OSEP working group updates

Paul Albertella, Codethink

ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

Aerospace · Automotive · Linux Features
Medical Devices · OS Engineering Process
Safety Architecture · Systems · Tools

Overview

- Introduction
- Key topics and activities in 2023
- Current focus and activities
- Opportunities for collaboration
- How to get involved

Working group introduction

- OSEP: *Open Source Engineering Process* working group
- Developing common processes and frameworks for ELISA
    - Establish a consistent framing / vocabulary for analysis and discussions
    - Develop safety analysis approaches and system models to enable comparison of results
    - Processes for drafting, reviewing and publishing results
- Have historically attempted to focus on safety analysis
    - What kind of *claims* do we want to make about Linux in the context of safety use cases?
    - How can we describe these safety use cases, and analyse the role that Linux plays in them?
    - Can we use this to derive a common set of safety requirements for Linux?
- Discussions are frequently more wide-ranging!
    - Processes, methodologies, technical topics, basis for safety claims, competency, etc

Key topics and activities in 2023

- Safety analysis process
  - In-context approach using STPA to define system context and safety requirements
  - Attempts to use methodology in Automotive and System Architecture working groups found STPA challenging to apply to Linux
  - Attempted to clarify intended purpose and approach to applying
  - https://github.com/elisa-tech/wg-osep/tree/main/safety-analysis
- Limitations of top-down analysis / STPA
  - Framing an argument at system-level only does not address some fundamental technical challenges with arguing in favour of Linux in safety systems
    - eg. Linux includes and supports many memory memory protection mechanisms and strategies, but kernel can theoretically corrupt any processes memory
  - Need to identify and understand these, and how they can impact a top-down argument

Current topics

- Why ‘proven in use’ arguments alone are insufficient for Linux
  - The fact that Linux is widely trusted in business-critical applications is not a sufficient basis for trusting it in safety-critical applications, or using the ‘proven in use’ argument in standards
  - Is there value in using this type of argument in another way?
  - See https://github.com/elisa-tech/wg-osep/pull/21 for current draft
- Linux ‘common safety issues list’
  - Document known limitations and/or potential weaknesses in the Linux kernel design or implementation, which must be considered as part of any safety analysis
  - See Igor Stoppa’s Systematic Approach to Using the Linux Kernel in a Safety Scenario [1] presentation for more details

[1] https://drive.google.com/file/d/1b37qOOHHixAbD3Cp9QosG3IYoxAQulMW/

Future topics

- Role of requirements specification
  - Specifying a verifiable set of applicable requirements for Linux (and other OS components) as the basis for safety arguments
  - Use of tools such as Basil (https://github.com/elisa-tech/BASIL) to support this
    - Developer of Basil (Luigi Pellecchia) joining OSEP call this week to discuss
- Review and publication of results
  - Establish common processes for creating, reviewing and publishing documents and diagrams describing results of ELISA workgroup discussions and analysis including:
    - Contribution guidelines, including use of GitHub
    - Review and approval process, including criteria to be used by reviewers
    - Publication process and format once accepted into mainline
  - Currently prototyping approaches in OSEP for current topic documents

Future topics *(continued)*

- Modelling safety role(s) of Linux in a system
  - Define a model for the role(s) that Linux might have in a safety-related system
  - Initial set of categories proposed
    - No role in any safety scenario, other than as a source of interference
    - Active role in a safety function, but no responsibility for ensuring that it is correct
    - Responsibility for some parts of a safety function or functions
    - Responsibility for all safety functions
- Modelling the behaviour of Linux as part of an OS
  - Define an abstract model for kernel functions in a Linux-based operating system, to provide a consistent framework for analysis and documentation of risk factors
    - See https://github.com/elisa-tech/wg-osep/pull/19 for first attempt
  - Combine with previous model of safety responsibilities assigned to Linux

Opportunities for collaboration

- Other open source communities applying safety and related processes
  - OSEP would welcome input from contributors to FOSS communities on this topic
  - e.g. Participants from Xen and SUSE have shared their experiences with Safety certification and ASPICE in previous ELISA workshops and seminars
- Linux system developers with insight into technical challenges
  - Contributions to ‘common safety issues list’ and documentation detailing challenges
- Other ELISA WGs
  - System WG: link their reference system to possible safety roles for Linux in a system
  - Automotive WG: build on their contribution workflow as basis for change review process

How to participate

Mailing List

You can subscribe to the OSEP mailing list at https://lists.elisa.tech/g/osep and read all of the messages at https://lists.elisa.tech/g/osep/messages

Weekly Meeting

The OSEP group meets on Thursdays at 14.00 (UK time). Please join the group and subscribe to the group's calendar https://lists.elisa.tech/g/osep/calendar to get the meeting details.

GitHub Repo

Please go to https://github.com/elisa-tech/wg-osep for additional details including current work led by this group and how to collaborate.

Any questions?

ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

Aerospace · Automotive · Linux Features · Medical Devices
OS Engineering Process · Safety Architecture · Systems · Tools

JOIN THE COMMUNITY

ELISA members are defining and maintaining a common set of elements, processes and tools that can be incorporated into specific Linux-based, safety-critical systems amenable to safety certification. ELISA is also working with certification authorities and standardization bodies in multiple industries to establish how Linux can be used as a component in safety-critical systems.

Join us to expand the use of Linux across new industries including healthcare, energy, transportation, and manufacturing. Learn more today to participate and support ELISA.

Join mailing lists

Participate in meetings

Contribute to documentations

Get involved in WGs

Collaborate at Workshops