Agenda and Minutes: FuSa SIG meeting 21/5/19

Recording download
https://citrix.sharefile.com/d-s278957a93044661b

Attendees

Lars Kurth
Artem Mygaiev
Stefano Stabellini
George Dunlap
Fachin, Vasco (ADITG/ESM1)
Shinya Konishi
Hisao Munakata
Antonio Priore
Francesco Rossi
Julien Grall
Kate Stewart
Alex Agizim

Action Review (Lars)

Completed actions in blue

1. Update SIG charter according to agreed work streams and selected leaders (Artem) – done
2. Create Wiki page to store links to all materials (Lars) – done https://wiki.xenproject.org/wiki/Category:Safety_Certification/FuSa_SIG
3. Create mailing (Lars) – done
4. Check Google Docs access (Lars) – use google docs for now
5. Create boards for streams and provide full access to Trello boards to all members (Artem) – done
6. New meeting invite and administrative items (Lars) – done
7. Missing from previous call: DEFER to future, when there is more clarity on
   - Create project timeline draft. Since it is not clear what shall be "implementation milestones" can fill in only the "scoping" activities
   - Review and agree on critical organizational topics related to scoping efforts and SIG operation

New Actions

1. Francesco to review and propose modifications to charter entry.
   Excerpt from SIG charter for Francesco's convenience - note that Lars wrote this section, but is not attached to it: *Define and implement guidelines and examples related to the verification of requirements, architecture, design and APIs as required for safety certification. Develop a strategy to produce missing documentation and work with the Community*

Interactions and Processes stream to ensure documentation stays up-to-date and is generated where needed.

2. Lars to set up a smaller meeting with Franceso, Kate, Artem & Vasco to walk through the test infrastructure we have. Will talk to Ian Jackson and/or other stake-holders.
3. Lars to add tools we have in the Xen community which might be useful to Kate's list and to remind everyone to provide input to Kate after the initial list is published
4. Francesco to introduce Italian Assessor to Lars and Artem
5. Lars to put together contact details spreadsheet and to publish using a private channel (not fusa-sig@) for privacy/spam-avoidance reasons
    a. Artem to share contact his contact list with Lars
    b. **ALL: record who has access to which standard, such that we could look things up if there is a question, after 6 is complete**

Agenda

Items for Work streams and their leaders

1. Finalize stream owners according to updated charter (done)
2. Set goals - in progress
3. Define what each stream needs in terms of input, resources, etc. – aka identify ideal team composition and review against volunteers - in progress
4. Start populating trello boards - defer until 1 & 2 have progressed more
5. Agree on how to track progress for each stream's group and how to coordinate within group, etc. - defer until 1 & 2 have progressed more

Confirmed Stream Owners

- Safety management system (Artem)
- Documentation (Stefano)
- Verification tests (Francesco)
- Open source community interactions and processes (Lars)
- Process automation tools (Kate)

Updates per Stream

Safety management system (Artem)

Have not got a plan yet. Investigating all the necessary tasks according to safety regulations, which will be followed by a work break down. Make the list public on fusa-sig@
Tasks: breakdown, estimation, plan

Franceso: The first item is defining the safety regulation
Must have items: ISO26262 and IEC 61508

ACTION - DONE: Antonio to add medical standard as there is a significant overlap and it has an agile angle

The standard I've mentioned today for your considerations is IEC 62304 (SW for medical device) which overlaps a lot with IEC 61508 part 3. For this standard, a TIR from the FDA provides guidance on how to apply such standard to an Agile development frameworks.

This might be of interest for some of you and certainly is for us.
See https://my.aami.org/store/detail.aspx?id=TIR45-PDF

Documentation (Stefano)

Has a rough plan in his mind. Checked with Saras what is required. The next step is to collect a list of APIs (aka key interfaces). From there, we can work backwards and find out how easy it is to document Requirements, Architecture, Specs and APIs and to scope out how much time it takes.

Artem: should we get verification from an assessor?

There was a little bit of discussion around this and the group came to the agreement, that in the interest of managing bandwidth available from assessors, we should not involve them assessors too early. Also see notes from Francesco and Artem below

Francesco: got in contact with an italian assessor, who will be able to contribute to this project for free.

Artem: talked to David, Robert, Piotr - they do not want to join every call. If we need, we need to ask.

Antonio, Lars and others agree.

Verification tests (Francesco)

Need to take some time to bootstrap and get familiar with what is in place. Dependency on safety management. Can start without much input. Francesco and Artem need to coordinate in the background

Open source community interactions and processes (Lars)

I have a clear view on potential obstacles and changes and need to write these down.
Most of the detail and complexity to manage the changes are dependent on details of other streams.
What processes we need are fairly independent of this.

Process automation tools (Kate)

Starting off with a google doc with existing tools. Will segment them by FOSS vs proprietary.
Francesco: can we add a category / group of tools. E.g.: Toolchain, tools to support standards, scanning?

Kate agrees. However, the best way to do this would be to refine categories after we have an initial list.

Contribution Model (Artem) - best effort, depending on group's progress, I don't think we'll manage to fit

Contribution model for Assessors - this has to be certainly funded. We need to understand how to get funding in the group (maybe as Kate suggested?)

Lars: enumerates funding options

- Advisory Board, but due to the board composition it is unlikely that any sums but pocket money (e.g. for MISRA-C specs) would be approved
- Research and government grants: there have been multiple examples for this in the past, e.g. through DARPA funding, EU funding, etc.
- A number of interested parties to fund/donate specific activities

Kate: suggests first to see who participates and revisit this topic then

All agree

Kate brings up the topic of Standards, which are not publicly available
Lars asks about the cost
Artem: subset of ISO 26262 costs

- 1000 swiss francs (approx equivalent to 1K USD)
- 300 swiss francs for software version (but there are dependencies on definition and so this is of limited use)
- 2000 swiss francs for the full version

Getting an overview would get rid of most problems with access.

There was a bit of discussion about the practicalities, and we all agreed that there would be no licensing problems if we

- Members who have access to specs, can help the group as long as we only use references and summarize key issues/outcomes
- If we came up with our own standard and wording - although doing this is likely impractical

Agreement: Will record who has access to each standard, such that we could look things up if there is a question

AOB

None