RTEMS-SMP QUALIFICATION

Marcel Verhoef

02/12/2018

Background (1)

- New GSTP activity started in November 2018

- 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 Optronics (Germany) → end user in space domain, application qualification expertise

- Investment: 700 kEuro, will run for 24 months (Dec 2018 – Dec 2020)

- Activity will be executed in close collaboration with the RTEMS community and end-users in the space domain

Background (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 this 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)

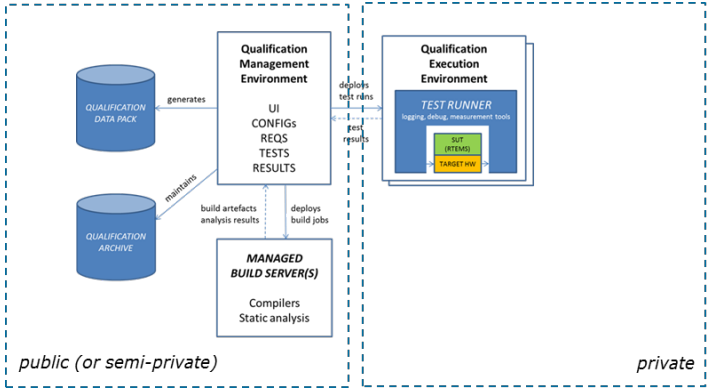
- Production of a (pre-) *qualification toolkit* that allows end-users to qualify their (space) applications on bespoke (space-qualified) hardware
  - Target application area is payload (instrument) data processing, software criticality level C
  - Primary focus is on qualifying the SMP elements of the 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
  - Currently out-of-scope (not fitting with project time and budget constraints)
    - LLVM / clang compiler support
    - Other multi-core SoC architectures (i.e. ARM based)

Objectives of the new activity (2)

- 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/)*
  - 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*
- Compliance to other standards (i.e. DO-178C, IEC 61508, ISO 26262) will be considered, but is out of scope for the ESA contract (but might be community contributed)

Objectives of the new activity (3)

- Definition and implementation of a qualification environment
  - qualification management environment
    - requirements and documents
    - test case and configuration definitions
    - automatic compilation and code analysis
    - test and analysis 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

- Q1 2019 : definition of the qualification environment → *your inputs are needed*
- Q1 2019 : definition of the RTEMS SMP “space subset” → *your inputs are needed*
- Q2 2019 : initial development of the qualification environment
- Q3 2019 – Q3 2020 : iterative development of the qualification environment
- Q3 2019 – Q3 2020 : iterative development of the qualification toolkit
- Q4 2020 : 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 (bi-weekly iterations - sprints)
- Active project communication through RTEMS mailing lists and web-site(s)

- Workshop / Telecon will be organised in January 2019 to discuss the “space subset”

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
- 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

- ***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

For questions or remarks, please contact:

Marcel.Verhoef@esa.int (technical officer of the activity)

We look forward to hearing from you!