**OSADL: Safety Critical Linux Working Group**

**Project # 4: Route $3_H$ - preliminary evaluation and investigation of compliance route option for pre-existing hardware**

Rationale:

IEC 61508 and derived standards assume that ASICs comply with one of two compliance routes:

→ Compliance route options 1 for HW: Route $1_H$ (FT + SFF)

a) Calculated safe failure fraction (SFF) of each element (treated as HFT 0 element).
b) Architectural protection is in place with each of the (semi-)independent channels having a comparable SFF.
c) The SFF for each element in the SIL2 system is 60%<SFF<90%

This requires a clear understanding of the safe respectively dangerous failures of the elements and the achievable (estimated) diagnostic coverage (DC) as a basis.

→ Compliance route options 2 for HW: Route $2_H$ (reliability data)

a) Field feedback for elements in similar applications and env – AND
b) Based on data collected in accordance with IEC 60300-3-2 or ISO 14224 – AND
c) Evaluated according to:
    i. The amount of field feedback – AND
    ii. The exercise of expert judgment - AND where needed:
    iii. The undertaking of specific tests;

Note that IEC 61508 assumes a HFT of 1 for type-B systems operating in continuous mode in compliance with SIL2 (see 61508-2 Ed 2 7.4.4.3.1). As all systems we are referring to here are conceptually type-B systems (see 61508-2 Ed 2 7.4.4.1.3).

Essentially it is though the vagueness of 61508-2 Ed 2 7.4.6 that on the one hand is problematic but on the other hand allows the freedom to assess the effective measures taken for mass production microprocessors during design, take credit for documented testing and generate adequate quality field data as well as the post processing of the same. The proposed route $3_H$ explicitly assumes the re-use of a pre-existing processor and not the generation of a specific processor for a project or system. All requirements for control of systematic faults critically hinge on the ability to understand the system elements (see notably 7.4.7.3 note on following good human-factor practice).

**Overview of development:**

| | |
|---|---|
| - *Phase 1:* | Initial assessment of 61508-1,3,3,5(,7)<br>• What does 61508 Ed 2 actually state about<br>• Pre-existing hardware with respect to:<br>  ○ Systematic capabilities |

| | |
|---|---|
| | ○ Random faults<br>○ Process level protection<br>○ General architectural options<br>○ General derating/decomposition options<br>• What do 61508 derived standards state<br>• What other sources or hardware assurance are there |
| - *Phase 2:* | Outline of a $3_H$ route<br>• Integration concept (position/phase/tables)<br>• Evidence definition (60300-3-2 and its referenced method standards)<br>• Review and possible extension of Annex-QR for methods and techniques tailoring/introduction<br>• Initial set of measures/techniques amendments<br>• Impact of $3_H$ on software qualification |
| - *Go/NoGo* | Meeting with hardware vendors and presentation of evidence needs<br>• What data (org, process, DLC, testing) is needed?<br>• What trade-offs are possible?<br>• What limits can be placed on non-disclosure? |
| - *Phase 3:* | Software level capabilities for hardware mitigation<br>• Conceptual mitigation capabilities at software level<br>○ Inherent diversity (hardware)<br>○ Diversified software elements<br>• Virtual NooM system software architecture capabilities<br>• Software based plausibilization |
| - *Phase 4:* | Hardware level capabilities for hardware mitigation<br>• General purpose diagnostics capabilities and shortcomings<br>• Virtualization technologies potentials and shortcomings<br>• Diversity potentials and shortcomings |
| - *Go/NoGo* | Concept review with partner safety engineers and TueV<br>• Review meeting (2 day workshop - Route $3_H$ concept - go/no-go |
| - *Phase 5:* | Detailed evaluation of $3_H$ options<br>• DLC mapping<br>• Initial measures and techniques specification (properties - effectively a 61508-3 Annex-C equivalent for part 2 at least for 61508-2 Annex-B)<br>• Tailoring of 61508-2 Annex-A/B/C (possibly extending Annex-QR methodology)<br>• Initial specification proposal for Route $3_H$ (clause) |
| - *Phase 6:* | Application of proposed $3_H$ |

| | |
|---|---|
| | • Hardware vendor data review<br>• Gap analysis and possible mitigation options<br>• Review of proposed measures and techniques against actually available data<br>• Maintenance and change management strategy (impact analysis) |
| - *Phase 7:* | Formal review meeting TueV and 2 day workshop<br>• Presentation of any adjustments to reality<br>• Presentation by hardware vendors on non-disclosed information<br>• Consolidation of disclosure needs of measures and techniques |
| - *Phase 8:* | Processing feedback from TueV/Partner safety engineering<br>• Update of Route $3_H$ specification<br>• Measure and techniques adjustments<br>• Final integration into system safety process - notably coupling with system software architecture and software related measures and techniques |
| - *Phase 9:* | Documentation of Route $3_H$ (ideally for a particular system) as example use:<br>• Complete interpretation mapping<br>• Documentation of relation to proposed route $3_S$ (SIL2LinuxMP)<br>• Resubmission of final draft to TueV |
| - *Phase 10:* | Dissemination:<br>• Discussion with the safety community, industry and FLOSS community. |
| **Participation form:** | |
| | • Established contact to nominated vendor representative to address low-level hardware issues<br>• Project development and data repository<br>• Project mailing lists (closed (for issues under NDA), development, review)<br>• Dissemination workshops (may be in context of other events) |
| **Responsibilities:** | |
| | • Project legal entity: OSADL with possible dependency on hardware vendors for some specified topics/issues.<br>• Project resource maintenance OSADL Safety Critical Linux WG<br>• Project Management: ??? (profile: ASIC design, hardware architecture)<br>• Technical lead: Nicholas Mc Guire<br>• Implementation: Markus Kreidl, Nicholas Mc Guire, TBD<br>• Certification Body: TBD |

| | |
|---|---|
| **Effort estimation:** | |
| | ToDo |
| **Timeline:** | |
| *Start* | Start as soon as a hardware vendor is available that is wiling to satisfy the information needs. |
| *Milestone 1* | Initial proposal workshop (hardware vendor participation) |
| *Milestone 2* | Formal concept workshop (CA participation) |
| *Milestone 3* | Initial release version (public/community) |
| *Milestone 4* | CA Report and all related artifacts published |
| *Maintenance phase* | |
| **Project format:** | |
| | Partner funded project (OSADL members) |