OSADL: Safety Critical Linux Working Group

Project # 9: Root cause analysis (statistical severity estimation basis)

Rationale:

The term root cause analysis is quite contended in the safety community so a short (imprecise) definition: root cause analysis; identify the logical life-cycle phase in which the error that manifested it self was introduced and what the subjective causal factors of the committer were. The goal of the root cause analysis effort is to allow quantification of the defect severity (e.g. for contingency planing) as well as improved detection of those defects that are of elevated severity.

This effort would result in an initial assessment against historic defects (classification and contingency estimation) as well as in the initiation of a continuous (low volume) project to conduct root-cause analysis on defects in -stable (or -cip).

Overview of development:

- Phase 1:	Definition • Investigation of CVE processing • Root cause definitions (e.g. DLC phase, human vs tool, HW and subjective causal factors e.g. developers understanding) • Root cause analysis concept outline definition (no consolidated agreed definition) • Severity classifications for Linux kernel
- Phase 2:	Process specification • Sources of input (git,PASTA,email queries) • Qualification/know-how profile needs • Analysis steps and recording (formats) • Verification (review, community) • Impact estimation (metrics based on tools e.g. L2S)
- Phase 3:	Validation • Use historic events • Use-Case based severity (via HD3 analysis of Use-Case) • Impact probability (e.g. based on SIL2DB and define Use-Case) • Uncertainty estimation based on set of N analysis • Correlation of events with DLC metrics (e.g. DLCDM)
- Phase 4:	Verification • Historic event correction (yes/no, time delay, explanation) • Interviews (email) for the no cases, confirmation for the yes cases • Assessment of test-cases and/or tools used for testing of historic findings.

	• Testing of known (historic) cases: probability and severity (give use case) • Summary report on verification
-Go/NoGo:	Concept review with community members partner safety engineers and TueV • Review meeting 1 day workshop • Methodology, data and results • Go/no-go
- Phase 5	Dissemination (non-safety related use-case) • Community integration, root-cause process HOWTO and database • Selection on automated back-ports (e.g. AUTOSEL) • LWN articles on method, process and findings - potential life-cycle improvements.
- Phase 6:	Formal review meeting TueV and 1 day workshop • Mapping to 61508-3 life-cycle and Annex-A/B/C • 61508-7 specification of method • Relevant references review and summary • Update of process and evidence specification • Measure and techniques adjustments (SIL2LinuxMP context) • Integration into system safety monitoring process
- Phase 7:	Training material • Formalized root-cause analysis guidelines • Workshop on root-cause analysis (e.g. at Linux Plumbers) • Supplemental material to formal documentation (phase 5/6)
- Phase 8:	Application to target kernel environment • Selection of adequate random sample (target kernels and related) • Traceable root-cause analysis on sample (target would be at least 250) • Review of root-cause analysis (kernel developers and partner safety engineers) • Preliminary conclusions: severity, main causes, mitigations • Presentation to CA (TueV Rheinland) at workshop
Participation form:	
	• Project data repository • Project mailing lists (development, review) • Project case review meetings (e.g. IRC) • 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 • Implementation: (if tool support is seen necessary - currently not expected) • Certification Body: TueV Rheinland (proposed)
Effort estimation:	
	• TODO
Timeline:	
Start	March 1, 2019
Milestone 1	Concept and historic event review workshop (community event)
Milestone 2	Formal review meeting
Milestone 3	Minimal set of 250 defects analyzed for target kernel
Milestone 4	CA Report and all related artifacts published (public git)
Maintenance and continuous extension phase	
Project format:	
	Partner funded project (OSADL members)