

2025 - Zephyr Safety Working Group

2025 - Zephyr Safety Working Group

** For Table of Contents / Document outline, select the  button to the upper left

Resources

- [Safety Working Group · zephyrproject-rtos/zephyr Wiki](#)
- [Safety Working Group - Google Drive](#)
- [Working Group Project on GitHub](#)
- [Requirements Repo](#)
 - [Requirements that need work](#)
 - [Requirements Guideline](#)

Prior Years: Safety Working Group Meeting Minutes

-  **Zephyr Safety Working Group - Live Minutes - 2023**
-

Meeting Information

Ways to join meeting:

1. Join from PC, Mac, iPad, or Android

<https://zoom-lfx.platform.linuxfoundation.org/meeting/95140294824?password=a727e28d-fc7d-4ef5-bc2b-1f7e157931da>

2. Join via audio

One tap mobile:

US: +12532158782,,95140294824# or +13462487799,,95140294824

Or dial:

US: +1 253 215 8782 or +1 346 248 7799 or +1 669 900 6833 or +1 301 715 8592 or +1 312 626 6799 or +1 646 374 8656 or 877 369 0926 (Toll Free) or 855 880 1246 (Toll Free)

Canada: +1 647 374 4685 or +1 647 558 0588 or +1 778 907 2071 or +1 204 272 7920 or +1 438 809 7799 or +1 587 328 1099 or 855 703 8985 (Toll Free)

Meeting ID: 95140294824

Meeting Passcode: 158007

International numbers: <https://zoom.us/j/95140294824>

2 December 2025 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees

- Stephane Parenti, Nicole Pappler, Klaus Nagel, Kurokawa Harunobu, Olivier Charrier

Agenda / Notes

- WG Elections
 - [Working Group Elections · zephyrproject-rtos/zephyr Wiki](#)
 - Questions
 - Can non-collaborators be nominated?
 - Is a chair nominated by default or is a vote needed?
- Process definition
 -
 -
- Requirements status
 - Updated <https://github.com/zephyrproject-rtos/zephyr/issues/68005> with all components
 - Added E2E example scope [Safety End to End example: Queue · Issue #121 · zephyrproject-rtos/reqmgmt](#)
 - Closed Timers [Add and update Timer requirements by simhein · Pull Request #75 · zephyrproject-rtos/reqmgmt](#) since already merged

4 November 2025 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees

- Tobias Kästner, Wilson Chiu, Nicole Pappler, David Leach, Peter Christ, Stephane Parenti

Agenda / Notes

- Requirements through AI to get started)
 - Formal review/rework afterwards alleviates need for qualification
 - AI may also help standardize way of writing requirements/code

21 October 2025 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees

- Roberto Bagnara, Olivier Charrier, Tobias Kästner, Wilson Chiu, Nicole Pappler, Madan (Linumiz GmbH)
- Regrets: Stephane Parenti

Agenda / Notes

- Recap of last
- Walkthrough of open requirement PRs
 - PR#83: follow up with Matthew and the other commenter on the PR to solve the comments
- Update regarding the static analysis tool in the CI: contracts seem to be signed now, Roberto will follow up with the progress, there are also some PRs to update the Zephyr Coding Guidelines
- Tobias is in contact with Stan regarding updates of StrictDoc
- Nicole has finished the requirements checklist, will go into the PRs after the release
- Regarding architectural constraints of Zephyr:
 - Roberto is currently working on software architecture topics of Zephyr
 - Does it make sense to have a small working group working on software architecture? To have architectural constraints also defined?
 - We need to take as much from the actual architecture and design descriptions and create a software architecture based on that. But more constraints need to be written down, like “Zephyr is written in C with ... subset.”. So we can make sure the actual design is in line with the defined constraints.
 - We also need to make sure that whenever a component returns an error code this code is reacted to, or a reason is given why it is not used.
 - Tobias offers Roberto to follow up on the discussion to evaluate what Roberto found out and to have something to talk about with the maintainers

07 October 2025 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees

- Stephane Parenti, Olivier Charrier, David Leach, Wilson Chiu, Roberto Bagnara, Harunobu Kurokawa, Nicole Pappler, Daniel Costin
-

Agenda / Notes

- Stephane paused working on the process definition document, so the current state can be discussed with the community
 - List of processes includes:
 - An introduction
 - The content of the [safety overview](#) will be put into separate sections
 - There will be also chapters on more topics like skill management, quality management, change management etc.
 - Confirmation measures and safety manual will also go there
 - Document will be in draft to gather feedback
 - It has been recommended to involve the process working group meeting in this
- Meeting minutes and other topics will be more often sent via the mailing list
 - This will allow more people to get involved

23 September 2025 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees

- Stephane Parenti, Olivier Charrier, David Leach, Wilson Chiu
-

Agenda / Notes

- AI with requirements: Joel Key has tested it and it yielded some results that served as good inputs for human to rework

09 September 2025 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees

- Stephane Parenti, Peter Christ, Gautier Stier, Joel Key, Matthew Wood, Nelson Ferragut, Roberto Bagnara, Tobias Kästner, Wilson Chiu, Anas Nashif, Ollivier Charrier, Roman Kellner
-

Agenda / Notes

- Process progress: Stephane Parenti, Tobias Kästner and Nicole Pappler will focus in creating the processes
- Documentation of the processes will be published in the docs and created in Shinx
 - We are then requesting feedback from everyone
- Requirements will go on the back burner until the processes are published
- Exploring ways to measure test coverages during testing; also focusing on tools that can be used by HW vendors or other integrators
- Question by Matthew: will we have an example from requirements to architecture to design to implementation and test by the end of the year?
 - We will have one end to end example that the community can use and work with it
- Question by Matthew: Regarding the processes that we need to have ready by the end of the year? Is there any bandwidth to continue with requirements?
 - Stephane will focus on the processes
 - Nicole can do reviews, if there are contributions to the requirements repo
- Joel asking for feedback on his PRs. Matthew will do the reviews, asking Joel to send him the PRs.
- Stephane will ask Tracey to suspend the Requirements meeting until next year

12 August 2025 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees

- Stephane Parenti, Tobias Kastner, Madan, Peter Christ, Bharathiraja Nallathambi, David Brown, Saravanan Sekar, Verena Abt

Agenda / Notes

- Process progress
 - Ongoing work by Tobias on how and Stephane on what
 - FAQ
- Requirements
 - Merged LIFO and FIFO
- Gcov vs llvm-cov
 - Historical decision from when other tools were not available
 - Full support for targets and HW is still pending on llvm side
 - Llvm-cov qualification activities already started, so Zephyr may benefit from it
 - [\[RFC\] Proposal to establish a Safety Group in LLVM - Community - LLVM Discussion Forums](#)
 - [LLVM Qualification WG - July 2025](#)
- Scope
 - Does scope includes scheduler / interrupts / timers?
 - Scope is Kernel folder and some decisions still need to be made on additional scope items (scheduler)
 - [System Initialization Requirements · Issue #96 · zephyrproject-rtos/reqmgmt](#)
 - Clarification was made live that the idea is to write requirements that are then put in the safety manual for integrators to implement. The files would be used as examples and/or tool for test/QEMU pipeline
 -

Backlog Topics

- 29 July 2025
 - Explore idea of live WG meeting @ Amsterdam during OSS
 - Find coverage report and communicate to WG
 - Confirm with Anas/Architects if llvm-cov should be considered - During committee meeting 8/19
- 29 July 2025
 - Work with Anas to understand what tooling could support flagging PR as safety related to introduce the safety topic. Roll out and communication plan.
- 15 July 2025
 - ~~Clarify safety scope and document it in req. issue under a 2nd list until approved~~
 - ~~Stephane with contribution of other SMEs~~
 - Provide list of components and dependencies - Anas / other architect?

- 27 May 2025
 - Plan qualification of gcov, with partners (Xen, Elisa) if needed - Nicole ~July
- 20 May 2025
 - Contact testing working group for contribution to safety effort - Nicole ~June
- 22 April 2025
 - Confirm location and format of coding guidelines deviations - ~Nov
 - Work on e2e concept using 1 topic/function (e.g. queue) - ~Dec
- 8 April 2025
 - Discuss concept with Kate and Safety Committee on use of strictdoc for coverage and trace - Stephane
- 25 March 2025
 - Add a task in github for Tool evaluation completion - Stephane ~Aug
 - Consider reusing the safety plan list.
 - Consider removing list from safety plan and keeping it in tool evaluation list

Resources

None

29 July 2025 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees

- Stephane Parenti, Nicole Pappler, Tobias Kastner

Agenda / Notes

- Process progress
 - Loaded discussions ongoing on Architecture / Design
- OSS Europe Amsterdam
 - Booth, BOF, F2F @ 28 Aug.
- Requirements
 - Completed
 - Queue
 - Approved, pending SDOC update
 - Timer
 - FIFO
 - LIFO

- Pending review/rework
 - Scheduling
 - Mailbox
 - Task watchdog
 - Timer
 - Thread
 - Mutex
- Safety introduction
 - Community should be slowly introduced to the safety practices instead of a big bang approach, e.g.
 - Safety tag
 - Adding coding guidelines enforcement
 - Adding documentation enforcement
 - Etc...
- Impact on existing development speed
 - Modified and added activities will inevitably have an impact on work, if we want each release to be compliant/certified
 - The processes allow for releases to happen while not vetted for safety

Backlog Topics

- 29 July 2025
 - Work with Anas to understand what tooling could support flagging PR as safety related to introduce the safety topic. Roll out and communication plan.
- 15 July 2025
 - Clarify safety scope and document it in req. issue under a 2nd list until approved - Stephane with contribution of other SMEs
 - Provide list of components and dependencies - Anas / other architect?
- 27 May 2025
 - Plan qualification of gcov, with partners (Xen, Elisa) if needed - Nicole ~July
- 20 May 2025
 - Contact testing working group for contribution to safety effort - Nicole ~June
 - Add link in readme to the reqmgmt Wiki for safety WG - ~June
- 6 May 2025
 - ~~Confirm legal topics are closed between Bugseng and Linux foundation - ~May Tobias/Nicola~~
 - ~~Create a POC with Eclair binary distribution to confirm everything is working, with a simple PR/code - ~May~~
- 22 April 2025
 - Confirm location and format of coding guidelines deviations - ~June
 - Work on e2e concept using 1 topic/function (e.g. queue) - ~May
- 8 April 2025
 - Discuss concept with Kate and Safety Committee on use of strictdoc for coverage and trace - Stephane

- 25 March 2025
 - Add a task in github for Tool evaluation completion - Stephane 6 May
 - Consider reusing the safety plan list.
 - Consider removing list from safety plan and keeping it in tool evaluation list
- 11 March 2025
 - ~~Confirm what is blocking PRs~~ [Pull requests - zephyrproject-rtos/reqmgmt](#)
 - Propose architecture & design approach & POC
 - Architecture & Design guideline (Stephane)
 - 2 tasks “playing pingpong” to understand what needs to be in safety scope
 - AI to reverse engineer architecture

Resources

None

15 July 2025 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees

- Stephane Parenti, Wilson Chiu, Josek Tkadlec, Nicole Pappler, Harunobu Kurokawa, Gaku Inami

Agenda / Notes

- Progress
 - Plans/Process
 - Done
 - Initial GANTT with components list
 - Requirements
 - In progress / Review
 - Safety analysis
 - Quality management
 - Planning
 - Requirements
 - Completed
 - Queue
 - In progress / Review

- Timer
 - FIFO
 - LIFO
 - Scheduling
 - Mailbox
 - Task watchdog
 - Timer
 - Thread
 - Mutex
- Safety scope / Safety requirements
 - Consider discussion safety requirements within the working group call
 - Discuss complete

Backlog Topics

- 15 July 2025
 - Clarify safety scope and document it in req. issue under a 2nd list until approved - Stephane with contribution of other SMEs
 - Provide list of components and dependencies - Anas / other architect?
- 27 May 2025
 - Plan qualification of gcov, with partners (Xen, Elisa) if needed - Nicole ~July
- 20 May 2025
 - Contact testing working group for contribution to safety effort - Nicole ~June
 - Add link in readme to the reqmgmt Wiki for safety WG - ~June
- 6 May 2025
 - ~~◦ Confirm legal topics are closed between Bugseng and Linux foundation ~May Tobias/Nicola~~
 - ~~◦ Create a POC with Eclair binary distribution to confirm everything is working, with a simple PR/code ~May~~
- 22 April 2025
 - Confirm location and format of coding guidelines deviations - ~June
 - Work on e2e concept using 1 topic/function (e.g. queue) - ~May
- 8 April 2025
 - Discuss concept with Kate and Safety Committee on use of strictdoc for coverage and trace - Stephane
- 25 March 2025
 - Add a task in github for Tool evaluation completion - Stephane 6 May
 - Consider reusing the safety plan list.
 - Consider removing list from safety plan and keeping it in tool evaluation list
- 11 March 2025
 - ~~◦ Confirm what is blocking PRs [Pull requests - zephyrproject-rtos/reqmgmt](#)~~
 - Propose architecture & design approach & POC
 - Architecture & Design guideline (Stephane)

- 2 tasks “playing pingpong” to understand what needs to be in safety scope
- AI to reverse engineer architecture

Resources

None

01 July 2025 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees

- Peter Christ, Tobias Kästner, Benjamin Hlophe, Nicole Pappler, Nelson Ferragut

Agenda / Notes

- Nicole proposes to work on our review policies
 - Reviews are too detailed and aim for perfection
 - Reviewers should
 - Propose in-line suggest changes that the author can accept directly with a button click
 - Leave comments for things which should be fixed later (by opening issues)
 - Reviews should not be blocking coming
 - In an open source project we cannot afford to aim for perfection
 - If there are too many issues raised and the author is busy elsewhere than we are blocked again
 - However, we need
 - Peter mentioned that this was already been discussed, that we discussed that Quality Gates have to be passed, when a PR is accepted
 - We need to define, what needs to be done for a first QA Gate for a PR
 - We need to create an issue to ensure that open topics get addressed, even if it closed later.
 - A GitHub PR is not a final QA, at least not automatically
 - But if the lists of issues grow too long, it is pile of unfinished work that grows in front of us
 - We need to find a way to bring in unfinished PRs to be able to complete unfinished work
 - Do we have community authorship of PRs?

- That would mean we have a writable repo
 - Tobias checks about the writing access rights and a solution
-
- Where to write down our RQTs review guidelines
 - Requirements
 - There are currently several locations regarding guidelines for requirements and related work:
 - <https://github.com/zephyrproject-rtos/reqmgmt/wiki/Requirement-adding>
 - <https://github.com/zephyrproject-rtos/zephyr/wiki/Safety-Working-Group>
 - https://docs.zephyrproject.org/latest/safety/safety_requirements.html
 - We need to consolidate the location for requirements related guidelines and information
 - The starting point works from the safety working group landing page on GitHub
 - We can start working on the guidelines and how-tos in the req-repo wiki at <https://github.com/zephyrproject-rtos/reqmgmt/wiki/Requirement-adding> - and then move it, once we have it complete and want to move it somewhere else
- Stricterdoc update will introduce breaking changes
 - [SECTIONS] needs to become [[SECTIONS]] throughout the entire text base
 - Rationale: improve interoperability with Doxygen/REQIF
 - Several improvements for stricterdoc code base (behind the scenes)
 - Current version of stricterdoc (v0.9.1) issues a warning
 - Later versions will turn this into an error
 - PR93 already incorporates the required changes
 - <https://github.com/zephyrproject-rtos/reqmgmt/pull/93>
 - Need a dedicated PR for everything already in-tree
 - Action between Nicole, Stephan and Tobias
 - Need to decide case by case for the going PR
 - Stricterdoc office hours every Tue 5pm CET to meet with Stan for more information
 - <https://calendar.google.com/calendar/u/0/embed?src=9e52bdb79398efa1c138c5938a54d48918b2858a9564f7326477879ec27c34b3@group.calendar.google.com&ctz=Europe/Berlin>
- Safety Working Group project on GitHub:
 - Benjamin and Nelson need to get the rights to collaborate on it, they currently cannot assign a task/issue to themselves
 - <https://github.com/benjaminkutleng>
 - <https://github.com/NelsonFerragut>

- How do we ensure completeness regarding requirements and test coverage
 - Two options on the table right now, decision is pending
 - Use the Doxygen capabilities that are currently used at other places in the project
 - Use native StrictDoc functionality

Backlog Topics

- 20 May 2025
 - Plan qualification of gcov, with partners (Xen, Elisa) if needed - Nicole ~July
- 20 May 2025
 - Contact testing working group for contribution to safety effort - Nicole ~June
 - Add link in readme to the reqmgmt Wiki for safety WG - ~June
- 6 May 2025
 - Confirm legal topics are closed between Bugseng and Linux foundation - ~May Tobias/Nicola
 - Create a POC with Eclair binary distribution to confirm everything is working, with a simple PR/code - ~May
- 22 April 2025
 - Confirm location and format of coding guidelines deviations - ~June
 - Work on e2e concept using 1 topic/function (e.g. queue) - ~May
- 8 April 2025
 - Discuss concept with Kate and Safety Committee on use of strictdoc for coverage and trace - Stephane 20 May
- 25 March 2025
 - Add a task in github for Tool evaluation completion - Stephane 6 May
 - Consider reusing the safety plan list.
 - Consider removing list from safety plan and keeping it in tool evaluation list
- 11 March 2025
 - ~~Confirm what is blocking PRs~~ [Pull requests - zephyrproject-rtos/reqmgmt](#)
 - Propose architecture & design approach & POC
 - Architecture & Design guideline (Stephane)
 - 2 tasks “playing pingpong” to understand what needs to be in safety scope
 - AI to reverse engineer architecture

Resources

None

17 June 2025 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees

Stephane Parenti, Tobias Kastner, Nicole Pappler, Rob Woolley, Anas Nashif, David Brown, Simon Hein

Agenda / Notes

- Requirements workshop & progress
 - In progres, working in closed group
- Architecture & Components guideline
 - Only getting started, should hear more in coming weeks
- Code coverage / Coding guidelines
 - <https://app.codecov.io/gh/zephyrproject-rtos/zephyr>
 - <https://github.com/zephyrproject-rtos/zephyr/actions/runs/15699979763/artifacts/3342805796>
 - Technical debt on coverage will need to be looked at sooner rather than later. Report already in place
 - Coding guidelines details will be worked on once the pipeline is in place, with staged deployment
 - Pipeline report
 - Guidelines enforcement for modified/added code
 - Guideline enforcement for legacy code
- Coverage tool qualification: gcov
 - ISO 26262 / IEC 61508 only required tool development process and proven in use argument
 - Additional requirements & validation can be performed to enhance confidence in tool
 - Many companies are providing coverage tools, we may use any of these tools if the pipeline enables them

Backlog Topics

- 20 May 2025
 - Plan qualification of gcov, with partners (Xen, Elisa) if needed - Nicole ~July
- 20 May 2025
 - Contact testing working group for contribution to safety effort - Nicole ~June
 - Add link in readme to the reqmgmt Wiki for safety WG - ~June
- 6 May 2025
 - Confirm legal topics are closed between Bugseng and Linux foundation - ~May Tobias/Nicola
 - Create a POC with Eclair binary distribution to confirm everything is working, with a simple PR/code - ~May
- 22 April 2025
 - Confirm location and format of coding guidelines deviations - ~June
 - Work on e2e concept using 1 topic/function (e.g. queue) - ~May
- 8 April 2025
 - Discuss concept with Kate and Safety Committee on use of strictdoc for coverage and trace - Stephane 20 May
- 25 March 2025
 - Add a task in github for Tool evaluation completion - Stephane 6 May
 - Consider reusing the safety plan list.
 - Consider removing list from safety plan and keeping it in tool evaluation list
- 11 March 2025
 - ~~Confirm what is blocking PRs~~ [Pull requests - zephyrproject-rtos/reqmgmt](#)
 - Propose architecture & design approach & POC
 - Architecture & Design guideline (Stephane)
 - 2 tasks “playing pingpong” to understand what needs to be in safety scope
 - AI to reverse engineer architecture

Resources

None

3 June 2025 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees

Stephane Parenti, Harunobu Kurokawa, Andres Schuster, Benjamin Engels, Anas Nashif, Benjamin Hlophe, Roberto

Agenda / Notes

- Requirements workshop & progress
 -
- Architecture & Components guideline

Backlog Topics

- 20 May 2025
 - Contact testing working group for contribution to safety effort - Nicole ~June
 - Add link in readme to the reqmgmt Wiki for safety WG - ~June
- 6 May 2025
 - Confirm legal topics are closed between Bugseng and Linux foundation - ~May Tobias/Nicola
 - Create a POC with Eclair binary distribution to confirm everything is working, with a simple PR/code - ~May
- 22 April 2025
 - Confirm location and format of coding guidelines deviations - ~June
 - Work on e2e concept using 1 topic/function (e.g. queue) - ~May
- 8 April 2025
 - Discuss concept with Kate and Safety Committee on use of strictdoc for coverage and trace - Stephane 20 May
- 25 March 2025
 - Add a task in github for Tool evaluation completion - Stephane 6 May
 - Consider reusing the safety plan list.
 - Consider removing list from safety plan and keeping it in tool evaluation list
- 11 March 2025
 - Confirm what is blocking PRs [Pull requests · zephyrproject-rtos/reqmgmt](#)
 - Propose architecture & design approach & POC
 - Architecture & Design guideline (Stephane)
 - 2 tasks “playing pingpong” to understand what needs to be in safety scope
 - AI to reverse engineer architecture

Resources

None

20 May 2025 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees

Stephane Parenti, Klaus Nagel, Peter Christ, Joel Key, Rob Woolley, Emilio Benavente, Nicola Vetrini, Tobias Kastner, Anas Nashif, David Leach, Nelson Ferragut

Agenda / Notes

- Requirements workshop & progress
 - [Safety Working Group · zephyrproject-rtos/zephyr Wiki](#)
- Progress on tooling
 - Testing working group is seeking collaboration
 - Team is going through test strategy and needs for other activities in project are covered. Need buy in from safety group for required artifacts as well as look at infrastructure (negative testing, traceability, coverage)
- Architecture & Components guideline

Backlog Topics

- 20 May 2025
 - Contact testing working group for contribution to safety effort - Nicole ~June
 - Add link in readme to the reqmgmt Wiki for safety WG - ~June
- 6 May 2025
 - Confirm legal topics are closed between Bugseng and Linux foundation - ~May Tobias/Nicola
 - Create a POC with Eclair binary distribution to confirm everything is working, with a simple PR/code - ~May
- 22 April 2025
 - Confirm location and format of coding guidelines deviations - ~June
 - Work on e2e concept using 1 topic/function (e.g. queue) - ~May
- 8 April 2025
 - Discuss concept with Kate and Safety Committee on use of strictdoc for coverage and trace - Stephane 20 May
- 25 March 2025
 - Add a task in github for Tool evaluation completion - Stephane 6 May

- Consider reusing the safety plan list.
 - Consider removing list from safety plan and keeping it in tool evaluation list
- 11 March 2025
 - Confirm what is blocking PRs [Pull requests · zephyrproject-rtos/reqmgmt](#)
 - Propose architecture & design approach & POC
 - Architecture & Design guideline (Stephane)
 - 2 tasks “playing pingpong” to understand what needs to be in safety scope
 - AI to reverse engineer architecture

Resources

None

6 May 2025 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees

Stephane Parenti, Klaus Nagel, Peter Christ, Joel Key, Rob Woolley, Emilio Benavente, Nicola Vetrini, Tobias Kastner, Anas Nashif, David Leach, Nelson Ferragut

Agenda / Notes

- Requirements workshop & progress
 - Issues & Assignment: Comment it!
- Progress on tooling
 - Working on how to get the Eclair tool rolled out. May go in a Docker image (would need private registry). Tool is 300-350mb. Let's start with that and optimize later. There may be a conflict with already existing Docker.
 - CI is all done in Kubernetes clusters. License server should ideally be in a pod in that cluster.
 - License is needed for both scanning and reporting.
- Architecture guideline
 - Project documentation shall be reused and enhanced as much as possible
 - Ideal situation would be to have both safety and non-safety architectural items at same location to get the whole story
 - Safety analyses feed back into architecture to close safety gaps in the architecture

Backlog Topics

- 6 May 2025
 - Confirm legal topics are closed between Bugseng and Linux foundation - ~May Tobias/Nicola
 - Create a POC with Eclair binary distribution to confirm everything is working, with a simple PR/code - ~May
- 22 April 2025
 - Confirm location and format of coding guidelines deviations - ~June
 - Work on e2e concept using 1 topic/function (e.g. queue) - ~May
- 8 April 2025
 - ~~○ Work with Tobias to get rights to assign people to issues for requirements - Stephane 15 April - DONE~~
 - Discuss concept with Kate and Safety Committee on use of strictdoc for coverage and trace - Stephane 20 May
- 25 March 2025
 - ~~○ Reschedule Thursdays 4pm to 6pm Berlin time - Stephane 3rd April - DONE~~
 - ~~○ Find tool spreadsheet and reuse information if possible - All committee members 1st April - DONE~~
 - Add a task in github for Tool evaluation completion - Stephane 6 May
 - Consider reusing the safety plan list.
 - Consider removing list from safety plan and keeping it in tool evaluation list
- 11 March 2025
 - Confirm what is blocking PRs [Pull requests · zephyrproject-rtos/reqmgmt](#)
 - Propose architecture & design approach & POC
 - Architecture & Design guideline (Stephane)
 - 2 tasks “playing pingpong” to understand what needs to be in safety scope
 - AI to reverse engineer architecture
 - ~~○ Tool classification and evaluation template proposal (Stephane) DONE~~
- 25 Feb 2025
 - Have teams assigned to the work to be done within [Add Requirements for the Zephyr project · Safety WG](#) or on other documents identified in XLS file

Resources

None

22 April 2025 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees

Stephane Parenti, Wilson Chiu, Tobias Kastner, Steve Lazzeri, Nicola Vetrini, Matthew Wood, Masanori Itoh, Joel Key, Harunobu Kurokawa, Emilio Benavente, David Leach, Anas Nashif, Nicole Pappler, Roman Kellner, Rob Woolley

Agenda / Notes

- Requirements workshop & progress
 - Issues & Assignment: Comment it
 - Fwd/Back trace: Strictdoc can now trace without code tags
 - Requirements scope
 - [Kernel — Zephyr Project Documentation](#)
 - More files/components need to be added to the scope of Zephyr
 - The above list could be used as baseline as well as source for architecture documentation and scope
- Architecture guideline

Backlog Topics

- 22 April 2025
 - Confirm location and format of coding guidelines deviations - ~June
 - Work on e2e concept using 1 topic/function (e.g. queue) - ~May
- 8 April 2025
 - ~~◦ Work with Tobias to get rights to assign people to issues for requirements~~
Stephane 15 April - DONE
 - Discuss concept with Kate and Safety Committee on use of strictdoc for coverage and trace - Stephane 20 May
- 25 March 2025
 - ~~◦ Reschedule Thursdays 4pm to 6pm Berlin time~~ - Stephane 3rd April - DONE
 - ~~◦ Find tool spreadsheet and reuse information if possible~~ - All committee members 1st April - DONE
 - Add a task in github for Tool evaluation completion - Stephane 6 May
 - Consider reusing the safety plan list.
 - Consider removing list from safety plan and keeping it in tool evaluation list
- 11 March 2025
 - Confirm what is blocking PRs [Pull requests · zephyrproject-rtos/reqmgmt](#)
 - Propose architecture & design approach & POC
 - Architecture & Design guideline (Stephane)
 - 2 tasks “playing pingpong” to understand what needs to be in safety scope
 - AI to reverse engineer architecture
 - ~~◦ Tool classification and evaluation template proposal (Stephane)~~ DONE

- 25 Feb 2025
 - Have teams assigned to the work to be done within [Add Requirements for the Zephyr project · Safety WG](#) or on other documents identified in XLS file

Resources

None

8 April 2025 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees

Stephane Parenti, Joel Key, Masanori Itoh, Nelson Ferragut, Stanislav Pankevich, Steve Lazzeri, Wilson Chiu, Emilio Benavente, Marcus Hahnel, Roman Kellner, Sudan Landge, Rob Woolley, Roberto Bagnara, Mike Skrtic, Klaus Nagel

Agenda / Notes

- Requirements workshop group: Dates/Time and objectives
 - https://docs.google.com/document/d/1rd6BitpAoxQ6WCCNv4aoT4HuGprVY0Et4yNJeb6i-AQ/edit?usp=drive_link
 - <https://zoom-lfx.platform.linuxfoundation.org/meeting/98731002652?password=ffc181c1-aa15-4333-9c77-379f4aec7608>
- Tool criteria evaluation report: Scope & completion
- Documents & Extracts to be made available to the public for contribution
 - List of all artifacts, location & scope of share
- GANTT breakdown into issues
- Coverage report (statement, branch, function and MCDC) and document the coverage gap (justifying why there is a gap) (as sent by Ayan Kumar Halder)
 - Existing tools and practices
 - Documented in separate document like coverage report or component document itself
 - Proposed approach
 - Other tooling was proposed by Anas to enable traceability between gaps & other artifacts
 - Stanislav StrictDoc proposal
[@ 33min08sec](https://zoom.us/rec/share/AAYI8E5PTBb6_Lje2RWaC3mIX9RtZ4YQbg1tRDEAvxAgg45apA8RDL-TiIMJLz7B.hylEUuVynxVmQRcv)

Backlog Topics

- 8 April 2025
 - Work with Tobias to get rights to assign people to issues for requirements - Stephane 15 April
 - Discuss with Kate and Safety Committee on use of strictdoc for coverage and trace - Stephane 15 April
- 25 March 2025
 - ~~○ Reschedule Thursdays 4pm to 6pm Berlin time - Stephane 3rd April - DONE~~
 - ~~○ Find tool spreadsheet and reuse information if possible - All committee members 1st April - DONE~~
 - Add a task in github for Tool evaluation completion - Stephane 1st April
 - Consider reusing the safety plan list.
 - Consider removing list from safety plan and keeping it in tool evaluation list
- 11 March 2025
 - Confirm what is blocking PRs [Pull requests · zephyrproject-rtos/reqmgmt](#)
 - Propose architecture & design approach & POC
 - Architecture & Design guideline (Stephane)
 - 2 tasks “playing pingpong” to understand what needs to be in safety scope
 - AI to reverse engineer architecture
 - ~~○ Tool classification and evaluation template proposal (Stephane) DONE~~
- 25 Feb 2025
 - Have teams assigned to the work to be done within [Add Requirements for the Zephyr project · Safety WG](#) or on other documents identified in XLS file

Resources

None

25 March 2025 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees

Stephane Parenti, Klaus Nagel, Nicole Pappler, Joel Key, Rob Woolley, Peter Christ, Roman Kellner, Tobias, Emilio Benavente, Olivier Charrier, Nicola Vetrini, Roberto Bagnara

Agenda / Notes

- Respawning the requirements workshop group
- Reviewing a proposed tool evaluation/classification matrix
 - [Tool Criteria Evaluation Report - Google Sheets](#)
 - Zephyr will be using the ISO 26262 way of evaluating and qualifying tools
 - https://docs.google.com/spreadsheets/d/12DBzOCXW3vUJc1cfnA5AIK_JldCKgUclKfuO3jeFlqM/edit?usp=sharing
- Scope of safety: Does it include user space?
 - For most target arch for Zephyr, no MMU so no virtual memory / isolation
 - How to deal with the K config matrix / cases? Restrict configuration set
- Requirement PR from Joel using Perplexity
 -

Backlog Topics

- 25 March 2025
 - Reschedule Thursdays 4pm to 6pm Berlin time - Stephane 3rd April
 - Find tool spreadsheet and reuse information if possible - All committee members 1st April
 - Add a task in github for Tool evaluation completion - Stephane 1st April
 - Consider reusing the safety plan list.
 - Consider removing list from safety plan and keeping it in tool evaluation list
- 11 March 2025
 - Confirm what is blocking PRs [Pull requests · zephyrproject-rtos/reqmgmt](#)
 - Propose architecture & design approach & POC
 - Architecture & Design guideline (Stephane)
 - 2 tasks “playing pingpong” to understand what needs to be in safety scope
 - AI to reverse engineer architecture
 - ~~Tool classification and evaluation template proposal (Stephane)~~ DONE
- 25 Feb 2025

- Have teams assigned to the work to be done within [Add Requirements for the Zephyr project · Safety WG](#) or on other documents identified in XLS file

Resources

- None

11 March 2025 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees

Matthew Wood, Stephane Parenti, Klaus Nagel, Roman Kellner, Joel Key, David Leach, Harunobu Kurokawa, Nelson Ferragut, Emilio Benavette, Olivier Charrier

Agenda / Notes

- Architectural approaches
 - Start with requirements then model components and 4+1 view
 - Graphviz to reverse engineer from code <http://graphviz.org/>
 - Plugins / Scripts to parse DB and suggest SW architecture representation
- Define safety scope for Zephyr and then propose rationale for FFI
 - Use 2 tasks “playing pingpong” to understand what needs to be in safety scope and what would not be in safety scope
- Using AI tool to reverse engineer architecture
 - Consider pointer tool to code repository

Backlog Topics

- 11 March 2025
 - Confirm what is blocking PRs [Pull requests · zephyrproject-rtos/reqmgmt](#)
 - Propose architecture & design approach & POC
 - Architecture & Design guideline (Stephane)
 - 2 tasks “playing pingpong” to understand what needs to be in safety scope
 - AI to reverse engineer architecture
 - Tool classification and evaluation template proposal (Stephane)
- 25 Feb 2025
 - Have teams assigned to the work to be done within [Add Requirements for the Zephyr project · Safety WG](#) or on other documents identified in XLS file

Resources

- None

25 February 2025 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees

Klaus Nagel, Marcus Haehnel, Harunobu Kurokawa, Stephane Parenti, Wilson Chiu, Peter Christ, David Leach, Nicole Pappler, Nelson Ferragut, Bud Caldwell, Kate Stewart, Roberto Bagnara

Agenda

- Opens
- Discussion: Missing information and planning documents - working group perspective
 - Status of Requirements, to have an overview and to be able to comment
 - Action item Nicole Pappler : look for the requirements status spreadsheet that Kate started.
 - Original top level requirements spreadsheet. → [all in github](#) at this point.
 - Add a link to the working group wiki where people can access the documents and things that needs work done; AI Nicole Pappler
 - Add a link to this document with information needed to start / work
- Stephane looking into tools to reverse engineer the architecture, looking for a second to try as well.
 - Considering getting a high level architecture, but then map out the safety scope as a subset for the argumentation with Tuev.

Backlog Topics:

- Topic in two weeks: have teams assigned to the work that needs to be done

Resources

- <https://github.com/orgs/zephyrproject-rtos/projects/23>

11 February 2025 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees:

Klaus Nagel, Loic Domaigne, Stephane Parenti, Tobias Kästner, Peter Christ, David Leach, Bud Caldwell, Olivier Charrier, Nelson Ferragut, Anas Nashif, Wilson Chiu, Nicole Pappler, Kate Stewart

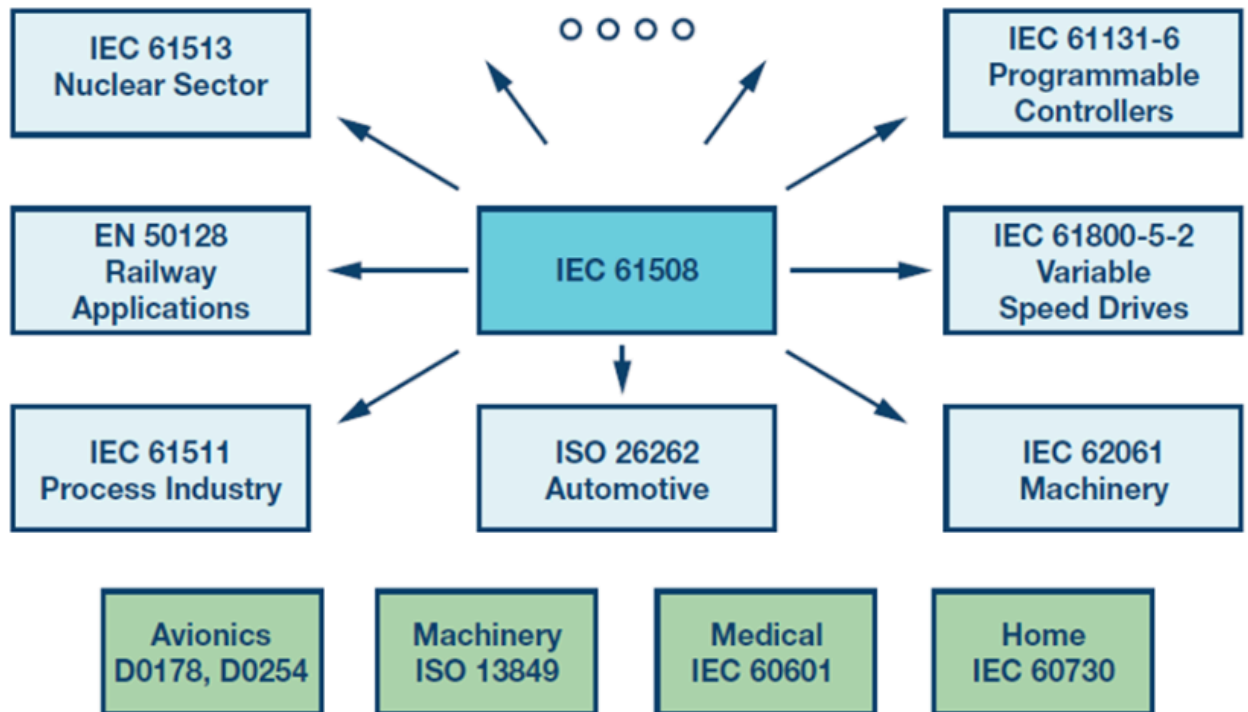
Agenda:

- Opens
 - None

Notes:

- A warm welcome to the first time joiners
 - Olivier and Stephane are from Windriver
 - Loic also joined for the first time
- Tobias gave a brief overview on how the safety working group is organized
- Certification goal is IEC 61508 SIL3. Route 3s has been chosen to reach that goal.
- Nicole acts as a safety advisor for the Project
- The position of the safety architect is still open. The safety chair has been taken from Matt from Cariad.
- TÜV SÜD (located in Germany) is our assessor for the safety certification
- Tobias explained that still a lot of requirements have to be created
- A first report from the TÜV certifies that we are on the right track.
- The deadline for an initial certified version cannot currently be guaranteed.
- The related documentation is currently available to platinum members only.
- Feedback from the participants: It is hard to contribute to the safety group if the TÜV documents are not publicly available.
- Nicole: It should be examined whether at least the safety plan can be made publicly available.
- Note from Bud: Since this is an out-of-context development, we need to understand any top-level safety goals, assumptions of use, and the technical safety concept. It's easy enough for experts in Zephyr to define non-safety requirements, but we need this information to define safety requirements.
- Anas: We should start working on safety topics (e.g. requirements) and stop discussing membership levels or other stuff
- Nicole:
<https://github.com/orgs/zephyrproject-rtos/projects/23?pane=issue&itemId=28916071&issue=zephyrproject-rtos%7Czephyr%7C68005>

- Tobias gave an update to the open Pull Requests:
<https://github.com/zephyrproject-rtos/reqmgmt/pulls>
- Finally, Nelson added PR #81. This is a further step in accordance with the previously presented and discussed approaches for implementing a watchdog controller. It is a new requirement to Zephyr. It is required by the standard for “home appliances” used by Whirlpool and therefore necessary for them.
- IEC 61508 was selected because it is a basic standard for other specific functional safety standards and there is a large intersection with other functional safety standards.



Source: <https://www.eeworldonline.com/embedded-basics-iec-61508-functional-safety-mcus-part-1-faq/>

-

Backlog Topics:

none

Resources

none

28 January 2025 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees:

Klaus Nagel, Roberto Bagnara, David Leach, Marcus Haehnel, Peter Christ, Tobias Kästner, Roberto Woolley, Bud Caldwell, Wilson Chiu

Agenda:

- Opens
 - none

Notes:

- Marcus and Bud introduced themselves as new members in the safety working group
- FYI: There are two regular meetings regarding safety aspects: Safety working group (open to everyone) and safety committee (for Zephyr Project platinum members)
- Currently the charter gives voting rights to the chair of a working group. This was not a problem in the past, since the chair was always from a platinum member. This has to be clarified. Maybe the charter has to be changed.
- The safety chair and architect are still vacant.
- David posted a link into the chat with all working groups:
<https://github.com/zephyrproject-rtos/zephyr/wiki/Zephyr-Committee-and-Working-Groups>
- Note from Tobias: The Discord channels are a good starting point to get in contact with other persons in the Zephyr context.
- Tobias showed the github website with open pull requests related to the safety requirements, <https://github.com/zephyrproject-rtos/reqmgmt/pulls>
Currently there are five open PRs.
- PR #77: <https://github.com/zephyrproject-rtos/reqmgmt/pull/77>
Is related to the Zephyr condition variables API:
https://docs.zephyrproject.org/apidoc/latest/group__condvar__apis.html
- Tobias gave a brief introduction on how to do a review in github on the pull requests.

- To create StrictDoc documents (HTML or PDF), the needed tools have to be installed on your local PC. This makes it much easier to read the documents, instead of reading the strict doc files
- The ownership of the PRs in github shall be clarified. Currently they belong to Simon.
- There are still some APIs to be specified, currently approx 6 out of 20 have been defined.
- TODO: There were no further comments on the PRs, so they can be merged.
- The maintainers of Zephyr can be asked to do a review on the requirements, if needed.
- The tool used for requirements engineering (StrictDoc) has been chosen to make it available to anyone interested in contributing to the safety working group.

Backlog Topics:

none

Resources

none

14 January 2025 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: Klaus Nagel, Tobias Kaestner, Marcus Haehnel, David Leach, Kate Stewart, Peter Christ, Nelson Ferragut, Roman Kellner, Wilson Chiu, Yves V, Nicole Pappler, Emilio Benavente

Agenda

- Opens
 - Status of the fault manager / fault management mechanisms
 - Where is help needed on Requirements traceability, where do we have linkage, where do we need more
- Project Status, Phase 1 complete
- Nominations for Safety Chair and Safety Architect

Notes

- Concept report with the concept approval has been delivered by TUV;
 - would be good to have a blog post about it
 - Is SMP in the scope? Yes.
 - Has there been mixed criticality considered in the scope? Not within the scope, as everything in the scope is handled to the highest criticality. FFI to the outside of the scope will be analysed in the software safety analysis; measures that need to be taken by the integrator will be mentioned in the safety manual
- Safety Chair and Safety Architect nomination
 - Simon cannot continue in his roles for 2025, therefore we need new nominees
 - Roles:
 - The Chair is responsible for running the meetings
 - The Architect is responsible for the technical direction and interfacing with the board
 - People for these roles should be from a project member organisation
- Fault Management Mechanisms:
 - Nelson suggests not to follow what has initially been proposed
 - Instead, pulling the task watchdog into the scope of safety
 - It does what has been proposed
 - And it does it better
 - David proposes to go on on the initial proposal, but shift the discussion to the new solution, so we won't lose the history
 - Initial commit of task watchdog was done by Martin Jaeger, Tobias tries to pull him into one of the next meetings
 - As the task watchdog is not in the kernel folder, we need to make an informed decision about it.

- Nelson will create initial requirements
- Update on requirements and traceability
 - Open PRs need to be reviewed, approved and then merged
 - If there are no new comments, we will merge them in two weeks
 - If there are no negative comments, please just approve them and they it looks good for you
 - [Requirements Guideline](#)
 - [Requirements Repo](#)
 - We are capturing requirements for the code/design as is, not adding new requirements for new functionality
- Fosdem channel:
<https://discord.com/channels/720317445772017664/1288551270822445066>

Backlog Topics:

- How can we gather all the reports in github

Resources

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req Focus Group:
 - [Zephyr Requirements Focus Group - Live Minutes - 2024](#)
- Overview: https://docs.zephyrproject.org/latest/safety/safety_overview.html
- Requirement guidelines: <https://docs.z>

2024 - Zephyr Safety Working Group

2024 - Zephyr Safety Working Group

** For Table of Contents / Document outline, select the  button to the upper left

Resources

- [Safety Working Group - Google Drive](#)
- [Working Group Project on GitHub](#)
- [Requirements Repo](#)
 - [Requirements that need work](#)
 - [Requirements Guideline](#)

Prior Years: Safety Working Group Meeting Minutes

- [2023](#)
-

Meeting Information

Ways to join meeting:

1. Join from PC, Mac, iPad, or Android

<https://zoom-lfx.platform.linuxfoundation.org/meeting/95140294824?password=a727e28d-fc7d-4ef5-bc2b-1f7e157931da>

2. Join via audio

One tap mobile:

US: +12532158782,,95140294824# or +13462487799,,95140294824

Or dial:

US: +1 253 215 8782 or +1 346 248 7799 or +1 669 900 6833 or +1 301 715 8592 or +1 312 626 6799 or +1 646 374 8656 or 877 369 0926 (Toll Free) or 855 880 1246 (Toll Free)

Canada: +1 647 374 4685 or +1 647 558 0588 or +1 778 907 2071 or +1 204 272 7920 or +1 438 809 7799 or +1 587 328 1099 or 855 703 8985 (Toll Free)

Meeting ID: 95140294824

Meeting Passcode: 158007

International numbers: <https://zoom.us/j/95140294824>

17 December 2024 - Zephyr Project Safety WG - Canceled

03 December 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: Anas Nashif, Niola Pappler, Peter Christ, Tobias Kaestner, Simon Hein, Klaus Nagel, Nelson Ferragut, Wilson Chiu, Matthew Wood, David Leach, Emilio Benavente, Rajesh Muraleenharan

Meeting Recording:

OOO:

Simon Hein: 18.12.2024 - 06.01.2025

Agenda:

- Opens
 - Cancel WG meetings in the holiday season
 - Simon will cancel them
- Safety WG Elections - Election / wrap-up
 - <https://github.com/zephyrproject-rtos/zephyr/wiki/Working-Group-Elections>
 - There are no objections from the present nominees to the proposed list
 - Tobias Kästner will be co-chair of the group
 - The list will be updated accordingly
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Eclair tool integration is set to Done
 - Simon gave an update on the tasks to the board, the list will be filled with more details by Simon within the next weeks
- Fault detection
 - <https://github.com/zephyrproject-rtos/zephyr/issues/80938>
 - This GitHub issue links to the Google Doc with more information
 - Regarding the requirements coverage, there is currently no information about the current coverage, but it needs to be provided in the end (contributions highly welcomed by Simon); clarification: the Macros in the Document needs requirements behind them
 - Safety Checks might or will be application specific, but the record/surveyor area might be something that can be provided by Zephyr

- Regarding the amount of Macros in Zephyr, Matt mentioned that it will get more difficult for safety the more we have in the safety scope there
- The context of what Nelson describes in this RFQ is also applicable to other verticals, as also confirmed by Matt for the automotive
- For the safety confirmation, Zephyr would need to guarantee that these safety checks are running
- David suggests to flush out the requirements for Surveyor and Run Record so people can start implementing the code for it
- This will be a change to the Zephyr Safety Scope, as it will add on to the existing Safety Concept
- AI-Simon: Propose a Problem Description
- Regarding the competence management discussion from the previous meeting
 - Competences per role were discussed last week
 - Matt proposes he can add competence information to the roles that are already defined
 - From the discussion with the assessor last Friday: it has been discussed that we can use the existing safety documentation as evidence for gained expertise
 - Common sense that a training would not help with all of this people will just make the training and it wouldn't change anything
 - Matthew will work with Simon and Nicole on a solution.

Notes:

- Tobias is asking if there is more need for onboarding information by Cariad; according to Matt there is currently no need; Note from Tobias, that there can always be a follow up on the onboarding meeting.

Backlog Topics:

- How can we gather all the reports in github
-

Resources

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req Focus Group:
 - [Zephyr Requirements Focus Group - Live Minutes - 2024](#)
- Overview: https://docs.zephyrproject.org/latest/safety/safety_overview.html

- Requirement guidelines:
https://docs.zephyrproject.org/latest/safety/safety_requirements.html

19 November 2024 - Zephyr Project Safety WG - Canceled

05 November 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees:

Meeting Recording:

https://zoom.us/rec/share/LO9LOv-t7H_Jj_mSpd46TRuI_24thrFca7j3WMJqj1RX-NZeI2R-3GbREca-22c.BYCca8lv4QSuWrNL

OOO:

Agenda:

- Opens
- Working groupe cadence
 - Bi-weekly cadence because of safety committee meeting
- Safety WG Elections - Election / wrap-up
 - <https://github.com/zephyrproject-rtos/zephyr/wiki/Working-Group-Elections>
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Fault detection

Notes:

- Opens
 - No opens
- Working groupe cadence
 - The Cadence changed to Bi-weekly
- Safety WG Elections - Election / wrap-up
 - Election is postponed because the co-chair spot is not filled.

- Tobias volunteered and step up as co chair but needs to clarify it with his manager
- Safety WG Project
 - No progress in the safety WG Project
- Fault detection
 - Nelson presented the status of his RFC for a Fault detection layer
 - The general question was how we can collaborate on defining a RFC for the fault detection layer
 - David Leach proposed to start out with a documentation and link the working document into the issue to track it in the project and get the proposal to a full RFC to present it the community and the needed working groups
 - Consensus of the group was reached to process as discussed
 - Document Link: [RFC_Fault_Detection.md](#)
 - Issue: <https://github.com/zephyrproject-rtos/zephyr/issues/80938>

Backlog Topics:

- How can we gather all the reports in github
-

Resources

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req Focus Group:
 - [Zephyr Requirements Focus Group - Live Minutes - 2024](#)
- Overview: https://docs.zephyrproject.org/latest/safety/safety_overview.html
- Requirement guidelines: https://docs.zephyrproject.org/latest/safety/safety_requirements.html

22 October 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: Wilson Chiu, Matthew Wood, Nelson Ferragut, Mehul sagar, Simon Hein, Roman Kellner, Emilio Benavente, Yves Vandervennet

Meeting Recording:

https://zoom.us/rec/share/L152RFGrhTkWUaWK7DP3YHBO6FqSJILzW9X5dWeo8YPaUpuabApf0Oo3NnwZ3FTr.HpEeK8qMjekLQcg_

OOO:

Agenda:

- Opens
 - Reminder:
<https://github.com/zephyrproject-rtos/zephyr/wiki/Working-Group-Elections>
 - Next Week WG Meeting canceled because of the committee meeting
 - Attention: Time change in europe (All meetings are 1 hour)
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - <https://github.com/zephyrproject-rtos/zephyr/tree/collab-safety>
 -

Notes:

- Opens
 - Reminder elections:
 - Simon reminded participants about the upcoming **Safety Working Group elections**.
 - A link was shared for those interested in nominating themselves, with a deadline set for the following week.
 - Safety WG meeting:
 - A **Safety Committee meeting** is scheduled at the same time as the usual Safety Working Group meeting, leading to the cancellation of next week's working group meeting.
- Safety WG Project

Backlog Topics:

- How can we gather all the reports in github
-

Resources

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req Focus Group:
 - [Zephyr Requirements Focus Group - Live Minutes - 2024](#)

- Overview: https://docs.zephyrproject.org/latest/safety/safety_overview.html
- Requirement guidelines: https://docs.zephyrproject.org/latest/safety/safety_requirements.html

15 October 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: Simon Hein, Nicole Pappler, Tobias Kästner, Wilson Chiu, Emilio Benavente, Klaus Nagel, Matthew Wood, Peter Christ, Roman Kellner, Sumitabh Ghosh, Vinoth Kumar, Yves Vandervennet, Kate Stewart

Meeting Recording:

https://zoom.us/rec/share/CTLfxpnL3L7w36_veHU-VwFRg3lKeY005qF7lm72XBF77uJjXCMN_I5S5hW1LnDr.rAHebLp-CPGTy_FV

OOO:

Agenda:

- Opens
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Simon Hein: simhein
- Working group nominations: <https://lists.zephyrproject.org/g/devel/message/9628>
 - Kate raised that this criteria is specific to TSC hosted WG, and may not be appropriate for the Safety WG Core team.
- Fault detection
 - Example Table Common Reqs 61508 vs 60730:

| Requirement | IEC 61508 | IEC 60730 |
|------------------|-----------------------------------|---|
| Safety Lifecycle | Detailed safety lifecycle | Safety considered throughout product life |
| Risk Assessment | SIL based on risk and severity | Class A, B, C based on risk level |
| Safety Integrity | Safety Integrity Levels (SIL 1-4) | Safety Classes (A, B, C) |
| Fault Detection | Diagnostics and fault tolerance | Self-test and fault detection |

| | | |
|-----------------------------|---------------------------------------|-----------------------------------|
| Systematic/Random Failures | Controls for both failure types | Focus on random failures |
| Software Safety | Software safety lifecycle and V&V | Self-test features for software |
| Redundancy | Required for higher SILs | Required for Class C devices |
| Validation and Verification | Extensive V&V for safety requirements | Testing and verification required |

Notes:

- Opens
- Safety WG Project
- Working group nominations
- Fault detection
 - Regarding the Table that mapping is quiet use full
 - <https://github.com/nutonomy/AVCDL> something similar was done within the opensource project were the AVCDL was mapped to ISO 26262
 - The Table should be extended maybe with more standards and also be opened for public

Backlog Topics:

- How can we gather all the reports in github
-

Resources

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req Focus Group:
 - [Zephyr Requirements Focus Group - Live Minutes - 2024](#)
- Overview: https://docs.zephyrproject.org/latest/safety/safety_overview.html
- Requirement guidelines: https://docs.zephyrproject.org/latest/safety/safety_requirements.html

01 October 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: Peter Christ, Tobias Kaestner, Nelson Ferragut, Nicole Pappler

Meeting Recording:

https://zoom.us/rec/share/zCrQNfBPI_kinjbAwZ-7COWF80zmg38uVYVyR1aYg6x_xsfWuJ3l_5s oc0Du_UL6.vr-lxatBTV6zU6wk

OOO:

Agenda:

- Opens
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Recap OSS and ZDS EU in Vienna

Notes:

- Opens
 - No opens
- Safety WG Project
 - No new updates or requirements from attendees.
 - Nicole encouraged people to get more engaged and review req. PRs or more submissions of PRs to keep the workflow moving.
- Recap OSS and ZDS EU in Vienna
 - Slides:
<https://docs.google.com/presentation/d/1x0jfwvNEjGrWMYqVObXNXWqjgpcFVSFFK73iVMwqM8A/edit?usp=sharing>
 - Shared presentation from the Open Source Summit, which highlighted the group's work on safety
 - The slide deck will be moved to the group's shared Google Drive for members to use and update for future events.
 - The automotive industry has shown interest in the group's work but is waiting for safety certifications before fully engaging.
 - The group expressed concern that this delay could slow progress and encouraged early involvement from companies.
 - A talk on Zephyr's role in the automotive industry was mentioned as worth watching. One member recommended viewing it for further insights
- Round Table:
 - In this portion of the discussion, Nelson Ferragut from Whirlpool shares Whirlpool's efforts to incorporate Zephyr into their safety requirements. He mentions that while Whirlpool has been using safety code for small, customized systems, aligning these with Zephyr's structure presents challenges. Whirlpool's safety standards, particularly IEC 60730, require additional memory protection, such as guarding against RAM corruption, which may not be fully aligned with the work of the Zephyr safety work group that is focused on industrial specs like IEC 61508.

- Nelson expresses concerns about the resource demands of implementing such memory protection in Zephyr, where solutions like duplicating variables to detect corruption may be costly and not ideal for Zephyr's core functionality. Nicole Pappler suggests the possibility of adding a configurable flag for diverse redundant storage of data, but acknowledges it as a future consideration, not something that aligns with current Zephyr safety goals.
- The conversation moves toward a discussion on whether duplicating data structures at the kernel level is a feasible safety measure, with some participants questioning if detecting issues early through mechanisms like watchdogs may suffice for certain applications, rather than comprehensive memory duplication. Ultimately, there's consensus that while data integrity is important, implementing such measures in Zephyr would be complex and not something that can be handled in the short term or by a small team.

Backlog Topics:

- How can we gather all the reports in github
-

Resources

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req Focus Group:
 - [Zephyr Requirements Focus Group - Live Minutes - 2024](#)
- Overview: https://docs.zephyrproject.org/latest/safety/safety_overview.html
- Requirement guidelines: https://docs.zephyrproject.org/latest/safety/safety_requirements.html

24 September 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: Peter Christ, Verena Schweinstetter, Tobias Kästner, Simon Hein, Nelson Ferragut, Roman Kellner

Meeting Recording:

https://zoom.us/rec/share/5M6YhLR2N9eidX_YFWxgdo5GzJEvUsGSHaae8D1J8tISJx37oXFpyXi35TAYRDre.0JDILCcSWC_hxctT

OOO:

Agenda:

- Opens
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Collab branch - update
 - <https://github.com/zephyrproject-rtos/zephyr/pull/78380>
- Follow up Request/Question from Nelson

Notes:

- Opens
 - Verena Schweinstetter introduced herself:
 - Working at ZEISS as a trainee.
 - Background in computational science and engineering.
 - Currently exploring Zephyr and its use in embedded projects.
- Safety WG Project
 - Static Code Analyzer Integration:
 - Simon provided updates on the Static Code Analyzer (SCA) integration:
 - Toolchain maintainer has been difficult to reach, causing delays.
 - But Simon is working on the integration fixes on a side track
 - Stefanos and Simon are collaborating to set up the infrastructure to integrate the tool into CI.
 - Requirements and Req. PR Status:
 - Not much movement in the requirements section
 - Tobias and Simon agreed that opening new PRs should wait until the current ones are addressed
- .Collab branch - update
 - PR : <https://github.com/zephyrproject-rtos/zephyr/pull/78380>
 - Anas have worked on integrating requirements into the documentation using Doxygen.
 - The requirements have been successfully imported into Doxygen and a sample linkage to a test case has been established.
 - Though the basic functionality of importing requirements and linking them to test cases is in place, there is still work needed to ensure two-way traceability:
 - **Current Status:** Only test cases link back to the requirements.
 - **Next Steps:** Scripts need to be developed to ensure that navigating from the requirements page will also show related test cases.

- Tobias mentioned, beyond linking source code, test cases should include preconditions, expected results, and other key details.
- These steps would transform the tests into comprehensive test specifications, making it easier to track and verify requirements.
- Static Code Analysis and External Tool Findings
 - Tobias shared that a client using Polyspace as a Static Code Analyzer has identified issues potentially relevant to the project, particularly in the Picolibc.
 - Simon welcomed the findings, affirming that any fixes identified by internal or external tools should be contributed via pull requests.
- Follow up Request/Question Nelson:
 -

Simon will follow up to provide more context Upcoming Agenda/Topics:

- Next Meeting (October 1, 2024)
 - Be determined based on project progress. Potential cancellation if no significant updates.

Backlog Topics:

- How can we gather all the reports in github
-

Resources

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req Focus Group:
 - [Zephyr Requirements Focus Group - Live Minutes - 2024](#)
- Overview: https://docs.zephyrproject.org/latest/safety/safety_overview.html
- Requirement guidelines: https://docs.zephyrproject.org/latest/safety/safety_requirements.html

Committee Topics:

10 September 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: Tobias Kästner, Peter Christ, Stephan Linz, Simon Hein, Nelson Ferragut, Roman Kellner, Andrew Hare

Meeting Recording:

https://zoom.us/rec/share/jxeARYoevuxl9pWvJ7WyV_VN4xbulsYOjSYnAm0wO1WfPljBLNvFUs wcqds5B_i_.Lfn8k23RYPxmEG6

OOO:

Agenda:

- Opens
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Round Table

Notes:

- Opens
 - No opens today
- Safety Working Group Project updates
 - Still not much progress from last time
 - Simon continues working on static code analyzer integration
 - CI integration
 - Work with Bugseng to setup licenses for CI
 - Also includes some client licenses for people working on fixing findings to improve their development experience
 - Still not enough people doing reviews and adding new requirements
 - Don't be afraid to provide any sort of reviews
 - First experiences with "Fixup" workflow to ease with reviewing PRs
 - Traceability branch work continues, will be published and announced in due course
- Round Table
 - Nelson: considers partitioning of firmware application into one part running under supervision of zephyr and another part not running under the zephyr scheduler, the latter being triggered by an interrupt. Question is about experiences by the others with such an approach.
 - Simon: silicon vendors distribute libraries for basic hardware checks which could be a use case for such a partitioning
 - Nelson: use case goes beyond that, requires product specific checks
 - Simon: is the question about how such an approach does fit with the work of the safety and/or architecture working group?
 - Simon: Need self-checks really be independent of the Zephyr scheduler?

- Nelson: Yes, to avoid Zephyr being put in higher assurance level (according to IEC 60730-1 which classifies Software into class A, B, C) or IEC 60335-X)
- Nelson: Would be a path for Zephyr to be used in safety products short term until Zephyr has adequate safety certification compatible with the needs of the higher assurance classes
- Nelson: Proposal to create dedicated workgroup to focus on this approach
- Simon: Safety working group committed to IEC 61508 for now, but worth to cross-check if there is relevant overlap with IEC 60730
 - Can add a task to pursue this further to the Working group's project board
- Nelson: what synergies can be exploited by people having the need for such a partitioning and the work of the safety WG not suggesting for the WG to consider 60730 as such
- Nelson: How can the collaboration between vendors and clients wanting such a solution be supported and is the Safety WG the right steward to facilitate this? Or some special interest group as a spin-off of the safety WG
- Nelson: company offers to work with relevant vendors to provide technical solution but seeks support somehow from the Zephyr community
- Peter: What is the content of this work with silicon vendors?
- Nelson: IEC requires evidence that interrupt driven safety checks are called correctly, this is easier to provide if Zephyr is not required for this to happen (as per using direct IRQs, e.g. ARM Cortex-M arch but also others)
- Simon: can we take a look at the specific requirement
- Nelson: not possible as what is required is more general than what's been described above which is a particular solution to it
- Simon: still not completely sure about what the ask is from the safety WG, can this be tracked with a RFC or dedicated branch inside the zephyr project?
- Peter: Since it is a strategy to implement a certain safety measure it somehow belongs to the safety WGs scope
- Nelson: agrees to provide clearer description of what the ask from the WG is in terms what the WG should consider to work on, if RFC were appropriate way, guidance is needed for how this works
- Tobias: Should continue the discussion via the discord channel and/or safety mailing list
- Simon: feels like something not considered so far, yet may be very well relevant for the safety working group as a specific safety measure
- Nelson: side note: other field of application is about motor control (think large brushless motors) where timing is not feasible from within any RTOS

- Introduction Andrew Hare
 - Working in Rail industry and considering usage of Zephyr for future products (timeline hinting at mid next-year)
 - Company has experience with embedded Linux in safety critical systems
 - Offers help to the working group, so looking for what's needed

Simon will follow up to provide more context Upcoming Agenda/Topics:

- Next Meeting (September 17, 2024)
 - Be determined based on project progress. Potential cancellation if no significant updates.

Backlog Topics:

- How can we gather all the reports in github
-

Resources

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req Focus Group:
 - [Zephyr Requirements Focus Group - Live Minutes - 2024](#)
- Overview: https://docs.zephyrproject.org/latest/safety/safety_overview.html
- Requirement guidelines: https://docs.zephyrproject.org/latest/safety/safety_requirements.html

Committee Topics:

-

03 September 2024 - Zephyr Project Safety WG - Canceled

- Canceled due to lack of activity in the safety wg tasks / requirements

20 August 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: Simon Hein, Nicole Pappler, Nelson Ferragut, Roberto Bagnara, Federico Serafini, Peter Christ, Roman Kellner, Kate Stewart, Olivier Charrier, Tobias Kästner

Meeting Recording:

https://zoom.us/rec/share/2Uvp5o75abKbTnaPPkxFMWpp_wcuJMsJuB9FZ7r-CV6b7zkUMu0m_u9pW2CwmKul.bmvX-qes0I7jDCsv

OOO:

Agenda:

- Opens
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Traceability branch - info
- Coding guideline CI integration PoC
- Round Table

Notes:

- Review comments on the “Add condition variables requirements” PR - Nelson’s comments have a good level, Simon will look into them
- Safet WG Project Board <https://github.com/orgs/zephyrproject-rtos/projects/23>:
 - More items have been added of work that is going on (the update of the docs section for the Coding Guidelines)
 - Eclair integration to the Zephyr CI, work has started on the integration into the Zephyr build environment, tool is working fine so far
- Request to start reviewing the requirements at the requirements repo PRs <https://github.com/zephyrproject-rtos/reqmgmt/pulls>

Requirement guidelines:

https://docs.zephyrproject.org/latest/safety/safety_requirements.html

- Requirements guidelines are in the [docs](#), also see the Resources section here
- We need to get the maintainers to sign of the requirements, we could do this at the same time when we get them to sign of the traceability
- Traceability branch has been set up and agreed on by the TSC
 - Will use Anas’ tooling
- Coding guideline check: proof of concept using a local GitHub runner on Simon’s PC
 - The fork is public
 - What will be the resource usage for running it?
 - The project and Bugseng need to finalize the license details first
 - From a technical point of view we need to integrate it into the infrastructure, when it runs we can see how much resources we need for

the run and how often we can afford to run it. Run it per PR, daily, once or twice a week etc.

- For Bugseng, running Eclair on auditable branch 3.7 takes one hour, the fixed branch takes 10 minutes. Running time depends on the number of violations and the computing power.
- It is possible to have an incremental analysis just on changed files, Roberto suggests only to reject when there have been no other violations of a rule; priority is to get the files clean and then keep them clean.
- Roundtable
 - When doing the reviews on GitHub, it is difficult to find comments again after a force push when revisiting the review.
 - Merging vs. pushing could conserve the history
 - Simon will look into the option to show outdated comments again (vs. the current comments)
 - There is an ELISA webinar tomorrow for SEooCs
<https://elisa.tech/event/elisa-seminar-the-seooc-concept-driven-into-extreme/>
 - https://zoom.us/webinar/register/WN_Z10-XMxDRRauusmMA8QmLg#/registration
 - The ELISA webinar on Cregit has been recorded
<https://youtu.be/5FjrUkWjgZY?si=u6P0rYYIQVImHyMs>
 - Getting the traceability working will also be important for basic quality topics
 - There will be an announcement of Zephyr in space soon

Upcoming Agenda/Topics:

- Next Meeting (August 13, 2024)
 - Be determined based on project progress. Potential cancellation if no significant updates.

Backlog Topics:

- How can we gather all the reports in github
-

Resources

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req Focus Group:
 - [Zephyr Requirements Focus Group - Live Minutes - 2024](#)
- Overview: https://docs.zephyrproject.org/latest/safety/safety_overview.html

- Requirement guidelines:
https://docs.zephyrproject.org/latest/safety/safety_requirements.html

Committee Topics:

- Ask for the state of the Bugseng quotation regarding the creation of more details for coding guidelines

13 August 2024 - Zephyr Project Safety WG - Canceled

- Canceled due to lack of activity in the safety wg tasks / requirements

06 August 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: Nicole Pappler, Tobias Kästner, Nelson Ferragut , Kate Stewart, Roman Kellner

Meeting Recording:

https://zoom.us/rec/share/emYS0jxwTu3iz3ApaYF9kzFhE47TSq_hhPM72Ci6Z24UifQaTf5iE4DOrn8g39X1.glaOJdxPtnU7OAUK

OOO:

Agenda:

- Opens
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Round Table

Notes:

Upcoming Agenda/Topics:

- Next Meeting (August 13, 2024)

- Be determined based on project progress. Potential cancellation if no significant updates.

Backlog Topics:

- How can we gather all the reports in github
-

Resources

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req Focus Group:
 - [Zephyr Requirements Focus Group - Live Minutes - 2024](#)
- Overview: https://docs.zephyrproject.org/latest/safety/safety_overview.html

Committee Topics:

- Ask for the state of the Bugseng quotation regarding the creation of more details for coding guidelines

30 July 2024 - Zephyr Project Safety WG - Canceled

16 July 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: Federico Serafini, Alessandro Zucchelli, Peter Christ, Simon Hein, Nicole Pappler, Roberto Bagnara

Meeting Recording:

<https://zoom.us/rec/share/a5YKWgZgpxZOJ2FcZ9BNBCF0wMEki3arN2AVucuQ6dz0OGdCrTUbDXDXpTgA-IS4.Lv0EC5P0U9ELbNOh>

OOO:

Agenda:

- Opens
- WG Changes - group elections - Info
<https://github.com/zephyrproject-rtos/zephyr/wiki/Working-Group-Elections>
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Guideline tool integration - Status
 - https://github.com/simhein/zephyr/tree/eclair_ci_integration
- Round Table

Notes:

- Opens:
 - Next week, safety committee meeting instead of the working group.
- WG Changes - group elections - Info
 - Reminder about working group elections; deadline was Friday last week.
 - Notification to be sent to the TSC (Technical Steering Committee) regarding participants who nominated themselves.
- Safety WG Project
 - Requirements State: progress is staling
 - Updated on coding guideline merges. Most are finished, some still open.
 - Project is in feature freeze due to release 3.7.
 - Call for writing and reviewing requirements for functional safety assessment.
- Guideline tool integration - Status
 - Integration for Coding Guideline enforcement is ongoing
 - Progress on the integration into the CI (Continuous Integration) system.
 - Hosted runner with the tool installed, working on license fetching.
- Note regarding the progress in the Safety Working Group: If nothing is done within the week, Simon will cancel the meeting, as nothing new is there.

Action Items:

1. **ALL:** Write and review requirements for functional safety.
2. **Simon Hein:** Monitor project progress and cancel future meetings if no movement is observed.

Upcoming Agenda/Topics:

- Next Meeting (July 30, 2024)
 - Be determined based on project progress. Potential cancellation if no significant updates.

Backlog Topics:

- How can we gather all the reports in github

Resources

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req Focus Group:
 - [Zephyr Requirements Focus Group - Live Minutes - 2024](#)
- Overview: https://docs.zephyrproject.org/latest/safety/safety_overview.html

Committee Topics:

- Ask for the state of the Bugseng quotation regarding the creation of more details for coding guidelines

9 July 2024 - Zephyr Project Safety WG - Canceled

2 July 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: Peter Christ, Nicole Pappler, Simon Hein, Erik Berces, Alexander kanavin, Tobias Kästner, Nelson Ferragut, Roman Kellner, Himanshu Pande

Meeting Recording:

https://zoom.us/rec/share/U_tfnMAaK6j8e6iCe124k5D3HnK1whM3UxD2uLoLLVG4ckppV1Tix6wdsp4VzJ3E.XH7ZTE4mq_gsBzfc

Agenda:

- Opens
- WG Changes
 - group elections - <https://github.com/zephyrproject-rtos/zephyr/wiki/Working-Group-Elections>
 - Info: https://docs.zephyrproject.org/latest/project/working_groups.html
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>

- Round Table

Notes:

- See meeting recording / transcript

Upcoming Agenda/Topics:

- Next Meeting (July 9, 2024)
 -

Backlog Topics:

- How can we gather all the reports in github

Resources

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req Focus Group:
 - [Zephyr Requirements Focus Group - Live Minutes - 2024](#)
- Overview: https://docs.zephyrproject.org/latest/safety/safety_overview.html

Committee Topics:

- Ask for the state of the Bugseng quotation regarding the creation of more details for coding guidelines

18 June 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: Alexander Kanavin, Peter Christ, Nicole Pappler, Roberto Bagnara

Meeting Recording:

<https://zoom.us/rec/share/c9FdCp-iNvIm6daaSXRpsO1dnOJ69fBCfajC-dcKCUB-7QgVJ5nJDeX9chcue2Fb.yyreC26Vs6CyCeB2>

Agenda:

- Opens

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Planning and onboarding information - gap analysis
- Round Table

Notes:

- Opens
- Safety WG Project
- Planning and onboarding information - gap analysis
 - As new members most likely do not have the standard (IEC 61508), it is not clear to them what needs to be done according to the standard, and what needs to be done for the project
 - https://docs.zephyrproject.org/latest/safety/safety_overview.html - do we need to add more information?
 - Semaphore Requirements can be a good starting point on how to create requirements, but for each component of Zephyr deep understanding of the code is necessary to create actual requirements
 - Create information pointing people to the Semaphore requirements,
 - Get official approval from TUV, so we can be sure that the style and level of detail is ok
 - Create material to guide people to what they need to know before creating requirements (understand the code, where to get help when don't understand the code etc.)
 - For the coding guidelines, we need a sharable description of them
 - It would be probably useful to get more understanding of the maintainers of MISRA, e.g. by them getting a MISRA training
 - Understanding of the MISRA rules is needed to properly explain and argument deviations of MISRA rules, when needed
- Round Table

Upcoming Agenda/Topics:

- Next Meeting (July 2, 2024)
 -

Backlog Topics:

-

Resources

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req Focus Group:

- [Zephyr Requirements Focus Group - Live Minutes - 2024](#)
- Overview: https://docs.zephyrproject.org/latest/safety/safety_overview.html

Committee Topics:

- Ask for the state of the Bugseng quotation regarding the creation of more details for coding guidelines

11 June 2024 - Zephyr Project Safety WG - Canceled

4 June 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: Simon Hein, Tim Wilcox, Peter Christ, Roman Kellner

Meeting Recording:

<https://zoom.us/rec/share/6t60kOzx6ojrXr-OsEOvqkqGAY1ZKaOLiNEAE3Ee60PqEXwTOxthuw4bEsdLy7M.nPB-L64Za0sXLVtc>

Agenda:

- Opens
 - <https://github.com/zephyrproject-rtos/zephyr/pull/73239> - Information
- Safety Req focus group meeting
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - New PRs
- Round Table

Notes:

- Opens
 - <https://github.com/zephyrproject-rtos/zephyr/pull/73239> - Information
 - Simon will keep the WG updated if there are any changes regarding the working group.
- Safety Req focus group meeting
 - Cancel the meeting and the discussions about the requirements shall be held in the working group and on PR base.

- Safety WG Project
 - <https://github.com/zephyrproject-rtos/reqmgmt/pull/61/>
 - Some Documented Interrupt descriptions are very HAL/Platform specific
 - The Multilevel interrupt is implemented in the HAL layer
 - This don't fit in the HAL layer abstraction
 - Tim will create a Issue to clarify and to track that problem
 - <https://github.com/zephyrproject-rtos/reqmgmt/pull/69>
 - This PR will make specific grammar fields as required
 - Right now the field could be left empty and the CI would not complain about it
 - <https://github.com/zephyrproject-rtos/reqmgmt/pull/67>
 - This PR removes the obsolete grammar filed review_comments
 - Also removes all review comments from the imported requirements.
 - <https://github.com/zephyrproject-rtos/reqmgmt/pull/68>
 - Baseline the UID of all requirements to unify the appearance
 - Also the described process from the guidelines could be applied to that
 - The PR is the PR to the proposal which were discussed via the mailing list (no objections in the mailing list)
 - This PR needs to be merged in time because of the traceability tooling.
- Round Table

Upcoming Agenda/Topics:

- Next Meeting (June 4, 2024)
 -

Backlog Topics:

-

Resources

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req Focus Group:
 - [Zephyr Requirements Focus Group - Live Minutes - 2024](#)
- Overview: https://docs.zephyrproject.org/latest/safety/safety_overview.html

Committee Topics:

21 May 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: Tobias Kaestner, Simon Hein, Erik Bereces, Nelson Ferragut, Rob Woolley, Tim Wilcox, Roberto Bagnara

Meeting Recording:

<https://zoom.us/rec/share/H0gQpuDP3udzIEsFtmxVllmVjZmVlqzMXIkfKCyrJ1K1hierU6pNAhFK7hM-qBvR.vBmfbSUZSH3kO6yj>

Agenda:

- Opens
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Round Table

Notes:

- Opens
 - Next WG meeting is on the 4th June because of the safety committee meeting on the 28th may.
 - No more opens
- Safety WG Project
 - Not much progress to report since our last meeting
 - Problems with onboarding new people solved
 - Tim: Regarding Interrupts Requirements
 - Implemented in HALs
 - At kernel level mainly interface requirements
 - Simon: Re-opened Thread Requirements
 - New PR to adjust to new guidelines as thread requirements got merged prior to the finalization of our guidelines
 - Simon: Still volunteers needed for Requirements work
 - Simon: Update to Coding Guidelines
 - Merging to main in progress, no showstoppers yet
 - Follow Issue <https://github.com/zephyrproject-rtos/zephyr/issues/48002> of the zephyr project for details on status
 - Please provide feedback

- Question to Requirements from Nelsson: Issues on the project board lack detail, is it possible to add some detail on what's needed for contributors to do
 - Simon: Suggest to use existing RQTs (Semaphore) and then look at existing documentation to extract the RQT in question
 - Tim: confirms that this is exactly his approach, however it is challenging in particular without a good architectural overview
 - Nelson: specifically points at Scheduling (#16) as the details mentioned therein as an example for the information that's missing from the other issues
- Simon: no progress on the draft issues so far, will inform about updates via the mailing list
- Simon: RQTs repo guidelines updated, reviewers should re-review the PR so that it can be merged in the next 2-3 days, focus on must-edits for now, further refinements can be made in later PRs
- Round Table
 - Tim: Gap analysis between Zephyr and IEC 62304
 - Tobias: offer to work on this together with P. Christ, Tim and Tobias
 - Tim to produce a list of questions to share and then schedule a meeting to discussions
 - Simon: make it public via the mailing list to incorporate feedback from the larger group
 - Simon: reminds everyone that for async questions/topics the group has the mailing list and also discord channel

Upcoming Agenda/Topics:

- Next Meeting (June 4, 2024)
 -

Backlog Topics:

-

Resources

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req Focus Group:
 - [Zephyr Requirements Focus Group - Live Minutes - 2024](#)
- Overview: https://docs.zephyrproject.org/latest/safety/safety_overview.html

Committee Topics:

14 May 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: Simon Hein, Tobias Kaestner, Kate Stewart, Tim Wilcox, Benjamin Cabe, Nelson Ferragut, Peter Christ,

Meeting Recording:

https://zoom.us/rec/share/IIznJQO715qP_zrWGaBZobwXMqMc1R1DcGIHxjj97MjRoSpDGOMT1jOJfZ8h5Mp_NSgDCgBUJezV5B-R

Agenda:

- Opens
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Requirement Guideline / Semaphore Requirements - Feedback TÜV
- Safety functionality / CRC / Checksum functionality - discussion [Tom]
 - Safety services for failure detection
- Round Table

Notes:

- **No opens**
- Simon presenting changes to the WG board on Github
 - Clean up, removing items belonging to the safety committee
 - Some issues moved to closed
 - New view to track "Requirements"
- Nelson: question about why multiple cards exist per topic, e.g. Mutex
 - Answer: boards show both issues and PRs at the same time
 - Might change later
 - For now can be distinguished by icon
- Semaphore requirements were merged
 - Some cleanups still needed after PR got merged, Simon takes care of this
- PR#71593:
 - Question by Simon: Should Benjamin be assigned for PR#71593 as he is maintainer for the Project Docs
- Updates on Coding Guidelines
 - Follow Issue #48002
 - Some rules are now fulfilled by work contributed by bugseng

- Question by Tim: What about architecture diagrams? Are there plans to create a coherent project level architecture diagram?
 - Simon: some sub-groups have started to align their diagramming with one another
 - Simon: need to refine issue “Generate architecture diagrams”, Tim emphasizes the importance and value of diagrams
- Tim: By reviewing the current documentation, lots of references are made to specific artifacts most likely to be found in-tree, yet mapping to “classical documentation landscape” is challenging
- Simon showing the Safety Committee’s Mapping to IEC document names as example for such an effort
- Simon also showing the kibana dashboard:

[https://kibana.zephyrproject.io/s/public/app/dashboards#/view/d0c795f0-0d26-4407-83c1-528a01a47c75?_g=\(filters:!\(\)\)](https://kibana.zephyrproject.io/s/public/app/dashboards#/view/d0c795f0-0d26-4407-83c1-528a01a47c75?_g=(filters:!()))
- Requirements Guidelines:
 - Simon to report about today’s call with TÜV
 - General agreement with the WG approach and no objections to proceed with the current efforts
 - Regarding phase 1 completion a workshop once Nicole is back from vacation was proposed to clarify the open issues
 - Question from Kate: When are we going to start upstreaming the traceability annotations? Need to make sure we are not interfering with LTS release activities, so might park it on a branch for now, but should move to main in due course
 - Question from Kate: Are more people now willing to pick up open work now the guidelines have become more solid?
 - Tim volunteers to look into interrupt requirements
- Regarding specific Safety functionalities
 - Examples include error detection mechanisms for faulty hardware (memory)
 - Also called safety mechanisms in some domains
 - Simon suggests to consider such things as additional safety services
 - Not supported in initial scope, so users need to take care of these services themselves
 - No reason to include highly demanded services in later safety releases
 - That’s what commercial RTOS suppliers have done in the past, too
 - For certification it’s important to state what’s in scope and what isn’t, ie. what users have still to do on their own if their application requires it
 - Nelson: what exactly was meant by CRC in the comment from Thomas in the previous call
 - Simon: was mainly for message passing to detect faulty communications
 - Nelson: CRC sometimes also used to detect flash corruptions executed periodically during runtime

- Round Table:
 - There is an problem with the WGs issues on Github when it comes to assigning people to an issue, Simon going to take a look after the call

Upcoming Agenda/Topics:

- Next Meeting (May 21, 2024)
 -

Backlog Topics:

-

Resources

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req Focus Group:
 - [Zephyr Requirements Focus Group - Live Minutes - 2024](#)
- Overview: https://docs.zephyrproject.org/latest/safety/safety_overview.html

Committee Topics:

7 May 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees:

Tobias Kästner, Erik Berces, Jan Herr, Nelson Ferragut, Roman Kellner, Tim Wilcox, Kate Stewart, Peter Christ, Anas Nashif, Tom Fleischmann, Nelson Ferragut, Francesco

Meeting Recording:

https://zoom.us/rec/share/fOuK6LL1uRuBcGtbWhu6v6glT-88NnZlxbfofbctxOg7Q4KVaSnYv4Os_vhmiMTB.f4J3PMHIMQrdvV7u

Agenda:

- Opens
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>

- Semaphore PR ready to review: <https://github.com/zephyrproject-rtos/reqmgmt/pull/30>
- Requirements guidelines: <https://github.com/zephyrproject-rtos/zephyr/pull/71953>
- Glossary [Roman]: <https://github.com/zephyrproject-rtos/zephyr/issues/72162>
- Round Table

Notes:

- Others:
 - Requirements focus group meeting cancelled due to bank holiday
 - Roman on vacation starting tomorrow until May 23, 2024
- Working through Safety WG Project - Kanban board.
 - <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Highlighting 4 lanes of status; contains committee & working group topics
 - Have added in the "ToDo" column - if folks interested in working on.
 - Please use mailing list and discord channel to sign up for tasks.
 - See where most interest is and getting started - weigh in on priority
 - Be useful to tag between between committee vs. working group.
 - **AI Simon:** given this is Safety WG - move Committee related tasks should be moved to their own tracking board. Safety scope & configurations, for instance.
 - Architecture diagrams & increasing test coverage.
 - **AI:** transfer from #68005 requirements traceability as bullets from (similar to #18 - Semaphores) - into kanban board, esp. When looking for help.
 - Once semaphore PR is merged, having a board for tracking these activities makes sense.
 - Open Question: Separate board for requirements & traceability? Or just use Safety WG board. What will it look like long term? Discuss with Simon.
 - Make it explicit where projects should be linked. Ie. requirements for zephyr in it's zephyr repo, rather than ZephyrProject.
- In Progress
 - Ordered topics to most active.
 - See PR on [requirements management repo #30](#)
 - Provide feedback on this into the PR, target is to merge it early to mid next week.
 - Provided overview of Strict doc, and PR that is being used.
 - Gave mini-tutorial on how to navigate github, and provide feedback.
 - See PR on Requirement Repository Guidelines (at Zephyr Project Level [#71593](#)); planned for documentation of Zephyr project. Quality goals & criteria. Goal is to have it as approachable as possible.
 - Discussion to follow language patterns, to help with remove ambiguity, (ie. EARS)

- Want this as a starting point; had a place to review. Acceptance into project documentation, shows that it is approved by group working on it.
- We want this to be reviewed this week, possibly another round of review in a meeting next time we meet, then merge.
- Note: These are the requirements of the project that are in the safety scope. In scope of certification is key. There may be other common requirements.
- Tim: Looking for requirement setting guidelines for project, than each working group, but recognizes this may be evolutionary.
- Roman: will transfer his prior comments from other PR, to this one.
- Transfer Github Google doc on Glossary
 - Some comments don't make sense in full project issue, so changed from doing specific PRs.
 - Have transferred content to RFC - added what what is in google doc to the <https://github.com/zephyrproject-rtos/zephyr/issues/72162> to come up with approach for the pull request.
 - Zephyr project wide glossary - has some safety specific glossary. Guidelines needed on where to put things.
 - Tim suggested saying "Safety" in front when conflict. It should also be in one universal place, conflict of terminology become obvious.
 - Kate agreed that this will make it clearer in overall project context
 - Discussion should this be against common glossary vs. Safety specific documentation
<https://github.com/zephyrproject-rtos/zephyr/blob/main/doc/glossary.rst>
 - If it's a committee specific term, it doesn't need to be merged into project wide glossary.
- Round Table:
 - Tom: looking discussion on CRC / Checksum functionality in Zephyr for possible end-to-end decompression. Viable safety mechanism from ASIL-D to ASIL-D. Tobias - agree looking for features that will make it more safe in future, for supporting application level design.

Upcoming Agenda/Topics:

- Next Meeting (May 14, 2024)

Backlog Topics:

-

Resources

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req Focus Group:
 - [Zephyr Requirements Focus Group - Live Minutes - 2024](#)
- Overview: https://docs.zephyrproject.org/latest/safety/safety_overview.html

30 April 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees:

Meeting Recording:

Agenda:

- Opens
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Semaphore PR ready to review: <https://github.com/zephyrproject-rtos/reqmgmt/pull/30>
- Requirements guidelines: <https://github.com/zephyrproject-rtos/zephyr/pull/71953>
- Glossary [Roman]: <https://github.com/zephyrproject-rtos/zephyr/issues/72162>
- Round Table

Upcoming Agenda/Topics:

- Next Meeting (May 14, 2024)

Backlog Topics:

-

Resources

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req Focus Group:

- [Zephyr Requirements Focus Group - Live Minutes - 2024](#)
- Overview: https://docs.zephyrproject.org/latest/safety/safety_overview.html

Committee Topics:

- New Participants:
 - Nelson Ferragut - attending to monitor progress.

30 April 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: Simon Hein, Nicole Pappler, Anas Nashif, Stanislav Pankevich, Benjamin Cabe, Thomas Fleischmann, Gregory Shue, Kate Stewart

Meeting Recording:

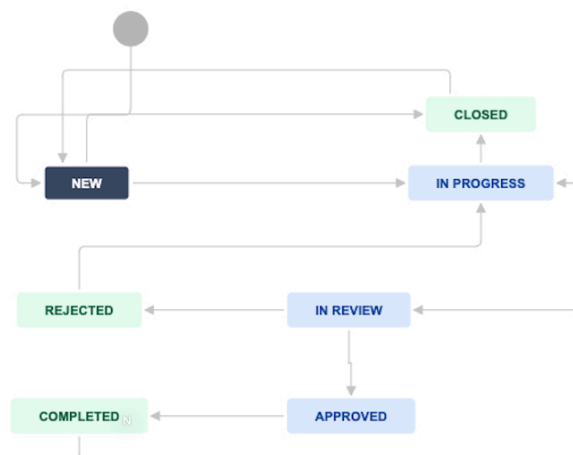
<https://zoom.us/rec/share/sMy6aA2iV3MzYf3g8uAiniHEHWSBLAeEErNFVQKMQDN4dCDZMP18Btz-Hes7dksm.j9k26N-skJGTA6vZ>

Agenda:

- Opens
- Safety Committee - Feedback loop
 - Last Tuesday of the Month Committee Meeting (instead of the working group meeting)
 - The safety committee is missing the feedback loop and getting more information about what is going on in the working group and if the direction of the working group aligns with the goals of the safety committee
 - If we need feedback directly from the safety committee, we can do this on the Safety-Committee mailing list and do not need to wait for the next meeting on the end of the month
- Safety WG - expectations committee, Scope and Goals
 - More focus to make progress, avoid side discussions
 - Getting the working group more work based
 - E.g. for the requirements we should work more PR based
 - Current focus is to have requirements that reflect the actual functionality, focusing on the kernel
 - Short term goal: get the requirements, establish linkage for traceability
 - Question from Stan: Who is on the Safety Committee? Which committee members are part of the safety working group
 - Answer: the platinum members of the project, usual attendees in the working group are from Zeiss (Tobias, Peter), Intel (Anas - representing

the project community, Francesco), Cariad (Tom), Simon (safety chair), Nicole (safety manager), Kate; NXP are interested, but have not yet joined the working group,

- We are also aware that we currently have no introduction material or landing page for people newly joining -> Simon is currently working on it
- Coding Guidelines
 - Re-work has been done by Bugseng to align existing code with the Coding Guidelines on the old auditable branch
 - People from Baumer now have started merging these changes to the main code base
 - Call for participation: see [Safety WG Project on GitHub](#)
 - Is there a public list available who is doing what at the moment? So that people are not working on the same issues?
 - No, not yet.
 - A workaround would be, that people add to the issue that they are currently working on
 - Simon will add this to the head issue
 - Simon is working on the integration of a tool into the CI
- Req States [Nicole]
 - Summary - focus group discussed states of requirements, the discussion was driven further on the mailing list.
 - Diagramm about the workflow is for the focus group
 - **Safety Requirements Focus Group**
 - Nicole: Obsolete is more like a state that we do not use because we are going back from the code.
 - Anas: Recommends that Active is renamed to Complete
 - The approved state would be reached if it is merged into the req repo tree
 - The Req will be approved if it fits for the project. (not safety, not security)
 - The PR itself is the Draft state if it gets merged into the tree it is complete
 - Anas: We have too much states
 - Stan: Two states are enough
 - Info about workflow
https://www.ibm.com/docs/en/SSUWLZ_7.0.3/doorsnext/com.ibm.rational.rrm.help.doc/images/default_workflow.png
 - Jira workflow, shared by Anas:



- Stan: Why do you need an extra state? Why are two states are not enough
- Anas: We should comply with the naming in the world and not come up with something new.
- The state need to be mapped into a github workflow
- Simon: Does the traceability matrix not showing the complete state
- Stan: The req should not show the complete state of the lower level
 - This shall be done by the traceability tooling
- Anas: Before we get the traceability tooling into place we need the requirements in place
- Anas: Showing the idea of req traceability -> See Recording
 - A lot of work needs to be done to close the gaps
- Round Table

Upcoming Agenda/Topics:

- Next Meeting (May 07, 2024)

Backlog Topics:

-

Resources

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req Focus Group:
 - [Zephyr Requirements Focus Group - Live Minutes - 2024](#)
- Overview: https://docs.zephyrproject.org/latest/safety/safety_overview.html

Committee Topics:


23 April 2024 - Zephyr Project Safety WG - Canceled

** See Meeting Dial-In Information in the header

Attendees:

Meeting Recording:

Agenda:

- Opens
- Zephyr Requirements Focus Group - Summary
 - <https://github.com/zephyrproject-rtos/reqmgmt/pulls>
- Scope
- Artifacts for IEC 61508
 - Starting point is in the docs
https://docs.zephyrproject.org/latest/safety/safety_overview.html
 -  Artifacts
- Round Table

Upcoming Agenda/Topics:

- Next Meeting (April 23, 2024)

Backlog Topics:

-

Resources

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req Focus Group:

- [Zephyr Requirements Focus Group - Live Minutes - 2024](#)

Committee Topics:


16 April 2024 - Zephyr Project Safety WG - Canceled EOSS 2024

** See Meeting Dial-In Information in the header

Attendees:

Meeting Recording:

Agenda:

- Opens
- Zephyr Requirements Focus Group - Summary
 - <https://github.com/zephyrproject-rtos/reqmgmt/pulls>
- Scope
- Artifacts for IEC 61508
 - Starting point is in the docs
https://docs.zephyrproject.org/latest/safety/safety_overview.html
 -  Artifacts
- Round Table

Upcoming Agenda/Topics:

- Next Meeting (April 23, 2024)

Backlog Topics:

-

Resources

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req Focus Group:

- [Zephyr Requirements Focus Group - Live Minutes - 2024](#)

Committee Topics:

-

09 April 2024 - Zephyr Project Safety WG - Canceled

02 April 2024 - Zephyr Project Safety WG - Canceled

26 March 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header



Attendees: Simon Hein, Greg Shue, Stanislav Pankevich, Nicole Pappler, Anas Nashif, Roman Kellner, Thomas Fleischmann, Tim Wilcox, Jan Herr

Meeting Recording:

https://zoom.us/rec/share/TE_xCwCROtM9PTRh3cOB01HxywLp-L1Hcr6xbt7ryiZJmbEBqbdApLUTj5Gor_s.wG0cfcE5Wh1y5HOq

Agenda:

- Opens
 - Nicole volunteers to drive meeting on 2 april 2024
 - Thomas Fleischmann asked for compliance to ISO 26262 as an add on to the current 61508 safety activities - he will look for somebody who can provide us with a comparison list of the two standards
 - Tim adds that when he gets access to the compliance artifacts list, he can also add the 62304 artifacts
- Zephyr Requirements Focus Group - Summary
 - <https://github.com/zephyrproject-rtos/reqmgmt/pulls>

- Stan gave an overview of the latest updates of StrictDoc, there is now the option to use fragments, that are used to form a complete StrictDoc document
-  Adding Requirements Guideline:
- Requirements phrasing discussion on the pull requests of Semaphore
 - Stan adds that there are now stable requirements for interfaces (from Greg) and pretty-ready requirements from Anas
 - There are now already multiple pull requests that make it hard to follow up and keep the overview of what is discussed - we need to improve and find a process to get better here
 - Simon adds that we must not loose pace and that there are now already some good requirements in there, and that we now should start merging the requirements into the documents, so that we have something we can work with and move forward. There can still be further PRs on the merged artifacts. It is important not to lose pace now.
- Roman brings up the discussion regarding the levels of requirements that need to be defined. If we have an interface specification or not.
 - Tim agrees
- Stan adds to Simon's statement of not losing pace that we can merge requirements when we agree on their stability
- Stan also adds that it will be good to know if somebody cannot attend in advance
 - Anas adds that discussions should be in the comments of the PRs, progress can happen outside of the meetings
 - Anas also adds that we should work with these PRs like we work in the complete project. If somebody wants something changed, comment on it, if somebody agrees, plus one it.
 - Simon, Tim and Nicole agrees
- Scope
 - <https://github.com/zephyrproject-rtos/zephyr/issues/57702>
 - Simon adds to this that the scope is not set in stone, e.g. if something is heavily used by the kernel but not in the initial scope, we should include it, as the effort to exclude it will be more effort than including it -> but this must be brought up and documented (in the issue above)
 - Greg asks which part of the CPU architectures tree is currently included - answer by Simon that non of this currently included, as we exclude the hw dependencies at the moment
 - Anas adds that this is not correct, as there are architecture interfaces called by the kernel, so the kernel depends that the architecture parts implement this
 - Greg adds the question how much of the HAL is currently included - answered by Anas that the HALs are not included
- Artifacts for IEC 61508
 - Starting point is in the docs
https://docs.zephyrproject.org/latest/safety/safety_overview.html
 -  Artifacts

- Round Table

Upcoming Agenda/Topics:

- Next Meeting (April 2, 2024)

Resources

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req Focus Group:
 - [Zephyr Requirements Focus Group - Live Minutes - 2024](#)

19 March 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: Simon Hein, Nicole Pappler, Nelson Ferragut, Anas Nashif, Benjamin Cabe, Erik Berces, Greg Shue, Kate Stewart, Patrick Ashby, Peter Christ, Roberto Bagnara, Roman Kellner, Stanislav Pankevich

Meeting Recording:

<https://zoom.us/rec/share/71Af4l4sQDtb6GsqIfI2hQd27lwBoH-oWX7zErPqkTj3Y1R5688qVhIYIbjez2p.wDjjCHDSt-3DcGTS>

Agenda:

- Opens
- Zephyr Requirements Focus Group - Summary
 - <https://github.com/zephyrproject-rtos/reqmgmt/pulls>
 - Adding Requirements Guideline:
 - AI of Simon and Nicole: Write a one pager guideline on how to add requirements
 - There is a Wiki Page where it will be added
 - Drafting the first version of the requirements guideline in the google doc linked up here
 - Greg adds that we need to consider when we limit our way how to create requirements, what the downstream user needs; Simon adds that we need to create them for the target audience, not over thinking corner cases
 - Greg questioned the approach, as we might need to change our approach every time a new industry wants to join; Simon and Nicole adding there that we are starting without specific standards, defense and aerospace

being the only standards that might need more than we are currently doing. We need to be decoupled from standards, we are focusing on requirements right now.

- Greg asked if this document is going to be a recommendation or a constraint. Anas says that it will be a guideline, Greg would call it a requirement, if it is not just a recommendation but a rule.
 - Simon further went through the draft guideline
 - Greg asked how we do keep a single source of truth, when we have user stories in the requirement. To avoid conflicts within the requirement, we need to keep user stories separate from requirements
 - Roman explains that the user stories first were created as an add on to previously existing requirements to get a better understanding of the requirements
 - Anas adds that the user stories can be beneficial on a certain level
 - Nicole agreed with Roman and Anas
 - Stanislav proposed to rename the user stories to rational
 - The group agrees that we need to add more details about how to handle configurability
 - There is an updated version of the requirements from Anas
 - Greg requested that Stan gives feedback on the pull request, where Stan thinks that Greg is too close to the implementation
-
- It has been decided in the Focus Group, to set more detailed targets and goals for the group.
 - Continuing discussion how to handle configurations; the consensus was that configurations are not handled within a requirement, but on a separate level (as separate requirement). If the requirement deeply depends on a configuration and cannot be described without it, the configuration can be part of the requirement; but generally the requirement shall be agnostic to configurations.
 - Anas presented the tracing mechanism into the actual coding environment, incl. Metrics that will help us to identify gaps
 - Clear commitment to use StrictDoc for requirements management
 - We need to manage our requirements somewhere and we need a tool for it
 - As a second phase we use the information captured in the StrictDoc Tooling to achieve traceability to code and testing
- Scope
 - <https://github.com/zephyrproject-rtos/zephyr/issues/57702>
 - Round Table

Upcoming Agenda/Topics:

- Next Meeting (March 26, 2024)
 - Scope
 - <https://github.com/zephyrproject-rtos/zephyr/issues/57702>

Resources

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req Focus Group:
 - [Zephyr Requirements Focus Group - Live Minutes - 2024](#)

12 March 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: Simon Hein, Nicole Pappler, Anas Nashif, Diego Sampaio, Greg Shue, Jan Herr, Nelson Ferragut, Peter Christ, Roberto Bagnara, Stephan Linz, Tim Wilcox, Tobias Kästner, Roman Kellner

Meeting Recording:

https://zoom.us/rec/share/wS2aLQLyv6eIQcfBySBpaCYmcL9PozkCylITdvQ1_jcp0CNQEhtsVXI30B_VOHnY.GCzWC5wBAsGEDeLr

Agenda:

- Opens
 - Question from Nelson Ferragut: What is the role of the HAL providers in the group and how do they reach their safety goals? What is the description of the safety working group expectations?
 - There is currently no point where people can find this information, but we will create something where people can find everything that we are doing and where we are needing help
 - Standards interest of the new members: IEC 62304 (medical) and IEC 60730 (home appliances)
 - For IEC 62304, Zephyr will be treated as SOUP, which is less than it is required by IEC 61508, but the documents can be used for medical. But as Zephyr is open source and we have requirements and test cases, it is treated as “glass house” and we have deeper insight to the system.
 - What are the planned artifacts? Can we find this in GitHub? Is it only kernel focused at this point?
 - The focus is becoming more and more clear, we will start with the kernel

- What is the work that needs to be done on top of what is there?
- WG Frequency
 - The working group frequency is increasing to a weekly cadence (except the last week of the month, where the committee meets at the same time)
- Zephyr Requirements Focus Group - Summary / Additions
 - Zephyr Requirements - <https://github.com/zephyrproject-rtos/reqmgmt>
 - <https://github.com/zephyrproject-rtos/zephyr/issues/68005>
 - We need to create requirements for meeting the expectations of safety and security - although we started with safety (IEC 61508), we need to be clear that we are creating requirements that are decoupled from any safety or security standard. The requirements are currently describing the behavior of Zephyr, and the specific needs of safety or security standards will then need to be discussed in the groups. Right now we try to find the base-requirements - functional requirements for the Zephyr project.
 - The scope of the requirements that we want to create in this group, do not include the requirements of the system that will include Zephyr.
 - From the view point of a product manufacturer, the easiest way to recognize this is how to understand how Zephyr content is generated; this is requirements, tools (like built system), constraints that apply upwards to it; this can be functional and non-functional;
 - Regarding the starting scope: this was set as a starting point, so we can start, but never was intended to be complete yet
 - We need to focus on what really is/will be the scope
 - The GitHub issue to discuss the scope:
<https://github.com/zephyrproject-rtos/zephyr/issues/57702>
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Round Table
 - <https://github.com/zephyrproject-rtos/reqmgmt/pull/29>

Upcoming Agenda/Topics:

- Next Meeting (March 19, 2024)

Resources

- Req Focus Group:
 - [Zephyr Requirements Focus Group - Live Minutes - 2024](#)

27 February 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: Rob Woolley; Stanislav Pankevich; Greg Shue; Francesco Sforza; Peter Christ, ZEISS; Anas Nashif; Simone Ballarin; Roman Kellner; Kyle Fabris; Tobias

Meeting Recording:

https://zoom.us/rec/share/CnuYtsbRV_YpyA1c7EO0ahAvg5vRE0D7jlsc3lQgaPqYCjSP-i0wOT2XavJEUZk.QxHe7GdJ8edXjDtx

Agenda:

- Opens
- New Member Rob Woolley, Wind River
- Zephyr Requirements Focus Group - Summary of First Meeting last Thursday 17 to 19 o'clock CET (Europe/Berlin)
- The "Zephyr Safety Requirements Focus Group" will take place every Thursday
 - [Link to the zoom meeting:](#)
<https://zoom-lfx.platform.linuxfoundation.org/meeting/94635874875?password=2c386b4b-b84f-4d3e-ba7f-985ef57830bb>
 - [Link to the meeting minutes:](#)
<https://docs.google.com/document/d/1rd6BitpAoxQ6WCCNv4aoT4HuGprVY0Et4yNJeb6i-AQ/edit#heading=h.s8n3zq5dqe9f>
- Stan: Currently some Zephyr source code files (C files) are quite large. It might be good to split them into smaller files to make it more granular. But it must be kept in mind, that changes to the file structure might have influence on other topics, like security for example. For details please check the meeting minutes linked above.
- Anas: Reviews are welcome for PR
<https://github.com/zephyrproject-rtos/zephyr/pull/69395> (kernel: some cleanup and fixes) and <https://github.com/zephyrproject-rtos/zephyr/pull/69482> (kernel: move priority queue handling to own file/header)
- Links posted to the chat by Stan:
<https://rtems-qual.io.esa.int/>
https://rtems-qual.io.esa.int/public_release/rtems-6-sparc-gr740-uni-4.tar.xz (the actual QDP)
<https://www.youtube.com/watch?v=DmZjrsO4RHU>
- Greg: Reviews are welcome, Zephyr system init functional requirements by gregshue · Pull Request #29 · zephyrproject-rtos/reqmgmt (github.com),
<https://github.com/zephyrproject-rtos/reqmgmt/pull/29>
- Stanislav classified the requirements added by Simon (<https://github.com/zephyrproject-rtos/reqmgmt/tree/main/docs>) into multiple categories.
- Anas: We should use "semaphores" as the initial example to run through the process of how to deal with the requirements. There was a great deal of agreement on this in the round.
- <https://docs.zephyrproject.org/latest/project/documentation.html> describes how documentation using doxygen should be done.
- No agreement has yet been reached on the exact scope of certification according to IEC 61508 (SMP, user space, ...).

- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Zephyr Requirements - <https://github.com/zephyrproject-rtos/reqmgmt>
 - <https://github.com/zephyrproject-rtos/zephyr/issues/68005>
 - Focus Group Requirements creation - call for action
- Round Table

Upcoming Agenda/Topics:

- Next Meeting (March 12, 2024)

13 February 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: Nicole Pappler, Stanislav Pankevich, Erik Berces, Francesco Sforza, Jose Paul, Peter Christ, Roberto Bagnara, Simone Ballarin, Roman Kellner, Greg Shue, Philipp Ahmann

Meeting Recording:

https://zoom.us/rec/share/P-Obdennr6YnQjKYLZoLA9fEGLennHBg5Lz9NfOEkjXWqS6PHTDo-ayboi935o.7uz9gbHIB3Bni_Xu

Agenda:

- Opens
- Zephyr Requirements Update [10 minutes, Stanislav]
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Zephyr Requirements - <https://github.com/zephyrproject-rtos/reqmgmt>
 - <https://github.com/zephyrproject-rtos/zephyr/issues/68005>
 - Focus Group Requirements creation - call for action
- Round Table

Upcoming Agenda/Topics:

- Next Meeting (February 27, 2024)

30 January 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: [[unknown]] [[unknown]]; Stanislav Pankevich; Erik Berces; Peter Christ; Simone Ballarin; Anas Nashif; Roberto Bagnara; Tobias Kaestner; Jose .; [[Unknown]] Sforza; [[Unknown]] [not provided]

Meeting Recording:

<https://zoom.us/rec/share/f5SpdoROrBgVEW1Y2AHx2nQYKpmGvCutY60zLGBZmdGBHRikFH3CFfOGiTyKddXW.LM1C79e4RmVHzdxR>

Agenda:

- Opens
 - Meeting will take place on 13.02.2024
 - New participant in the safety working group, Jose Paul, medical background
 - Stanislav: Update regarding SPDX
- WG planning 2024:
 - <https://github.com/zephyrproject-rtos/zephyr/issues/61500>
 - Identify Safety requirements for LTS3 (LTS3 is 3.7, date is still t.b.d., planned for early summer)
 - Currently we are looking on process related topics to satisfy the requirements of the 61508.
The safety manual should give hints to the developers on how to use Zephyr to be compliant to the standard 61508
 - A dedicated meeting shall be scheduled to discuss technical requirements of Zephyr to reach technical safety claims
 - Focus topics
 - Requirements
 - Coding guidelines
- Safety WG Project Issue Board - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- New requirements will be transmitted via PR into github in strictdoc language and then be merged into strictdoc. Currently this merging is done by Simon since he is the safety architect.
- Zephyr Requirements - <https://github.com/zephyrproject-rtos/reqmgmt>
 - <https://github.com/zephyrproject-rtos/zephyr/issues/68005>

- The list of requirements in this ticket still has to be completed, but is a good starting point. It would be good to specify all features from the kernel folder.
 - A prototype of requirements (“requirements skeleton”) shall be created, with high-level requirements and more detailed requirements with direct relationship to the source code. The traceability between these levels of requirements shall be demonstrated. “Threads” could be an appropriate example.
 - <https://github.com/zephyrproject-rtos/reqmgmt/pull/15>
 - <https://github.com/zephyrproject-rtos/reqmgmt/issues/23>
- Stanislaw: Update regarding SPDX
 - StrictDoc has been expanded to add SPDX informations (additional SPDX element in the grammar of StrictDoc)
 - It is still in discussion if this fits the needs of the safety wg, since some manual work is to be done to keep the data up to date if the source code has been modified
- Round Table

Upcoming Agenda/Topics:

- Next Meeting (February 13, 2024)

Open Topics

- Requirements:
- Architecture Specifications
- Coding guidelines
- Tests and test coverage

Resources:

- Project: <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Issue Label: “Safety”
- Discord: <https://discord.com/invite/Ck7jw53nU2>
 - #safety
- Safety Working Group Mail List: <https://lists.zephyrproject.org/g/safety-wg>
 - Calendar: <https://lists.zephyrproject.org/g/safety-wg/calendar>

16 January 2024 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: Stanislav Pankevich, Simon Hein, Anas Nashif, Peter Christ, Roman Kellner, Tobias Kästner, Nicole Pappler, Francesco Sforza

Meeting Recording:

https://zoom.us/rec/share/Mxl48GcKpDqFQAiFzDS8ULILEJxmpM5MfRMd3UxRRDDoIQ3KeaKuXF6wX14Ztsn.M0sFJBj_Es-oXFeR

Agenda:

- Opens
- Update on StrictDoc [stanislav]
- WG planning 2024:
 - <https://github.com/zephyrproject-rtos/zephyr/issues/61500>
 - LTS3 is 3.7
 - Focus topics
 - Requirements
 - Coding guidelines
 - Goals
 - Requirements:
 - Get the number of layers fixed defined
 - Populate every layer with one valid requirement and define the process
 - Trace one requirement to the source code
 - How to achieve the goals
 - Volunteers to take over topics to work parallel on topics
 - Pick one Req and define and drag it through the process
 - AI -Simon - Continue the discussion offline.
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Zephyr Requirements - <https://github.com/zephyrproject-rtos/reqmgt>
 - <https://github.com/zephyrproject-rtos/reqmgt/pull/15>
 - <https://github.com/zephyrproject-rtos/reqmgt/issues/23>
- Round Table

Upcoming Agenda/Topics:

- Next Meeting (January 30, 2024)

Open Topics

- Requirements:
- Architecture Specifications
- Coding guidelines
- Tests and test coverage

Resources:

- Project: <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Issue Label: "Safety"
- Discord: <https://discord.com/invite/Ck7jw53nU2>
 - #safety
- Safety Working Group Mail List: <https://lists.zephyrproject.org/g/safety-wg>
 - Calendar: <https://lists.zephyrproject.org/g/safety-wg/calendar>

2023 - Zephyr Safety Working Group

Zephyr Safety Working Group 2023

Permalinks: [Safety Working Group - Google Drive](#)

** For Table of Contents / Document outline, select the  button to the upper left

Prior Years: Safety Working Group Meeting Minutes

- N/A
-

Meeting Information

Ways to join meeting:

1. Join from PC, Mac, iPad, or Android

<https://zoom-lfx.platform.linuxfoundation.org/meeting/95140294824?password=a727e28d-fc7d-4ef5-bc2b-1f7e157931da>

2. Join via audio

One tap mobile:

US: +12532158782,,95140294824# or +13462487799,,95140294824

Or dial:

US: +1 253 215 8782 or +1 346 248 7799 or +1 669 900 6833 or +1 301 715 8592 or +1 312 626 6799 or +1 646 374 8656 or 877 369 0926 (Toll Free) or 855 880 1246 (Toll Free)

Canada: +1 647 374 4685 or +1 647 558 0588 or +1 778 907 2071 or +1 204 272 7920 or +1 438 809 7799 or +1 587 328 1099 or 855 703 8985 (Toll Free)

Meeting ID: 95140294824

Meeting Passcode: 158007

International numbers: <https://zoom.us/j/95140294824>

19 December 2023 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: Nicole Pappler, Peter Christ, Roberto Bagnara, Stanislav Pankevich, Roman Kellner, Tobias Kästner, Francesco Sforza

Meeting Recording:

<https://zoom.us/rec/share/tlYcfCvEUIT0QJTaMpesL8qUIRCjPboswC23YBWsjPPJoM1JO4qW5SyiOLUmdlry.2E6hyMUhcZ6fYM8c>

Agenda:

- Opens
 - WG Meeting 2 January 2024 - canceled
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Zephyr Requirements - <https://github.com/zephyrproject-rtos/reqmgmt>
- Update on StrictDoc Functionality
 - Diff Functionality: same format with two sections for the diff, with MID and e.g. HEAD, all changes are listed with numbers and a description of the change - now it is really possible to count the number of changes. Changes are counted by node.
 - In StrictDoc, all tool requirements are now identified by MIDs, MID is an option that can be enabled. If it is enabled, StrictDoc will generate the MIDs automatically
 - The update is yet not released in the public version, but will be released soon.
 - Decision pending, if we want to use the MIDs for the Zephyr requirements.
- Round Table
 - Software Requirements naming of requirements levels:
 - Before starting starting on StrictDoc, we wanted to use the names from IEC 61508
 - High level requirements and functional requirements as document names do not really fit into what we have - the terms are pretty vague
 - Roman will create an RFC to discuss suitable names in the reqmgmt repo

Upcoming Agenda/Topics:

- Next Meeting (December 19, 2023)

Open Topics

- Requirements:
- Architecture Specifications

Resources:

- Project: <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Issue Label: "Safety"
- Discord: <https://discord.com/invite/Ck7jw53nU2>
 - #safety
- Safety Working Group Mail List: <https://lists.zephyrproject.org/g/safety-wg>
 - Calendar: <https://lists.zephyrproject.org/g/safety-wg/calendar>

5 December 2023 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: Simon Hein, Peter Christ, Erik Berces, Roberto Bagnara, Stanislav Pankevich, Nicole Pappler, Roman Kellner, Tobias Kästner, Jan ?,

Meeting Recording:

https://zoom.us/rec/share/ICsH0kFIF7CxFIQYsQ1I_JzMOznLbSwvB9hYQ_FuHtDcYkCOLsokoMRiAPEV7_Kb.DIQLIzWiSMiV9YD

Agenda:

- Opens
 - WG Meetings 19 December and 2 January 2024
 - Nicole volunteers to host
- StrictDoc tool Update(s) [10 min Stanislav]
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Zephyr Requirements - <https://github.com/zephyrproject-rtos/reqmgmt>
 - Threads PR <https://github.com/zephyrproject-rtos/reqmgmt/pull/15>
- Round Table

Upcoming Agenda/Topics:

- Next Meeting (December 19, 2023)

Open Topics

- Requirements:
- Architecture Specifications

Resources:

- Project: <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Issue Label: "Safety"
- Discord: <https://discord.com/invite/Ck7jw53nU2>
 - #safety
- Safety Working Group Mail List: <https://lists.zephyrproject.org/g/safety-wg>
 - Calendar: <https://lists.zephyrproject.org/g/safety-wg/calendar>

21 November 2023 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees: Simon Hein, Benjamin Cabe, Jim Donlin, Peter Christ, Stanislav Pankevich, Tobias Kästner, Erik Berces, Nicole Pappler, Francesco Sforza, Jan

Meeting Recording:

<https://zoom.us/rec/share/A72aqkXXoLIY5v98k7p7T9MJbyaQNALWiNBt2Rxr4siLorc3o8GXX4yEVgpovsdK.yTxcD2iHIDq2cJqZ>

Agenda:

- Opens
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Zephyr Requirements - <https://github.com/zephyrproject-rtos/reqmgmt>
- Round Table

Upcoming Agenda/Topics:

- Next Meeting (December 05, 2023)

Open Topics

- Requirements:

○

Resources:

- Project: <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Issue Label: "Safety"
- Discord: <https://discord.com/invite/Ck7jw53nU2>
 - #safety
- Safety Working Group Mail List: <https://lists.zephyrproject.org/g/safety-wg>
 - Calendar: <https://lists.zephyrproject.org/g/safety-wg/calendar>

07 November 2023 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees:

- Stanislav Pankevich, Peter Christ, Roberto Bagnara, Tobias Kaestner, Gregory A Shue, Simon Hein, Nicole Pappler

Meeting Recording:

Agenda:

- Opens
 - Update Strict doc
 - Parent/ child statistics improve
 - Currently in the nightly version
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - [New issue on how to define requirements in the repository](#)
- Zephyr Requirements - <https://github.com/zephyrproject-rtos/reqmgmt>
 - Generation of missing requirements IDs is done
 - Component level
 - We can use the existing documentation, but need to change it, formalize it a little bit more (TUV Feedback)
- Round Table

Upcoming Agenda/Topics:

- Next Meeting (November 21, 2023)

Open Topics

- Requirements:
 -

Resources:

- Project: <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Issue Label: "Safety"
- Discord: <https://discord.com/invite/Ck7jw53nU2>
 - #safety
- Safety Working Group Mail List: <https://lists.zephyrproject.org/g/safety-wg>
 - Calendar: <https://lists.zephyrproject.org/g/safety-wg/calendar>

24 October 2023 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees:

- Stanislav Pankevich
- Gergory A Shue
- Simon Hein
- Roberto Bagnara
- Roman Kellner
- Nicole Pappler
- Eric Berces
- Anas Nashif

Meeting Recording:

Agenda:

- Opens
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Closed the issue about UIDs
- Zephyr Requirements - <https://github.com/zephyrproject-rtos/reqmgmt>
 - Requirement Prefixes/ UID handling
 - <https://github.com/zephyrproject-rtos/reqmgmt/issues/7>
 - <https://github.com/zephyrproject-rtos/reqmgmt/pull/9>
 - Component level
 - We can use the approach to specify the APIs as the most detailed level, this has been clarified with the assessor from the certifier
 - Question: how do we deal with unspecified code with this approach

- Requirements for tests need to be set in the verification plan
 - There are also already coding guidelines in place that forbid dead code, also static analysis tools will find dead code
 - Requirements and obligations that prevent dead code or code linked in by the compiler/linker will need to go to the Safety Manual
 - Coverage is in the end not only automatically recorded test coverage, but also coverage by provision of additional information or explanation.
 - We can start writing component level requirements now, we still need an issue for that in the repo
- Update on StrictDoc
 - Req relations and roles have not been implemented and tested
 - File editing is not yet supported in the UI
 - REFS fields are now deprecated, using RELATIONS instead
- StrictDoc updates for Zephyr
 - Naming convention for ZEP-xxxxxx UIDs has been implemented, generated UIDs will be unique per StrictDoc file
 - Request to make Grammar more global has been postponed
 - Current roadmap can be found online in the project
- Questions
 - ZEP prefix relates to requirements related to Zephyr in the sense of namespace, we are currently limiting it to the repository
- Useful Metrics to track Req progress
- Round Table

Upcoming Agenda/Topics:

- Next Meeting (November 7, 2023)

Open Topics

- Requirements:
 -

Resources:

- Project: <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Issue Label: "Safety"
- Discord: <https://discord.com/invite/Ck7jw53nU2>
 - #safety
- Safety Working Group Mail List: <https://lists.zephyrproject.org/g/safety-wg>

- Calendar: <https://lists.zephyrproject.org/g/safety-wg/calendar>

10 October 2023 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees:

- Gregory A Shue, Erik Berces, Stanislav Pankevich, Patrick Ashby, Peter Christ, Anas Nashif, Simon Hein, Nicole Pappler

Meeting Recording:

Agenda:

- Opens
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - No new issues to add and no progress on other
- Zephyr Requirements - <https://github.com/zephyrproject-rtos/reqmgmt>
 - Requirement Prefixes/ UID handling
 - <https://github.com/zephyrproject-rtos/reqmgmt/issues/7>
 - Conclusion of the WG go with ZEP-Number for all req documents to stay portable in the future but avoid conflicts in name spaces
 - Add pro con list how we came to the conclusion

| Criteria (concerns raised by) | Numeric simple (ZEP-001, ZEP-2, ...) | Numeric (ZEP-ARCH-001, ZEP-HIGH-001) (per functional group or per document level/type) | UUID-based |
|---|---|--|--|
| Human readability / communication (Anas) | Most easily readable. | Readable. | Reading (and talking about an UUID) is hard. More opportunities for making mistakes. |
| How easy to create a consistent convention scheme (everyone) | No need to create a schema because ZEP-* is the only prefix. | Needs more work. The created schema can be subject to changes in the future. | No need to create any schemas. |
| Portability: Changing | Moving is | Need to rename | Moving is |

| | | | |
|---|--|--|---|
| from one naming schema to another / moving requirements between documents or sections (Stanislav, Peter) | straightforward. | requirement prefixes when moving requirements around. Need to establish a new convention in the future. | straightforward. |
| Support by all requirements tools (Nicole) | Definitely supported. | Very likely supported. | May not be supported |
| Handling collisions when doing parallel work. (previous SWG meeting) | Collisions are expected but they can be resolved when rebasing the requirement branches against the latest main requirements branch. | Collisions are expected but they can be resolved when rebasing the requirement branches against the latest main requirements branch. | Collisions are not possible. |
| Implications for other projects with requirements (Greg) | ZEP- means Zephyr. Everything else is not affected. | Implications are not clearly understood yet due to lack of information. Example: Understanding and relying on an elaborate ZEP-*-schema can cause confusion by the downstream users. | UUIDs do not influence anything in the downstream projects. |
| Work across repositories | A simple numeric prefix can only work within a single repository. | The chosen prefixes can only work within a single repository. | Full flexibility. |

- Useful Metrics to track Req progress
- Round Table

Upcoming Agenda/Topics:

- Next Meeting (October 24, 2023)

Open Topics

- Requirements:
 -

Resources:

- Project: <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Issue Label: "Safety"
- Discord: <https://discord.com/invite/Ck7jw53nU2>
 - #safety
- Safety Working Group Mail List: <https://lists.zephyrproject.org/g/safety-wg>
 - Calendar: <https://lists.zephyrproject.org/g/safety-wg/calendar>

26 September 2023 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees:

- Stanislav Pankevic, Patrick Ashby, Peter Christ, Nicole papperl, Erik Berces, Hein Simon, Roman Kellner, Anas Nashif, Christian Schlotter, Benjamin Cabe, Tobias Kaestner, Stephan Linz, Roberto Bagnara

Meeting Recording:

https://drive.google.com/file/d/1FF1Br28vAyJU0Uky8a4POkP_LW_2471H/view?usp=sharing

Agenda:

- Opens
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Zephyr Requirements - <https://github.com/zephyrproject-rtos/reqmgmt>
- - Requirement Prefixes/ UID handling
 - <https://github.com/zephyrproject-rtos/reqmgmt/issues/7>
 - Main topics for today:
 - Prefixes and convention of UID
 - Useful Metrics to track Req progress
- Round Table

Upcoming Agenda/Topics:

- Next Meeting (September 26, 2023)

Open Topics

- Requirements:
 -

Resources:

- Project: <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Issue Label: "Safety"
- Discord: <https://discord.com/invite/Ck7jw53nU2>
 - #safety
- Safety Working Group Mail List: <https://lists.zephyrproject.org/g/safety-wg>
 - Calendar: <https://lists.zephyrproject.org/g/safety-wg/calendar>

12 September 2023 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees:

- Tammy Leino, Stanislav Pankevich, Peter Christ, Roman Kellner, Nicole Papperl, Patrick Ashby, Nadav, Roperto Bagnara, Gregory A Shue, Kate Stewart, Benjamin Cabe, Tobias Kaestner, Christian Schlotter

Meeting Recording:

<https://drive.google.com/file/d/1QgydtFtoGijc1bYfpZyXbyey9nRDUCC9/view?usp=sharing>

Agenda:

- Opens
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Zephyr Requirements
 - Requirement doc structure/s
 - Requirement Prefixes
 - UID handling
 - StrictDoc configuration
 - Common field definition for all SRS, SAIS, SCDS sdoc's

- Link naming: parent / child vs refines, refines, implements etc. as in and out
- Round Table

Upcoming Agenda/Topics:

- Next Meeting (September 26, 2023)

Open Topics

- Requirements:
 - Useful Metrics to track Req progress

Resources:

- Project: <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Issue Label: "Safety"
- Discord: <https://discord.com/invite/Ck7jw53nU2>
 - #safety
- Safety Working Group Mail List: <https://lists.zephyrproject.org/g/safety-wg>
 - Calendar: <https://lists.zephyrproject.org/g/safety-wg/calendar>

29 August 2023 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees:

- Roberto Bagnara, Tammy Leino, Simon Hein, Peter Christ, Stanislav Pankevich, Benjamin Cabe, Patrick Ashby, Tobias Kaestner, Gregory A Shue, Nicole Papperl, Christian Schlotter, Francesco, Nashif Anas, Kate Stewart

Meeting Recording:

<https://drive.google.com/file/d/1Rd6tHzQTW1OX03rZeQ9qlfWWuCet7pW/view?usp=sharing>

Agenda:

- Opens
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Zephyr Requirements update
 - Slides: 📄 2023-08-29 - Update on Zephyr requirements work
 - PR: <https://github.com/zephyrproject-rtos/reqmgmt/pull/4>

- Round Table

Upcoming Agenda/Topics:

- Next Meeting (September 12, 2023)

Open Topics

- Requirements:
 - Requirement Prefix
 - Useful Metrics to track Req progress

Resources:

- Project: <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Issue Label: "Safety"
- Discord: <https://discord.com/invite/Ck7jw53nU2>
 - #safety
- Safety Working Group Mail List: <https://lists.zephyrproject.org/g/safety-wg>
 - Calendar: <https://lists.zephyrproject.org/g/safety-wg/calendar>

15 August 2023 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees:

- Gregory A Shue, Roberto Bagnara, Tobias Kaestner, David Brown, Stanislav Pankevich, Simon Hein, Anas Nashif, Christian Schlotter, Roman Kellner

Meeting Recording:

Agenda:

- Opens
 - Cadence of the WG stays at it is for now because of the TÜV Engagement and organization topics around the committee
- Req tooling decision and next steps
 -  Requirement Tool
 - <https://github.com/zephyrproject-rtos/zephyr/issues/57703>
 - Decision of the committee was for the req tooling: Go on with StrictDoc as tool of choice

- No objections from the working group to go with StrictDoc
- Has this decision been synchronized with other Committees like the security committee?
- No, but does this need to be done?
- The way it would be done is that this group which drives the effort and the topic will report up to the project and present their recommendation and how this can be done and if it is feasible the final decision would be made on a project level.
- Next Steps:
 - Putting a “PoC” together with real data. And who wants to volunteer in driving this effort?
 - Is a PoC really what we need? Poc were made to evaluate the tool itself
 - PoC was the wrong wording here, more like a real example.
 - How should we move forward with the req topic should it be integrated into the tree from day one or should it be started in an extra repository
 - **Conclusion:** Best way to move fast forward with the requirements is to start within a separate repository and start writing requirements in there. Test on that repository the handling and use cases of the tool and also the limits of the tooling we might face. From this base we can think about moving it into the tree or how we want to do it in the future.
 - Simon And Stanislav will setup the repository and move the Safety Committee Requirements into the repository which is already created: <https://github.com/zephyrproject-rtos/reqmgmt>
 - After that it will be published via the mailing list and everyone who is interested can write requirements.
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - <https://github.com/zephyrproject-rtos/zephyr/issues/58882> -> No progress Tobias was on vacation
 - <https://github.com/zephyrproject-rtos/zephyr/issues/57703> -> Will be closed after tool decision
 - <https://github.com/zephyrproject-rtos/zephyr/issues/58903> -> Simon couldn't work on the topic and was facing some problems with the Build system. Will connect with the tool chain wg
- Round Table

Upcoming Agenda/Topics:

- Next Meeting (August 29, 2023):
 -

Resources:

- Project: <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Issue Label: "Safety"
- Discord: <https://discord.com/invite/Ck7jw53nU2>
 - #safety
- Safety Working Group Mail List: <https://lists.zephyrproject.org/g/safety-wg>
 - Calendar: <https://lists.zephyrproject.org/g/safety-wg/calendar>

01 August 2023 - Meeting Canceled

** See Meeting Dial-In Information in the header

Attendees:

-

Meeting Recording:

Agenda:

- Opens
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - New Issues / Tasks and who will volunteer to drive topics?
- Req tooling: How to come to a conclusion and decision
- Round Table

Upcoming Agenda/Topics:

- Next Meeting (August 8, 2023):
 -

Resources:

- Project: <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Issue Label: "Safety"
- Discord: <https://discord.com/invite/Ck7jw53nU2>
 - #safety
- Safety Working Group Mail List: <https://lists.zephyrproject.org/g/safety-wg>
 - Calendar: <https://lists.zephyrproject.org/g/safety-wg/calendar>

18 July 2023 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header


Attendees:

- Peter Christ, Gregory A Shue, Tammy Leino, Maryna Balioura, Anas Nashif, Nicole Pappler, Patrick Ashby, Robert Bagnara, Christian Schlotter, Francesco Sforza, Stansilav Pankevich, Benjamin Cabe, Simon Hein

Meeting Recording:

<https://drive.google.com/file/d/12HjOoG6f8MzIHxJkSHUeWCE7idEQxGxm/view?usp=sharing>

Agenda:

- Opens
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req: StrictDoc PoC [Stanislav] [~40min with Q & A]
 - Slides:  2023-07 – Zephyr and StrictDoc.pdf
- Round Table

Upcoming Agenda/Topics:

- Next Meeting (August 1, 2023):
 -

Resources:

- Project: <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Issue Label: "Safety"
- Discord: <https://discord.com/invite/Ck7jw53nU2>
 - #safety
- Safety Working Group Mail List: <https://lists.zephyrproject.org/g/safety-wg>
 - Calendar: <https://lists.zephyrproject.org/g/safety-wg/calendar>

4 July 2023 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees:

- Stanislav Pankevich, Tobias Kaestner, Nicole Pappler, Peter Christ, Christian Schlotter, Benjamin Cabe, Roman Kellner, Johann Fischer, Roberto Bagnara, Simon Hein

Meeting Recording:

https://drive.google.com/file/d/1eQKk_87OfcPDEfYlfBO8ZsDppgEsnrHy/view?usp=sharing

Agenda:

- Opens
 -
- Safety WG - Further proceeding planning
 - Project board
 - Monitor on what people are working
 - Present what status
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Req: Sphinx Needs - first approach [Roman]
- Round Table

Upcoming Agenda/Topics:

- Next Meeting (July 18, 2023):
 -

Resources:

- Project: <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Issue Label: "Safety"
- Discord: <https://discord.com/invite/Ck7jw53nU2>
 - #safety
- Safety Working Group Mail List: <https://lists.zephyrproject.org/g/safety-wg>
 - Calendar: <https://lists.zephyrproject.org/g/safety-wg/calendar>

20 June 2023 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees:

- Kaestner Tobias, Christ Peter, Ashby Patrick, Pankevic Stanislav, Schlotter Christian, Nicole Pappler, Hein Simon, Gregory A Shue, Sofrza Francesco, Karthik Veluswamy, Kellner Roman

Agenda:

MEETING MINUTE recording:

https://drive.google.com/file/d/1Kfb4kz-4jOt4u6UQjC_1Rc0GKqKclsGz/view?usp=drive_link

- Opens
 - EOSS participation: 5 from the WG will come
 - Overview Presentation: Question about the Access table which was added again if it is old. Answer yes the topic is still under work and the one in the presentation is the old one
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Round Table

Upcoming Agenda/Topics:

- Next Meeting (July 4, 2023):
 -

Resources:

- Project: <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Issue Label: "Safety"
- Discord: <https://discord.com/invite/Ck7jw53nU2>
 - #safety
- Safety Working Group Mail List: <https://lists.zephyrproject.org/g/safety-wg>
 - Calendar: <https://lists.zephyrproject.org/g/safety-wg/calendar>

06 June 2023 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees:

- Roberto Bagnara, Tammy Leino, Nicole Pappler, Roman Kellner, Tobias Kaestner, Peter Christ, Patrick Ashby, Stephan Linz, Christian Schlotter, Simon Hein

Agenda:

- Opens:
 - Handle meeting minutes: Recording meetings and link it in here as minutes
 - Would also be good if someone is on vacation and wants to follow up
 - Simon need to get in contact with Brett to be able to record

- Starting scope proposal ([Safety starting scope proposal · Issue #57702 · zephyrproject-rtos/zephyr · GitHub](#))
 - Update Safety Committee consensus (committee meeting 30.05.2023): Starting scope is folder kernel/* , without SMP in the starting scope
 - Question RFC process stay open to be extended?
 - It will normally be closed because the starting scope is defined for now
 - Stays open because simon is adding scripting via pull request to identify the starting scope and scope in general
 - If the scope is extended the safety committee needs to agree on it.
 - But most of the safety committee members are also in the call, so the agreement is a formality which needs to be discussed and documented in the committee meeting
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Intention and expectation of this Project is that people from this group can add gaps which they want to close to work towards the safety effort of the project and to track the progress on closing the gaps.
 - Tobias created one issue of these gaps <https://github.com/zephyrproject-rtos/zephyr/issues/58882>
 - He is missing the basic tracing in the documentation of what functionality (e.g mutex) where tested where?
 - Add label Safety into the issue. If you can't post it in the safety channel or message Simon in it to add the label or mention Simon (GH account: simhein) in the issue to add the label for you.
- Round Table
 - Info Regarding the issue from Tobias: There is a traceability tooling PoC
 - Starting from scratch would not make sense
 - Instead of linking test cases to api functionality requirements linking would be better
 - AI-Simon Link PoC of traceability tooling into the issue
 - Requirements:
 - Regarding Tooling would it be good to write Requirements for the tooling itself?
 - The tooling is one topic and the documentation or export of the Reqs are another one
 - Consider the Integration of the Req into the code repository itself instead of an extra repository to make it easier to differentiate between user documentation and requirement documentation in the end.
 - Writing detailed Req for the Requirements tooling itself might take another year to get to a tooling decision
 - Roberto Volunteer to present strictDoc to the group and what is possible with strictDoc
 - 2 examples for the presentation

- One with code and the other one was requirements with documents and specifications only
 - Decision was to use the one with code.
- Tobias look into the RTEMSvariant and could present the difference to strictDocs after Roberto's presentation
- Proposal Tobias: To move on with the Tooling topic compare the tools with the same examples
 - Only allow another tool option if a community member will contribute to also try it with the example
 - Time box the “challenge” to implement such a sample on a specific tooling
 - After the time we can choose the tooling which fits the best and if there is only one example with a tool presented then we go with this.
- Roman will add expectations for the tooling and with what the evaluation examples will be measured into the Issue
<https://github.com/zephyrproject-rtos/zephyr/issues/57703>
- Question: What options of tools are available?
 - Doorstop
 - StrictDoc
 - Sphinx needs
 - Open needs?
 - RTEMS
- Peter: UID should be unique and a number with an addition maybe
- What is with open needs`?
 - Concept phase and state funded
 - Nicole does not recommend state funded projects because the tools could be gone and not continued if the fund drops.
- Next Steps: Roman start adding the expectations for the tool and the examples in the issue and other should add also missing expectations into the issue

Upcoming Agenda/Topics:

- Next Meeting (June 20, 2023):
 -

Resources:

- Project: <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Issue Label: “Safety”
- Discord: <https://discord.com/invite/Ck7jw53nU2>
 - #safety

- Safety Working Group Mail List: <https://lists.zephyrproject.org/g/safety-wg>
 - Calendar: <https://lists.zephyrproject.org/g/safety-wg/calendar>

23 May 2023 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees:

- Benjamin Cabe, Brett Preston, Christian Schlotter, David Brown, Francesco Sforza, Gregory Shue, Kevin Townsend, Kumar Gala, Patrick Ashby, Peter Christ, Roberto Bagnara, Simon Hein, Tammy Leino, Tobias Kaestner

Agenda:

- Opens
 - WG Cadence
 - Will increase cadence to first, second and third Tuesday of each month, starting in August // working to clear some topics in the Safety Committee first
- Safety development concept (RFC: [Safety development concept](#)) - short follow up
 - Would it make sense to break the diagram up into smaller packages?
 - Discussion around the 3 big topics:
 - Requirements Management
 - Scope Handling
 - Coding Guidelines
 - Conclusion around how we can proceed with some of the topics of the concept?
 - Greg: Need alignment on Does the requirement management tool have to meet the needs of Safety and Security?
 - David B: What are the requirements of the requirements tool? Can we find enough overlap?
 - Greg: Both safety and security are related to quality. Most of the content has to apply to both the safety and security view of things. A few items unique to each of those views. Lots of motivation for using the same tool.
 - At the requirements level, eventually they need to describe the same system
 - David B: Important to be able to resolve what may come across as conflicts
 - Simon: Requirement tooling itself - Does it need to have special cases besides filtering, tagging in a special way?
 - Greg: I need to be able to have a tool that supports development of the HALs that the chip vendor provides, that's developed to a secure/safety lifecycle; but it's going to be in a different module. Capturing content across modules and linking them together appears to be lacking from

doorstop. Need to come to alignment on what is the scope on where the requirements are going to be captured and how they are going to be related together.

- Simon: If we speak of scope, we need to be careful what scope we need
- Greg: Multiple definitions of scope. Build system allows me to inherit drivers from other parties. One option for defining scope: what's inside of the executable. Don't think we can talk about just one scope. Have to be clear about which one we're talking about when.
- Tobias: Would like to see a safety manual. Important that we can grow the scope over time. Zephyr is content (kernel, drivers) but also the meta system (building, config). Responsibility of the upstream project to provide tools that downstream modules can also use.
- Greg: Product line terminology discussion in the TSC - <https://github.com/zephyrproject-rtos/zephyr/issues/44528>
- Simon: Processes and scope both need to be extended. First certification/pre cert needs to be on a little scope.
- Tobias: Needs to be a process that would allow continuous updates
- Tobias: Should be possible at some point in time to make it extendable
- Greg: Zephyr mission/vision statement – one of the most difficult things that is committed to in those statements refers to the accessibility of the certification artifacts. Available to platinum members. Does process support reusing Zephyr in a downstream integration without touching any of the SHAs in Zephyr. Would be a requirement on whatever solution – must support the ability for the certified artifacts to get reused at the SHA; in order to meet what's committed to in the mission statement.
- Greg: Does this option support the reuse implied in the mission statement?
- Simon: If you take the Safety release and build up an application on it, the artifacts bring value in that you don't need to certify that part of Zephyr in your product again. You only need to do the application certification. Are you not allowed to change something if you can justify that it can still work as intended?
 - Tobias: Agree. You have to justify it.
- Tobias: Whatever we do in Safety should go in accordance with what we see in upstream.
- Simon: Pinning down on a release. Mission of Safety Committee/WG is on the main branch
- Greg: If there is a security issue with a safety critical product, it's going to need to be addressed also. Security is going to drive us to continuous delivery of safety. Because of having to delivery security fixes in a timely manner (30-60 days), we will need to imagine this as needing to be a continuous delivery stream of safety certification stream. Everybody who is pulling in has to have the freedom to reproduce their own artifacts. What are restrictions on how Zephyr gets integrated into an end product.

Have to be thinking about this as a continuous delivery of safety certifiable content.

- Tobias: Agree - must be automated
- Simon: Keeping in mind things will be pulled in later on, starting with the basic things. Start with something; define the process.
- Greg: Have started using doorstep before; found that doorstep does not natively have an ability for referencing requirements outside the repo that it is in.
- Greg: What is the range we are going to measure these tools by.
- Greg: The breakdown of documents (on the left) - do those need their own separate releases/baselines? How do those layers get affected when these things get integrated into downstream projects? What is the mechanism of submodule providing? Does this stuff scale?
- Greg: Need to figure out scalability
- Tobias: Look at RTEMS – they have a working process and tools. Futureproof of extensibility of submodules. Tying nicely into sphinx is nice given it ties into documentation. Have a way that whatever downstream is happening being contributed back into upstream.
- Tobias: Suggest working on a proof of concept over the next couple of weeks with different tools.
- Simon: Gathering detailed requirements from existing code is something people are looking for
- Simon: Starting out with the tooling to contribute the requirements itself would help to go forward; but don't leave behind potential for a better option for scaling
- Simon: Tooling will prove itself when it's used. Can approve tools only if we start writing requirements
- Greg: Connected IoT devices - need to recognize that requirements engineering starts at the stakeholder/systems level. Zephyr is coming into the middle of a much larger problem space. We shouldn't think that it starts with Zephyr requirements. How does Zephyr fit into what the users are already needing?
- Greg: The system is much larger than the device. You may choose to use Zephyr's tooling, but if Zephyr's tooling won't support doing things at the systems level, that's not a practical option
- Simon: Will follow up on the task where this was discussed.
- Tobias:
 - Looking at the picture, process may get too complicated from the get-go; stall activity
 - Should leverage what could be learned from [RTEMS](#) project
 - Comment:
<https://github.com/zephyrproject-rtos/zephyr/issues/57516#issuecomment-1535758682>
 - **AI - Simon:** Follow up with RTEMS / invite to Safety WG meeting?

- Starting scope proposal ([Safety starting scope proposal · Issue #57702 · zephyrproject-rtos/zephyr · GitHub](#))
- Safety WG Project - <https://github.com/orgs/zephyrproject-rtos/projects/23>
- Round Table

Upcoming Agenda/Topics:

- Next Meeting (June 6, 2023):
 -

Resources:

- Project: <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Issue Label: “Safety”
- Discord: <https://discord.com/invite/Ck7jw53nU2>
 - #safety
- Safety Working Group Mail List: <https://lists.zephyrproject.org/g/safety-wg>
 - Calendar: <https://lists.zephyrproject.org/g/safety-wg/calendar>

09 May 2023 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees:

- Anas Nashif, Benjamin Cabe, Brett Preston, Francesco Sforza, Gregory Shue, Johann Fischer, Patrick Ashby, Peter Christ, Roberto Baganara, Roman Kellner, Stephanos Ioannidis, Tammy Leino

Agenda:

- Opens
 - Introduction from Tammy (Siemens)
 - WG Cadence
 - Currently biweekly
 - Propose increasing cadence of the WG to 3x/month
 - No objections to the proposal
 - **Next Step:** Roman will work with Simon to update
- Safety development concept (RFC: [Safety development concept](#))
 - RQM
 - Doorstop was decided upon by the Safety Committee // up to the Committee on whether to revisit
 - Would generated requirements be visible to all, or restricted to Platinum Members?

- End goal would be that everything is covered by requirements, not restricted to safety
 - Are we planning on investing in any improvements in Doorstop?
 - Decision has been made. If a volunteer would like to run a comparison across requirements tools, then the evaluation could be brought back to the Committee to see if they would like to revisit.
 - Greg volunteered to participate in the evaluation task // set up task/Issue
 - Current plan is to start with Doorstop
- Scope Handling
 - Need to define and control what is in/out of scope
 - Concept outlined in RFC – The safety scope as defined will be marked using two mechanisms: SPDX and maintainer.yml
 - First, we need to define what is the problem we are trying to solve. SPDX/maintainer.yml are implementation details.
 - Reason to do this is to keep it under control; people understand what is in safety scope and what is not.
 - The way Zephyr is structured/built/how we manage features - is that suitable right now. Can you carve a piece of that and say that part is certifiable. Is Zephyr ready for this? A lot of dependencies have been added over the years. Can we take a small part of this, and say this limited scope is certified (and how do we manage that).
 - A lot of things need to be looked at. Need to figure out how all of this is going to work in the end // once you have defined the scope, how do you manage that?
 - Once scope is defined, we need a mechanism to control it in the end
 - As a user, if I build something and configure the build environment using Kconfig, want to ensure that I stay in my safety scope for what I want to build
 - SPDX is a part of it. Need to manage at the Kconfig level.
 - Look at the scope / what we are trying to certify. Figure out how it can be certified/managed in a way that does not interfere.
 - When it comes to files, we want to ensure enough isolation.
 - Safest way to make this work may be by identifying folders
 - By partitioning Zephyr to allow the scope to be managed
 - The approach of marking files will leave you always playing catch-up
 - Possibly have architectural constraints at the moment that we need to resolve
 - Need verification of layering in Zephyr. Able to build a basic application without pulling too much unnecessary stuff. Figure out how to partition. Add to the scope without interference. One of the

major problems we have right now is headers/how we include headers. When you build an application, you are pulling more than you need.

- If we do based on what we have right now, we will be adding hundreds/thousands of files
- If you use SPDX and have an implementation file that is marked to be in the safety scope, which includes headers, if they appear in SPDX report - you would see tons of headers that come from stacks not marked as part of the Safety Scope.
 - Before we go there, we need to evaluate Zephyr as ready for it
 - Try to solve some of the problems – layering, headers – first
- Need to have a tool environment that supports keeping safety scope under control; and coding guidelines in line.
- Need the framework // can work on items in parallel
- Coding Guidelines
 - Commercial vs Open Source Tooling // potential for too many false positives
 - Maintaining one tool is already a lot of work
 - Have to differentiate between campaigns and the occasional contributor
 - Major gap that we have right now is figuring out workflow; that makes it easy for us to verify changes
 - Consistency is important
 - With supported commercial tooling
 - For someone focused on fixing coding guidelines violations, figure out how developers can have access to the full suite of tools
 - Recently tested CPP check on professional test suite. Test suite does not cover all MISRA guidelines. CPP check has a high rate of false positives and false negatives.
 - False positives – Developers will attempt to change code if they see a violation
 - Consider talking with folks at trustedfirmware.org // they have complex CI structure
 - They are using Eclair in the CI
 - One of the problems with current tool is the time to run
- SCA
- Starting scope proposal (<https://github.com/zephyrproject-rtos/zephyr/issues/57702>)
- Round Table
 - Major Topics // need to figure out how we can proceed + move in parallel. Divide and conquer
 - Requirement System
 - Coding Guidelines

- Scope/Marketing Scope
- Consider subgroups dedicated to each of the topics / solution proposals

Upcoming Agenda/Topics:

- Next Meeting (May 23, 2023):
 -

Resources:

- Project: <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Issue Label: "Safety"
- Discord: <https://discord.com/invite/Ck7jw53nU2>
 - #safety
- Safety Working Group Mail List: <https://lists.zephyrproject.org/g/safety-wg>
 - Calendar: <https://lists.zephyrproject.org/g/safety-wg/calendar>

25 April 2023 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees:

- Benjamin Cabe, Brett Preston, Christian Schlotter, Greg Shue, Igor Misic, Nicole Pappler, Peter Christ, Roberto Bagnara, Roman Kellner, Simon Hein, Stephanos Ioannidis, Timo Kuehn

Agenda:

- Opens
 - Zephyr Project page - Overview Presentation
 - Former presentation included Safety Committee excel slide (Safety Collateral proposal) that was removed - Why?
 - Removed as it's still being discussed (primarily around the sharing model)
- Continue scope discussion
 - Reference [Safety Scope slides](#) (slide 5)
 - Simon - From the perspective of the Committee, discussed scope - what should go in/out
 - Proposed: We shouldn't define the whole scope at once. Going a step back and picking essential features; start with an initial WG Safety Scope. Can be expanded if necessary. Set a focus area where we can concentrate (requirements, testing, coding guidelines...)

- Greg - Building products that don't use a RTOS // minimal configuration. No scheduler/drivers there. Are there boxes that we should move outside of the Zephyr box to represent the scalability and composability of this?
 - Simon - Possibly
 - Greg - There were still some pieces of code related to fatal errors. Had to have a device tree description of the cpu core. Weren't any timers, memory heaps, condition variables, mmu. Entirely usable configuration of Zephyr that doesn't actually have an os as a c runtime environment
 - Greg - If we are trying to diagram what is inside the Zephyr OS, we may need to tweak a little bit.
 - Simon - Most people use Zephyr as RTOS
 - Update the title of the slide? Only a portion is actual RTOS
- Peter - One needs deeper insight into the architecture of Zephyr to properly just the diagram. What would be the SBOM if we were only to configure the minimum project. What would be left of the diagram.
- Greg - minimum configuration doesn't use Zephyr APIs to do anything
- Greg - For the minimal config build, likely has versions and fatal errors, and maybe common architecture interfaces
- Greg - Change title of diagram and not have implication on our scope discussion? As long as we recognize that Zephyr is composable, that might have an impact on our discussion. Content is all stuff we need to be mindful of at some point.
- Greg - update title to Zephyr Safety Scope?
- Simon - pick essential blocks for the Working Group
- Greg - Haven't seen pad/pin control / gpio control – may need to be boxes for?
- Roman - looking at other comparable rtos, don't include hardware. You have to do that on your own.
- Greg - These are things provided with Zephyr
- Roman - Isn't that device model?
- Simon - First scope / safety certification should be hardware agnostic.
- Simon - Thinking to create an issue / recap of discussions tied to Scope (for better tracking / discussion than in the meeting minutes)
 - Roman: +1, helps for offline discussion // RFC Safety Scope
- Roman - always discussing the diagram; Size of the boxes doesn't say anything about the complexity.
- Roman - We need is a list of code that shall be in the scope and what shall not
- Simon - Discussion around how we can proceed from the picture to concentrate on 5-6 of the points // start to work on things like requirements for the 5 items identified
- Peter - start with points that will be used by every user // minimum configuration
- Simon - first thing is to get the minimum configuration right
- Take Issue. Write down a list with boxes as titles. Give priorities. What should be done first.
- What will be drawn into a binary by that philosopher sample application

- It may be too simple. Doesn't include an interrupt controller driver.
- Simplest will at least involve interrupts and timers?
- If we are blocked in defining what is in the scope, this is a good approach
 - Focus on what everyone is using // in parallel, figure out which additional blocks we want to look at as well
- Simon - we need to start somewhere
- Roman - if we want to do a minimal application, probably have some interrupts, some timers, fill it with peripherals in some way. Everything that becomes microspecific is out of scope. Minimal application: main loop, single thread, some hardware timers (expand to multithreading?). Do we have such a sample application?
- Greg - Do we have a Test Case that exercises the above? When we build an executable image, starting with config file; we don't have to have any logic in that project that's getting built. Can be a non-zero length empty file. Zephyr profiles a definition of main as a default. Any tests that we have that configure the system for the scope that we're talking about? Test that the interrupt api works. Tests of the kernel services.
- Roman - looking at samples // minimal sample application has several configurations
- Greg - we can also specify our own test cast for this. This is the functionality that we are exercising at this point
- Greg - Move on to requirements and start to fill in on the most common needed for the blocks. Will help us reveal what are natural partitions
- Simon - Start with sample application
- Greg - Start with user needs? Capture user needs and then choose a sample that meets the user needs. Higher level user needs – need to be able to reflash a device. I need to be able to configure a device for the functionality that I need.
- Greg - need to have a system that supports an immutable bootloader.
- Simon - we have a Zephyr RTOS, and the RTOS has functionality
- Greg - what we don't know is if the existing Zephyr functionality actually meets user needs
- Roman - don't want to certify an entire ecosystem. Trying to get the inner core / basic functionality...
- Greg - Portion of the system that you are certifying must also meet those other requirements
- Simon - it meets the requirements of the users. If it doesn't, someone would need it
- Greg - we have to gather the user needs
- Simon - that is not the work of the Safety WG
- Greg - Safety WG is concerned with some of the requirements that must be fulfilled.
- Greg - we don't have to certify everything, but we have to recognize that there are high level requirements that whatever portion we are certifying must fit within
- Roman - can't take it all in scope

- Greg - get a requirement structure in place. Begin to populate layers and dependencies. Capture what are the dependencies that the portions we are looking to safety certify are also having to meet
- Greg - whatever tool we use for capturing requirements, has to be used for all requirements across the entirety of the Project
- Simon - want minimal scope defined; for Safety WG to work within the tool. The goal is that the Safety WG wants to find a way to make it happen that an open source project does a safety certified RTOS.
- Simon - Before we go into the requirements discussion, start with limited scope. In the end, need the safety scope for the horizon goal.
- Greg - Can we formalize the proposal of interrupt, timer, fatal errors / that we start with
- **Next Step:** Simon will propose the blocks over an Issue, announced over the mailing list
- Draft Safety Environment Overview (idea from committee)
 - Propose that we do the same for the tool environment
 - **Next Step:** Will raise as an Issue in a RFC, announcing over the mailing list
- Round Table

Upcoming Agenda/Topics:

- Next Meeting (May 9, 2023):
 -

Resources:

- Project: <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Issue Label: "Safety"
- Discord: <https://discord.com/invite/Ck7jw53nU2>
 - #safety
- Safety Working Group Mail List: <https://lists.zephyrproject.org/g/safety-wg>
 - Calendar: <https://lists.zephyrproject.org/g/safety-wg/calendar>

11 April 2023 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees:

- Anas Nashif
- Benjamin Cabe
- Brett Preston
- Christian Schlotter
- David Brown

- Gregory Shue
- Johann Fischer
- Nicole Pappler
- Patrick Ashby
- Philipp Ahmann
- Roberto Bagnara
- Roman Kellner
- Simon Hein
- Stephanos Ioannidis
- Timo Kuehn
- Timo Wilkening

Agenda:

- Short Intro Infrastructure
 - <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - safety label created
 - How to set up panels/boards. What additional boards may be needed
 - Greg: Discussing issues that are common with the secure development process. Discussion and management around how we get a common process that works for safety and works for security. How to make distinct from issues that are pure safety. Need to come up with one process that works for both – requirements, ... // How to identify what is common versus what is safety unique. Would it make sense to have a different board for the stuff that's common? Tooling, Issues, How we manage requirements. As we talk about process, will need a solution that works for both.
 - Nicole: we need to align Safety and Security practices. Security ppl are looking at how Safety is going to start doing things.
 - Anas: +1 – this is the beginning of the Safety WG so let's focus on what parts of Zephyr we are going to touch, and which parts we are going to gather requirements for.
- Scope/s
 - Simon presented an initial slide deck with the proposed scope [\[\[Presentation Slides\]\]](#)
 - Focus should be the RTOS itself – not the larger “Zephyr framework”
 - Safety / Certification scope: the kernel + dependencies the kernel needs to run
 - Greg: where's the “cut” re: API boundaries, ex. libc? What is the explicit list of what is “outside”
 - Roman: maybe the diagram could be updated to capture this.
 - Greg: we need to capture a description of what we're currently addressing/not addressing w.r.t catastrophic -mechanical- failures (ex. Cutting the power of a motor)
 - Nicole: we need to address this with the requirements at least: here's what is addressed by Zephyr // here's what's addressed by the system integrator
 - Anas: where is userspace?

- Simon: it's missing, as it was originally forgotten in the diagram
- Anas: userspace is going to be a game changer for both security and safety, esp. combined with MPU and the rich API there needs to be addresses.
- Anas: file system and settings are probably auxiliary features. Not even sure if it's currently maintained / pushed forward. So probably could be added later.
- Timo: memory domains, memory protection APIs, not highlighted in the diagram? They are important to help support safety critical scenarios
- David Brown: userspace hasn't helped so far with the kind of vulnerabilities that have been reported to date.
- Roman: does the size of each box need to reflect the complexity better? How do we get to a full picture? Maybe start a collaborative document to map folders to boxes, and involve experts/maintainers for each area?
- Greg: it would be useful to capture the (proprietary) tools that we will use and that we need to be mindful of.
- Anas: start with the kernel, i.e. "something basic that works" with the most minimal dependencies. Try to isolate/delete as much of the non-needed functionality (ex. Bluetooth, networking) to obtain a self-contained code base.
- Roman: that's not enough to define the scope, ex. what's inside vs. what's outside.
- Anas: what are the 3-4 bullets of "this is what we definitely want"?
- Greg: the exercise of clarifying scope will help us identify requirements. Can we get some requirement tooling in place so that Security can leverage it?
- Anas: does Security WG have requirements already captured?

- Round Table

Upcoming Agenda/Topics:

- Next Meeting (April 25, 2023):
 -

Resources:

- Project: <https://github.com/orgs/zephyrproject-rtos/projects/23>
 - Issue Label: "Safety"
- Discord: <https://discord.com/invite/Ck7jw53nU2>
 - #safety
- Safety Working Group Mail List: <https://lists.zephyrproject.org/g/safety-wg>
 - Calendar: <https://lists.zephyrproject.org/g/safety-wg/calendar>

28 March 2023 - Zephyr Project Safety WG

** See Meeting Dial-In Information in the header

Attendees:

- Aleksei Savin (Mujin)
- Anas Nashif (Intel / Zephyr TSC Chair)
- Brett Preston (Zephyr Program Manager)
- Christian Schlotter (Zeiss)
- Florian Guhl (Medical Devices)
- Francesco Sforza (Intel)
- Greg Shue (Legrand)
- Hernan Gutierrez-Vazquez (Qualcomm)
- Johann Fischer (Nordic Semiconductor)
- Kate Stewart (Zephyr Director / LF VP of Dependable Embedded Systems)
- Kevin Townsend (Linaro)
- Nicole Pappler (Zephyr Functional Safety Manager)
- Patrick Ashby (Qualcomm)
- Peter Christ (Medical Devices)
- Philipp Ahmann (ELISA TSC Chair)
- Simon Hein (Baumer / Zephyr Safety Committee / WG Chair / Safety Architect)
- Stefan Grambach (SEW-EURODRIVE)
- Stefan Linz (Navimatix)
- Timo Kuehn (Real Time Systems)
- Timo Wilkening (SEW-EURODRIVE)
- Tobias Kaestner (UL Method Park)

Agenda:

- [Meeting Recording](#)
- Kick-off Presentation - [Slides](#)
 - Introductions
 - Nicole (Functional Safety Manager)
 - Simon (Safety Committee / WG Chair / Safety Architect)
 - Expectations towards the Zephyr OS safety WG?
 - Provide via In-meeting Chat / in # safety Discord channel
 - Which certifications do you prioritize?
 - Provide via In-meeting Chat / in # safety Discord channel
 - Project safety goal
 - IEC 61508 SIL 3 / SC3 Safety Certification (initially limited scope with future growth)
 - Status of Zephyr Safety
 - FSM plan ready for TUV review
 - Test coverage in core modules is high but not yet 100%
 - Coding guidelines not enforced with limited adoption up-stream
 - Requirement process and tool in place but not completely set up and established
 - Requirements and traceability needs to be populated
 - Safety scope defined at block diagram level, mechanism to signal changes to be review need to be determined
 - Questions on Status

- What are the main claims / high level safety requirements for Zephyr?
 - Limited scope / claim all the systematic capability for SIL 3
 - Defining higher level functional requirements is ongoing
 - High level requirements is a gap // need to define and agree upon
- For requirements, will Zephyr do reverse engineering? Or introduce something new?
 - Confirmed. Reverse engineering
- Goal is SIL 3. Main problem that we could run into is that we don't have the needed test coverage in the end; but that is a gap that can still be closed
- Goal of the safety WG
 - Integration of Code Guideline Checks into the CI flow
 - Help improving test coverage in the safety scope
 - Help to write and populate the requirements
 - Help link traceability from tests to test specification
 - Help link requirements to source code and to tests
 - Help reduce coding guideline violations
 - Help setting up or improving tooling and tool evaluation
 - Help in safety documents (architecture diagrams, processes, etc..)
- Difference WG <-> Committee
 - WG
 - Actively contribute work items
 - Evaluate safety use cases of zephyr
 - Committee
 - Planning
 - Steering
 - Approving
 - Certification body engagement
- Contribution
 - How do you plan to contribute?
 - Greg - Contributing requirements from Users of Zephyr. What is needed for both Safe and Secure Devices.
 - Kevin - Open Source Certified Safety RTOS. Open handling of artifacts. What will be the availability of those certification artifacts? Or only the intermediate artifacts that will be openly available?
 - Artifact availability is under discussion in the Committee, as well as the Board
 - Anas - Missing planning/roadmap part. Contribute to what? We need to have a lot of things defined and planned, so that any contribution happens at the right time; and within the right context/scope. Items that need to be agreed upon first include: if work is to happen in the main branch, then our target certification code is something that doesn't exist yet. Need to define/update

the scope. re: Requirements - who is going to do the work? A lot of questions that need to be talked about. Need both the input as well as the participation. What do we need to get done first? Shouldn't just be a forum for collecting contributions without getting results.

- Next Steps
 - Call for first topics
 - Send to # safety channel in Discord or the safety-wg mailing list
 - Set up open Safety Project
 - Safety Overview in documentation (Reviews welcome)
- Round table
- Additional links provided via chat
 - Here is the free LF course on SW Engineering I mentioned:
<https://training.linuxfoundation.org/training/software-engineering-basics-for-embedded-systems-lfd116/>

Upcoming Agenda/Topics:

- Next Meeting (April 11, 2023):
 -

Resources:

- Discord: <https://discord.com/invite/Ck7jw53nU2>
 - #safety
- Safety Working Group Mail List: <https://lists.zephyrproject.org/g/safety-wg>
 - Calendar: <https://lists.zephyrproject.org/g/safety-wg/calendar>

Onboarding the Safety Working group

Onboarding the Safety Working group

Useful links

- Read the Safety Working group wiki [Safety Working Group · zephyrproject-rtos/zephyr Wiki](#)
 - Register to the mailing list
 - Register to the meetings
 - Safety Working Group
 - Topical: Requirements
 - Review the GitHub project issues
 - Review the Zephyr Safety Overview & Guidelines
- Be aware of the working repositories
 - Requirements [zephyrproject-rtos/reqmgmt](#)
 - And their doc. version [Zephyr Project Requirements - Project index](#)
 - Safety overview & guidelines [zephyr/doc/safety at main · zephyrproject-rtos/zephyr](#)
- Understand the roles & responsibilities
 - [TSC Project Roles — Zephyr Project Documentation](#)
 - [Repository roles for an organization - GitHub Docs](#)

Contributing

Setup

- Download & Install your favorite code editor and git client
- Setup git [Contribution Guidelines — Zephyr Project Documentation](#)
- Setup a fork [Contribution Guidelines — Zephyr Project Documentation](#)

Working on an issue

Find an issue in [Board · Safety WG](#).

As a contributor, you have 2 ways of showing your interest on working on an issue

1. Commenting on the issue so that it can be assigned to you
2. Directly working on an issue, following [Contribution Guidelines — Zephyr Project Documentation](#) and making a pull request against the issue

Making a pull request

- Follow the Pull request guideline [Contribution Guidelines — Zephyr Project Documentation](#)