RTEMS-SMP QUALIFICATION

user consultation meeting

Marcel Verhoef (ESA), Helder Silva (EDISOFT),
Sebastian Huber (Embedded Brains)

27/03/2019

Agenda for the workshop

- General introduction to the ESA GSTP activity
- Background to the RTEMS qualification user consultation
- Questionnaire and definition of RTEMS space subset
- Follow-up and Q&A

Background to the qualification activity (1)

- New ESA GSTP funded activity formally started in February 2019
- Consortium is composed of
  - EDISOFT (Portugal – consortium lead) → RTEMS qualification experience, strong ties with industry
  - Embedded Brains (Germany) → RTEMS SMP development expertise, strong ties with community
  - LERO (University of Limerick, Trinity College Dublin, Ireland) → formal methods expertise
  - Jena Optronik (Germany) → end user in space domain, application qualification expertise
- Investment: 700 kEuro, will run for 24 months (Feb 2019 – Feb 2021)
- Activity will be executed in close collaboration with the RTEMS community and end-users in the space domain

Background to the qualification activity (2)

- To complement many completed ESA sponsored R&D for RTEMS
  - EDISOFT RTEMS (http://rtemscentre.edisoft.pt)
    - Based on RTEMS 4.8.0, qualified to DAL-B, applied in many space missions
    - Open source, but qualification data pack is licensed
    - Available for ERC32, LEON2, LEON3 (single core)
    - This product is maintained by EDISOFT (latest is R14) and will remain available, the new activity will not replace (or support evolution of) this existing product
    - Contact EDISOFT on license cost and support contracts
  - RTEMS-SMP, as is available in the RTEMS mainline, as part of the 5.x release
    - Co-developed with the RTEMS community, with significant ESA investment, now *production ready* for LEON3 dual-core and LEON4 quad-core (final report available at http://microelectronics.esa.int/NGMP)
    - Several device drivers made SMP compliant by Cobham Gaisler (own investment)

Objectives of the new activity (1)

- Production of a (pre-) *qualification toolkit* that allows end-users to qualify their (space) applications on bespoke (space-qualified) hardware
  - Target application area is payload (instrument) data processing, software criticality level C (caveat: this is the perceived as the typical use case for the SMP capability)
  - Primary focus is on qualifying the SMP elements of the RTEMS super core, and the MIL-STD-1553 and SpaceWire interfaces – exact scope to be finalized (see "space subset")
  - Qualification of RTEMS 5.x on single core is *not* a priority (we have RTEMS EDISOFT)
  - Base-line target platforms are the Cobham Gaisler GR712RC (LEON3 dual core) and GR740 (LEON4 quad core) System-On-Chips
  - The pre-qualification toolkit uses the GCC-based cross-compiler provided by the RTEMS Source Builder as baseline (RSB - currently at GCC v7.3, but this may evolve during the project)
  - Alignment with the (qualified) Mathematical Library for Flight Software (MLFS) see https://essr.esa.int/project/mlfs-mathematical-library-for-flight-software

Objectives of the new activity (2)

- Production of a (pre-) *qualification toolkit* that allows end-users to qualify their (space) applications on bespoke (space-qualified) hardware (… cont)
  - Currently out-of-scope (not fitting with ESA project time and budget constraints)
    - LLVM / clang compiler support
    - Other multi-core SoCs or CPU architectures (i.e. ARM based, RISC-V)
    - Independent Software Verification and Validation (ISVV)

- Caveat on qualification / pre-qualification:
  - The *scope of qualification* is always the full application software stack running on the *bespoke target hardware* operating in its *intended environment*
  - RTEMS is just *a part of* this application software stack (statically linked library)
  - It is not possible to fully qualify RTEMS as a stand-alone component
  - Verification and validation done on specific board and software configurations only (test sw)
  - This project provides the inputs needed to qualify at (sub-)system level
  - Repeatable approach on bespoke target hardware / customizable / extensible

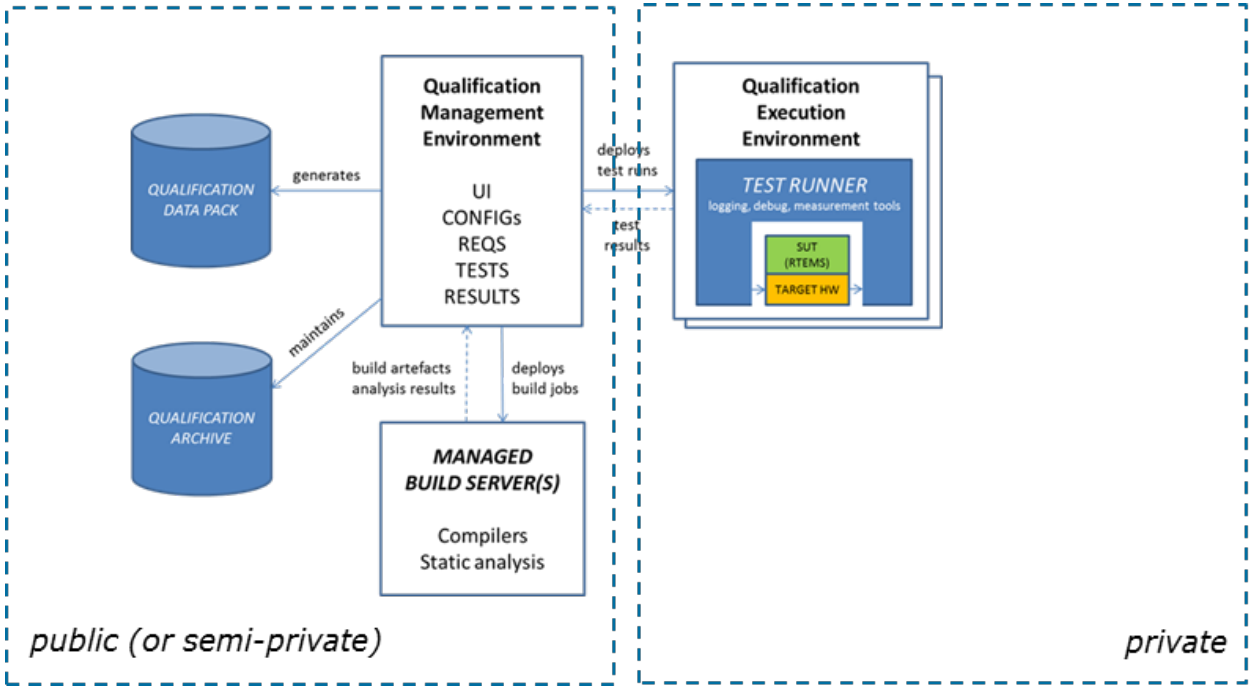
Objectives of the new activity (3)

- The foreseen *Qualification toolkit* contents
  - Curated version of the source code and related documentation, including all resources needed (i.e. compiler, build scripts) to build RTEMS itself
  - *All verification and validation evidence, obtained from analysis, testing and proof, for the identified target configurations, in the form of documents required by ECSS-E-ST-40C and ECSS-Q-ST-80C (these standards are freely available at http://ecss.nl/) this includes all artifacts flowing down from all product assurance activities performed*
  - Curated test suite and all supporting resources required to automatically execute the test suite and reproduce the test evidence for each identified target configuration
  - Set of instructions of how to use the qualification toolkit (user manual)

- The challenge is to keep this activity *as close as possible* to the RTEMS main-line evolution
- The qualification toolkit will become *fully open source*
- Review of DO-178C, IEC 61508 and ISO 26262 to minimize work for potential qualification towards these related standards (out of scope for the ESA contract, but might be community contributed)

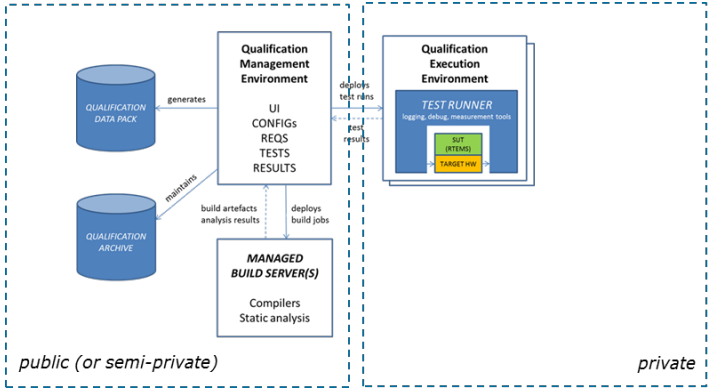
Objectives of the new activity (4)

- Definition and implementation of a qualification environment



Objectives of the new activity (5)

- Definition and implementation of a qualification environment
  - qualification management environment
    - requirements and documents
    - test case and configuration definitions
    - automatic compilation and code analysis
    - test, analysis and verification result reporting
    - product assurance activities and reporting
  - qualification test execution environment
    - on target deployment



- Aim is to automate the (management of the) entire qualification process as far as possible
- Qualification environment will also be open source tooling (with the possibility to attach proprietary tools)
- Alignment / integrated with RTEMS community processes (to be discussed / developed with community)
- Can also be instantiated in-house (to overcome company security restrictions)
- Extensible (to integrate other target platforms, compliance to other standards)
- Flexible (not smothering the spirit of open source development and innovation)

Time-line of the project (up-to-date)

- Q1 2019 : definition of the qualification environment → *your inputs are needed*
- Q1 2019 : definition of the RTEMS SMP “space subset” → *questionnaire*
- Q2 2019 : initial development of the qualification environment
- Q3 2019 – Q4 2020 : iterative development of the qualification environment
- Q3 2019 – Q4 2020 : iterative development of the qualification toolkit
- Q1 2021 : consolidation

- The intent is to provide full visibility to the community during this process
- Project artifacts will be shared and any feedback received will be taken into account
- Agile development process will be followed (monthly iterations - sprints), within a normal ECSS workflow
- Active project communication through RTEMS mailing lists and web-site(s)
- Iterative development to support early adopters (you don’t need to wait to Q4-2020)

Summary

- RTEMS SMP qualification for LEON3/4 multicore to criticality level C (no ISVV)
- Qualification towards ECSS standards, we “reverse engineer” the compliance based on what is currently available, we complement, modify and improve where needed
- We welcome community contributions (i.e. other target platforms, other standards)
- We follow (and contribute to) the RTEMS main line development to minimize deviations
- Iterative and agile approach to allow early adoption and ensure community involvement
- Goal is to provide community with the means to maintain qualification level artifacts
- Two-sides of the same coin:
  - (-) Qualification is (considered) boring, at best a “necessary evil” that should not limit innovation
  - (+) Qualification is an enabler for industrial uptake and provides proof of quality

The bottom line

- ***But, what's in it for me?***
  - Technically challenging (and very interesting) work ahead, i.e. : test automation and reporting, static source code analysis and formal proof of key OS primitives
  - A pre-qualified RTOS in ECSS Category C
  - A qualification toolchain to use in the qualification of other applications

- ***And for the RTEMS community at large?***
  - The potential to increase the adoption in industry (with all qualification artifacts in open source)
  - To be able to maintain the qualified state of RTEMS for many years to come at low cost

Definition of an RTEMS space subset (1)

- RTEMS has a very feature rich eco-system
- Qualifying the entire scope is not feasible (time / budget constraints)
- Qualifying the entire scope is not needed (not all features are used)
- As with previous qualification activities, we define a *space subset*:
  - based on needs of the (ESA) space software community
  - based on past applications and usage experiences
  - based on future usage expectations (in particular: multi-core)

- Step-wise approach
  1. questionnaire sent to the (space) community at large (done)
  2. consolidate results into a space subset definition document
  3. iterate space subset definition document with community for review

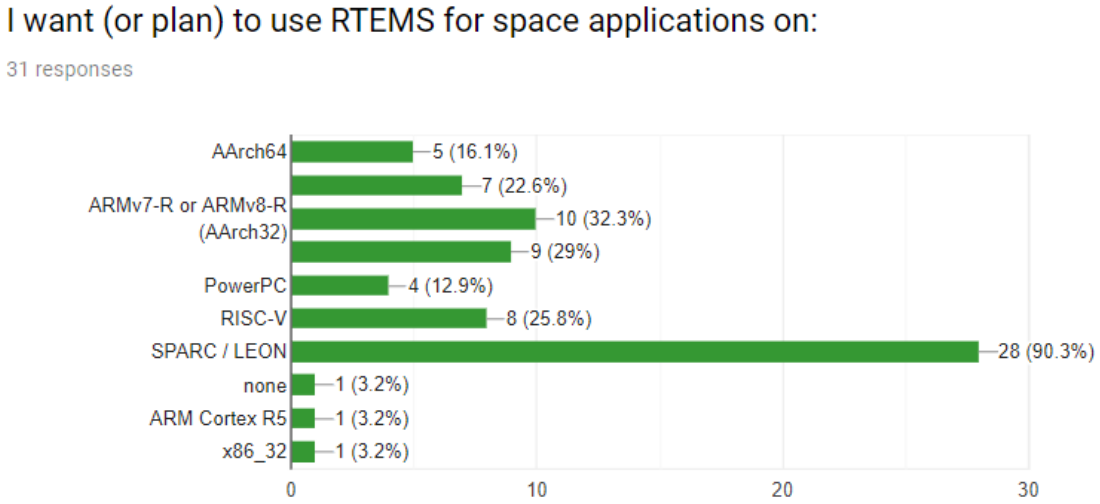
Definition of an RTEMS space subset (2)

- Questionnaire was sent out to the community on 7 March 2017
- Submission deadline was set to 25 March 2017
- 31 responses were received (mostly from ESA member states, 2 from USA)

- Main questions w.r.t. space subset scope:
  - what elements of the RTEMS APIs should we focus on
    - as was used in the past (to allow migration of existing SW)
    - what is needed in the future (i.e. to support higher level APIs)
  - what platforms should we target or take into account
  - what device driver support is considered as important

- Many thanks to everyone that provided their inputs!

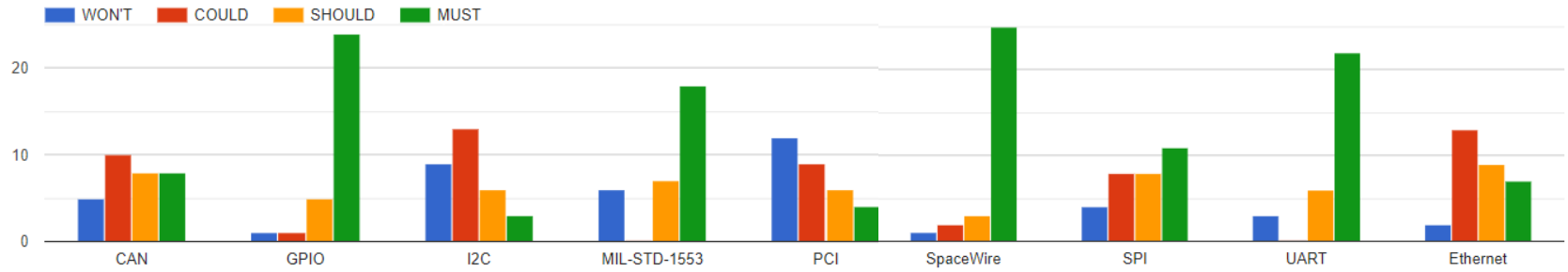
Questionnaire – early results (1) - platforms



- Focus on LEON / SPARC confirmed, both single and multi-core
- ARM and RISC-V interest noteworthy / in-line with expectations

Questionnaire - early results (2) – device support

I need drivers for the following devices in my space application:



- Focus on MIL-STD-1553 and SpaceWire confirmed
- UART and GPIO also needed
- SPI and CAN likely contenders

Questionnaire – early results (3)

- Dynamic memory allocation
  - ECSS : only allowed at initialization time, not allowed during run-time
  - need a scalable SMP memory allocator not confirmed
- Thread support
  - ECSS : thread creation / deletion only at initialization time
  - ability to restart threads confirmed
  - need for thread to processor affinity confirmed
- Locking protocols
  - potential need identified / confirmed for SMP application management
- Scheduling
  - deadlock detection and schedulability analysis support confirmed
  - EDF support possibly, no interest in CBS, clustered scheduling not confirmed

Questionnaire – early results (4)

- Gaisler driver manager support : yes

- Language support
  - Ada : yes, but only required by few
  - C++: yes, requested by many
  - Java : no
  - Go : no
  - (micro) Python : yes, contender like C++/Ada
  - Rust : no

Questionnaire – early results (5)

- High-level APIs for application level parallelism
    - OpenMP support preferred over MTAPI
- File-system support: yes there is interest / need identified
- Thread local storage: need identified
- C-locale support : no
- Barrier manager : inconclusive
- Clock manager : yes
- Event manager : yes
- Interrupt manager : yes
- IO manager : inconclusive
- Message manager : yes

Questionnaire – early results (6)

- Partition manager : inconclusive
- Rate monotonic manager : yes
- Region manager : no
- Semaphore manager : yes
- Signal manager : inconclusive
- User extension manager : inconclusive
- Task manager : yes
- Timer manager : yes
- Fatal Error manager : inconclusive

Questionnaire – early results (7) - POSIX

- POSIX barriers : inconclusive
- POSIX clocks : inconclusive
- POSIX condition variables : inconclusive
- POSIX keys : no
- POSIX message queues: inconclusive
- POSIX mutexes: inconclusive
- POSIX read-write locks: inconclusive
- POSIX (named) semaphores: inconclusive
- POSIX spin-locks: inconclusive
- POSIX thread management: inconclusive

use of POSIX seems to be of interest only to a small set of users

needs more investigation

Space profile – next steps

- Further analysis of questionnaire results – proposal qualification scope
- Potential follow-up questions to clarify issues with individual respondents
- Write the space profile document (April 2019)
- Release *space profile document* for comments to community (May 2019)
- Consolidate report – baseline for ESA project (June 2019)
- Follow-up actions for those elements that are deemed important but are outside the current project scope

- On communication:
  - further announcements via SAVOIR FAIRE, RTEMS mailing lists
  - if there is interest: more meetings like the one today (interactive)

Questions and answers (1)

- *Who approves the qualification toolkit?*
  - ESA will approve the documents delivered for ECSS compliance (most likely this will follow the normal RTEMS release cycle - TBC)

- *I need category-B qualification for my project!*
  - This activity is prepared for category-B (execute ISVV as shadow activity)
  - Find funding support for performing ISVV in parallel
  - ISVV as community supported activity – feasible?

Questions and answers (2)

- *Feature … is not included in the foreseen space profile, what should I do?*
  - The qualification approach is extensible → you can add your own feature
  - Find funding support to extend current project / community contributed

- *Does the ESA qualification generally include a hazard analysis?*
  - No: hazard analysis is performed at (sub-)system level and is specific to
    - the bespoke hardware on which the software executes
    - the application software that uses RTEMS features
  - Analogous to: schedulability analysis and budget reports
  - The ESA project will provide a set of documents and guidelines on how to support these (ECSS) processes at (sub-) system qualification level

Questions and answers (3)

- *What is the approach to support other CPU architecture / SoCs?*
  - the qualification environment will be extensible
    - adding test runners for these additional CPU architectures / SoCs
    - the ability to specialize (add) requirements / test cases / expected outcomes
    - verification and validation artifacts may also require adaptations
  - this customization can be done by end-users / community contributed
  - ESA project will provide guidelines on how to do this tailoring (SUM)
  - formal approval / acceptance process of the “qualified extension” is still TBD

- *How can the community contribute / provide feedback on project outputs?*
  - the ESA project will ask for feedback via the (RTEMS) mailing lists and SAVOIR
  - we intend to hold regular (i.e. quarterly) user consultation meetings (see slide 27)

Questions and answers (4)

- *What role will formal methods play in the project?*
  - to compensate for those aspects where testing is known to be incomplete, very hard or very hard to reproduce → demonstrate correctness of some of the key algorithms (and their implementations) using formal verification and proof
  - to improve our ability to maintain test suites and demonstrate their completeness / correctness
  - exploit the advances in modern deep static analysis techniques to inspect existing code and perform impact analysis of any modifications made (RTEMS already uses coverity scan)

- *What is the impact on the use of the Mathematical Library for Flight Software (MLFS)? Can I use another mathematical library?*
  - MLFS is a qualified subset of the well-known libm/newlib, with full ECSS compliant documentation available to ESA member states; it will become a baseline for all next generation ESA missions
  - RTEMS does not depend on any mathematical library, the impact on supporting MLFS is minor (related to errno handling)

How to contact the project / follow our progress

- Our main communication channel will be the RTEMS mailing list(s)
  - https://lists.rtems.org/mailman/listinfo/devel (high bandwidth)
  - https://lists.rtems.org/mailman/listinfo/qualification (low bandwidth)

- ESA members of the SAVOIR FAIRE working group will be contacted via e-mail
  for more details see http://savoir.estec.esa.int/

- We intend to organize more user consultation meetings with remote access via Skype

- For questions specifically related to the ESA GSTP project, please contact:
  - Marcel Verhoef (ESA ESTEC, technical officer) : Marcel.Verhoef@esa.int
  - Helder Silva (EDISOFT, consortium lead) : Helder.Silva@edisoft.pt