EUROPEAN WORKSHOP ON ON-BOARD DATA PROCESING (OBDP2021), 14-17 JUNE 2021

SPACE QUALIFICATION FOR OPEN-SOURCE REAL-TIME MULTICORE OS RTEMS

Matthias Göbel[(1)], Sebastian Huber[(1)], Thomas Dörfler[(1)]
[(1)]embedded brains GmbH, D-82178 Puchheim, Germany

ABSTRACT

RTEMS has become a popular Real-Time OS in the space domain during the recent years. This is very much supported by its Open-Source nature and the availability of a qualified (single-core) version.

However, over time this technology is more and more outdated, as many recent improvements cannot be included in this branched-off-version with reasonable effort. Further, the introduction of RTEMS multicore-version (using Symmetric Multiprocessing) has established a completely new software architecture which code basis cannot be merged with code from old versions (although compatible interfaces are provided).

In order to enable a low-threshold entrance to the contemporary multicore RTEMS, a new ECSS space qualification initiative was set up by ESA. In difference to past approaches, the qualification itself follows an open-source approach, and the basic documentation and test software ("RTEMS-SMP qualification toolkit") is made available to the public without royalties being imposed. It is intended to spark a self-sustaining initiative for a continuous further development, carried out by community members.

This paper discusses the background of RTEMS and the details of the current qualification. Further, the implications of using open-source software in professional environments are highlighted.

1. BACKGROUND

RTEMS (which stands for Real Time Embedded Operating System) was originally developed for the US Army in the 1980s (named „Real-Time Executive for Missile Systems"). Since the mid 1990s RTEMS is continued as Open Source Software under „GPLv2 w/linking exception" license, recently moving to "two paragraph BSD" based licensing [1].

RTEMS is a „hard" real-time OS with high flexibility, permitting minimal resource demands and maximum performance. It is available for a broad range of processors and provides all common interfaces for embedded requirements. Originally designed for single-core processors a SMP (Symmetric Multiprocessing) is available since 2015. An ECSS Space pre-qualification (Cat. C and D) shall be completed shortly.

RTEMS is used in embedded systems for a broad range of applications, such as

- Space industry (satellites),
- Industrial equipment (e.g. hand tools, autonomous vehicles, quality control),
- Professional audio, and
- Machine control (e.g. for radio telescopes).

In the Space Domain RTEMS is used for many European and US satellite launches, such as

- NASA Perseverance Mars Rover (SPARRC v7 based Command and Data Management Unit and Altitude Control Computer),
- NASA Parker Solar Probe (SPARC Flight Computer),
- DLR Eu:CROPIS (SPARC based life-support, growing tomatoes in space),
- UAE KhalifaSat (SPARC LEON3 based remote sensing satellite capable of imaging the earth at 0.7 meters),
- NASA ICESat-2 (Advanced Topographic Laser Altimeter System runs RTEMS on a mix of SPARC and PowerPC CPUs), and
- ESA BepiColombo (RTEMS on Mercury Radiometer and Thermal Infrared Imaging Spectrometer).

Main arguments for choosing RTEMS are its high flexibility for many processor types and interfaces, and its low resource demand. Simple versions provide a real-time OS using less than 16kB RAM. Meanwhile compatible versions run on 32 and 64bit processors, providing POSIX and API interface, OpenMP support, C11/C++11 threading and synchronization support, Flattened Device Tree (FDT) support, and Support for QorIQ DPAA including 10 Gbit/s Ethernet.

A major revision has introduced Symmetric Multiprocessing (SMP) capability for multicore processors from RTEMS version 5 on [2]. This is technically a new development, however with features and interfaces compatible to the single-core RTEMS.

It provides

- Scalable timer support
  - Priority queued timers (e.g. red-black trees)
  - Timer expiration distributed across processors
- Fine grained locking (Big Kernel Lock removed)
- Locking Protocols for Mutual Exclusion (Transitive priority inheritance tracked across multiple resources)
- Priority ceiling
  - O(m) Independence-Preserving Protocol (OMIP) extends priority inheritance to clustered scheduling
  - Multiprocessor Resource-Sharing Protocol (MrsP) extends priority ceiling to clustered scheduling

Alike the single core RTEMS it is particularly strong for realising high-performance with relatively minimal hardware resources. For example, RTEMS SMP incl Open MP just requires 50kB of memory. However, this comes along with a lack of memory protection separating different applications.

Meanwhile a large variety of BSP's is available for SMP, such as:

- SPARC (1 to 4 cores): GR712C and GR740
- PowerPC (1 to 24 cores): QorIQ (e.g. P1020, P2020, T2080, T4240)
- ARMv7-A (1 to 4 cores): Altera Cyclone V, Xilinx Zynq, Raspberry Pi2, and
- RISC-V (1 to 2 cores).

2. ECSS QUALIFICATION OF RTEMS-SMP

Older single-core version of RTEMS have been qualified more than 10 years ago (v4.6 and v4.8.0, respectively). Those versions are not only limited to single-core and only partially available for interested parties, but the branching-off of a contemporary versions in the past has rendered the consideration of updates and functional extensions almost impossible since then. Consequently, those version are very much outdated.

In order to avoid a similar dead-end the SMP qualification initiative was set up with a different approach: Sponsored by ESA, it aims to provide a free „starter-kit" for RTEMS qualification, hence enabling a low-threshold qualification process.
This starter-kit includes

- A Pre-qualification for ECSS Cat. C and D for selected configurations,
- Verification evidence for RTEMS and a selection of libraries,
- Validation evidence to demonstrate that requirements are met, and
- Guidance to end-users on how to replicate and use (or extend) these results for a full qualification.

An international consortium consisting of

- edisoft (Portugal),
- embedded brains (Germany),
- Lero (The Irish Software Research Centre / Trinity College Dublin, Ireland), and
- Jena Optronik (Germany)

is performing this project between Dec 2018 and Dec 2021. This includes not only the qualification documents, but also the software tools (test suite and toolchain). Further it includes the application of formal testing and a practical use case. Therefore, Promela/ SPIN is used to generate tests for critical parts of RTEMS e.g. thread queues. A use case provides a reality-check of the qualification toolbox.

The Tookit Concept

As RTEMS SMP has no memory protection separating applications, OS and application software cannot be qualified separately. This is why the RTEMS toolkit concept is coming into play:

The Toolkit includes a pre-qualified package with documents, test suite, toolchain and a use-case for the LEON3 & LEON4 (Gaisler GR712RC and GR740, respectively) processors. The API subset corresponds to the function subset of the RTEMS repository [3] and the Space Profile [4] which was defined according to a requirements survey among users in the space domain.

The application software resides on top of the RTEMS OS in the executable. This construct must be qualified as a whole, using the Toolkit as a basis. This can be done by the user on its own or with the help of expert support, particularly in order to allow a smoother start of the framing software. The effort of applying the Toolkit is comparable to a separate qualification of OS and application software, considering that testing the application normally requires an OS or an emulated OS to run on.

The Toolkit can be extended for other controllers and further interfaces and subsets on demand.

Qualification Data Package (QDP)

The Qualification Data Package (see [5]) is available for free and includes

- Project results,
- All source code,
- Documents,
- Binaries, and
- Test-suites

ready to build applications, re-run tests and work with qualification documentation.

The Toolkit includes verification activities such as

- Static code checker results form Coverity, CLANG, and CppCheck,
- Product and process metrics,
- Assessment of testing and validation activities, and
- Problem and none-conformance reports.

In principle it is also usable for the application software testing (but likely will require extensions specific to the application software).

3. OPEN SOURCE IMPLICATIONS

The Toolkit is publicly available and can be used free, alike the RTEMS software itself. This has a lot of advantages, such as

- No loyalties
- Easy start without bureaucracy
- 100% transparent source code
- Supportive community (hopefully), no monopoly for product support
- No changes in business model of supplier, and
- No update obligation induced by the supplier.

However, the use of open-source software and tools comes along with some well-known implications that should be considered in advance for professional use:

- The roadmap depends on independent software developers, hence it may become difficult to address strategic investments.
- No active marketing is provided, hence product information does not compare to commercial software.
- The license conditions may imply restrictions for own source code, for example requiring to publish own code.

Apart from those attributes of Open-Source Software some other, much more important challenges come along with the options and the responsibilities of manipulating the software. We label this the "DIY-Syndrome":

- The effort required for creating new functions or interfaces is widely underestimated.
- Creation of a „private" version brings the risk, that sooner or later this private version will be completely outdated, as the public version will develop separately.
- The need to keep updated with many (or all main) developments in the community version is very much underestimated. This is particularly the case for large software packages.

Using the Qualification Data Packages has similar implications, however the complex nature of qualification will require a substantial effort to functionally implement a tailored and updated QDP. In order to minimize total effort it might be useful to make use of external expertise (e.g. [6]) in order to avoid redundant effort with no productive value.

4. OUTLOOK

In order to make use of the advantages of Open-Source-Software while avoiding its negative implications the RTEMS Foundation shall take some responsibility in the coordination of activities and to protect investments in an appropriate way. This shall be performed in a transparent and independent way.

The provision of the RTEMS-SMP qualification toolkit on the basis of the LEON3 & LEON4 (Gaisler GR712RC and GR740, respectively) and subset and interfaces according to the Space Profile [4] marks a starting point for the most popular use-cases.
In the future we plan to develop QDPs for other controllers, such as the DAHLIA SoC, various ARM-cores and the RISC-V. BSPs are already available for the latter both families.

Further interfaces and drivers shall be added as well as the subset of qualified RTEMS API functions shall be expanded over time.

An Independent Software Verification and Validation (ISVV) is on its way to obtain ECSS cat. B qualification (sponsored by ESA).

The success of all those initiatives depends very much on an effective cooperation in order to avoid redundant activities. As a result, the effort required for a qualified high-performance multicore OS may drop dramatically.

ACKNOWLEDGEMENTS

This work was sponsored by the European Space Agency (ESA): "Qualification of RTEMS Symmetric Multiprocessing (SMP)".

REFERENCESS

[1] https://ftp.rtems.org/pub/rtems/people/sebh/rtems-smp-dasia-2017.pdf
[2] https://www.rtems.org/license/LICENSE
[3] https://git.rtems.org/
[4] https://rtems-qual.io.esa.int/qdp/tn-space-profile.pdf
[5] https://rtems-qual.io.esa.int/
[6] http://www.embedded-brains.de