic amount of time, i.e. the Worst Case Execution time is “reasonably” bounded.

- Some aspects of Temporal Determinism can also be addressed by FuSa as part of the “Freedom from Interference” efforts, specifically those related to Timing and temporal program flow monitoring.
Purpose: Ensure Real-Time applications function correctly even in presence of Naïve or malicious concurrent workloads.
DEMONSTRATING WORST CASE EXECUTION TIMES AND BOUNDED INTERFERENCE
SUMMARY

- FuSa and SER requirements pose challenges in markets such as autonomous vehicles.

- SER is one of the most important and limiting failure mechanisms for functional safety applications.

- Methodology to analyze and meet the reliability of a functional safety component takes into account its safety goal, soft error testing and modeling methodologies, error classification and the use of innovative mitigation strategies in HW and SW.

- We need to explore innovations in all layers, including mitigation in technology, hardware, software and firmware. Combination of on-chip and off-chip features and techniques are critical to meet safety requirements.