OSADL : Safety Critical Linux Working Group

Project # 3: Tools qualification for kernel verification tool-set.

Rationale:

Utilizing the Linux kernel for safety related systems hinges on the claims of adequate development rigor in general and the ability to detect and mitigate defects. Tools used for the kernel development thus play a key role.

While the kernel development life-cycle process has largely been outline by key kernel developers (Documentation/process as of October 2016) this forms the basis. In the development work-flow tools are mentioned at a number of points which addresses many of the formal needs but an assessment of the actual usage and the effectiveness can not rest on process records as in a bespoke process but must be assessed under the assumption of incompleteness and possibly incorrect application of tools and methods.

Provided the process is adequate and the use of tools is confirmed to be effective, that is classes of faults claimed to be addressed are actually addressed by developers, the question of tools completeness is still open. This is to be addressed by a adequate qualification of the individual tools - in context of the Linux kernel - as well as uncover possible gaps and inconsistencies.

Based on this assessment possible mitigations (e.g. by extension) are to be developed and finally executed to provide a complete assessment of tools and the tools generated artifacts for the certification process of the Linux kernel.

Overview of development:

- Phase 1:	Definitions • Tools set and dependent technologies • DLC specification related to tools usage • Tool set specification for potential kernel candidates • Execution environment for specified tool set
- Phase 2:	Investigation • Development of tools contributions (Clause 7 and Annex-A,B) • Tools gaps • Verification overlaps • Report on tool landscape for safety related system • V&V
- Phase 3:	Requirements • Tools requirements specification • Consolidation of requirements with maintainers

	• Mapping/interpretation of 61508-3 7.4.4 and 7.9 • Specific contributions of tools in context of Annex A/B and 61508-7 Annex-F/61508-3 Annex-C
- *Phase 4:*	Process specification and derived minimal tool verification • Data specification (notably false negative handling) • Defined criteria (bounded false-negatives and unhandled). • Formalized execution environment (as T1 tool)
- *Phase 5:*	Verification requirements and procedures specification • Review of tools with community (maintainers) • Formalized ATCs • ATC workshop with maintainers and community members (could be held in context of OSS event)
- *Phase 6:*	Implementation and mitigation • Mitigation of uncovered gaps • Implementation of infrastructure and extensions for tool and process verification requirements
- *Phase 7:*	Example run on common kernel tools (e.g. Coccinelle, sparse, KSAN, etc.) ideally 3 distinct tools to have a reasonable completeness of procedure and verification • Generate set of artifacts in CDP repo • Generation of formal ARs
- *Phase 8:*	Submission • Verification report for tools generated in phase 7 • Submission to TueV and partner safety group
- *Phase 9:*	Update of tools • Merge feedback/findings back into tools, verification • Process and reports • Feedback findings into community process • Post proposed tools amendments for mainline inclusion (e.g. adding a Coccinelle virtual mode for verification or sparse switches for verification purposes)
- *Phase 10:*	Dissemination to community and interested industry.
Participation form:	
	• Project development and data repository • Project mailing lists (development, review) • Dissemination workshops (may be in context of other events)

Responsibilities:	
	• Project legal entity: OSADL • Project resource maintenance OSADL Safety Critical Linux WG • Project Management: ??? • Technical lead: Nicholas Mc Guire (coordination) - tools maintainers for individual tools • Implementation: focus on tools community, Markus Kreidl, TBD • Certification Body: TueV Rheinland (proposed)
Effort estimation:	
	TODO
Timeline:	
Start	March 1 2019
Milestone 1	Initial tool landscape report
Milestone 2	Initial proposal of requirements, process and tool specific ATCs.
Milestone 3	Run of V&V efforts on selected set of kernel tools
Milestone 4	CA Report and all related artifacts published
Maintenance phase	
Project format:	
	Partner funded project (OSADL members)