IMA Separation Kernel Qualification Campaign

teletel fentISS AIRBUS DEFENCE & SPACE ThalesAlenia Space

Final Presentation Days
ESA/ESTEC, 3-4 December 2019

Presentation Contents

- Project Information
- XtratuM Hypervisor Overview
- Qualification Platform Overview
- Test Suite Overview
- Main activities within the study
- Validation & Qualification results
- Main conclusions and next steps

Project Information

- Project: IMA Separation Kernel Qualification Campaign (ESA Contract No. 4000118802/16/NL/AF/as)
- Actual Duration: 36 months, Budget: 500KEuro
- ESA Technical Officer: Ms Maria Hernek

- The objective was to perform the IMA XtratuM Separation Kernel Upgrade and its Qualification through the IMA Kernel Qualification Platform and the associated Qualification Test Suite that was designed and verified within the study.

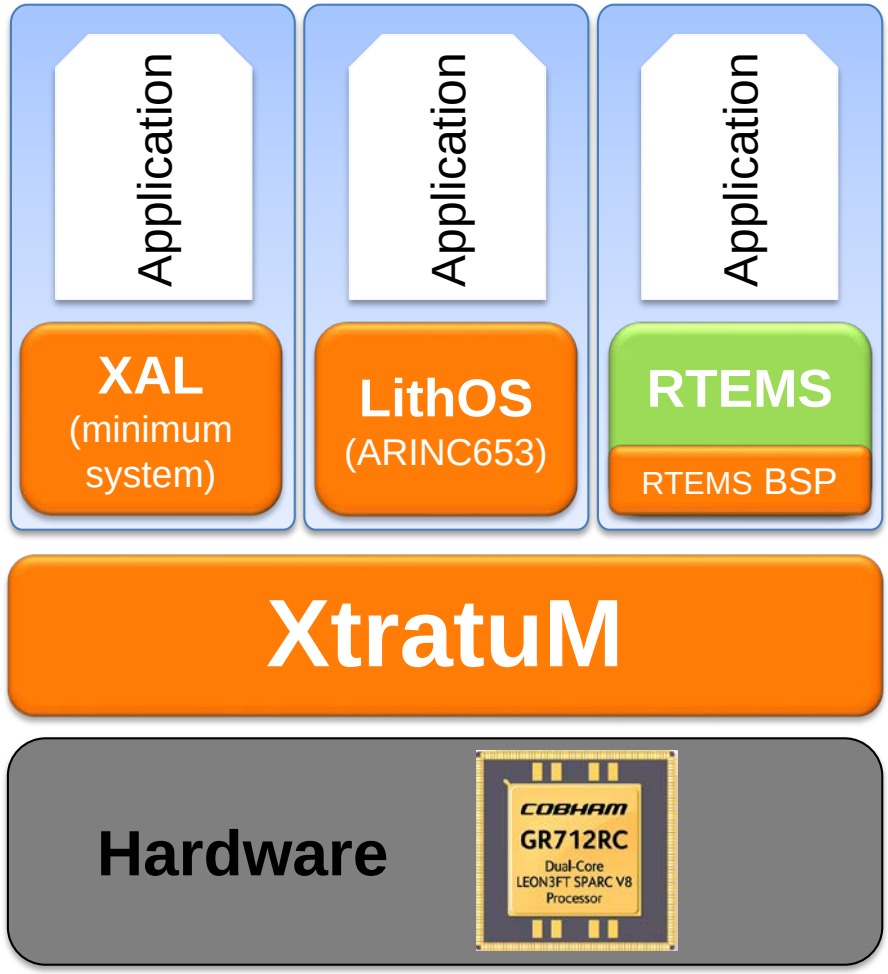
- Prime Contractor: TELETEL (Greece)
- Sub-Contractors:
  - FENTISS (Spain)
  - AIRBUS DEFENCE & SPACE (France)
  - THALES ALENIA SPACE (France)
- The activity was supervised by CNES

Main Work Areas – Background of companies

- XtratuM Separation Kernel Design, Development and testing
  - Responsible: FENTISS (Spain)
  - Background: Expertise in TSP based software architectures, safety-critical embedded systems, virtualization and hypervisor technologies
- Qualification platform and Test Suite
  - Responsible: TELETEL (Greece)
  - Background: Significant expertise in TSP architectures, on-board data handling technologies, validation of on-board data networks (SpaceWire, 1553, CAN, SpaceFibre, TTEthernet etc.), ISVV.
- Review and support activities
  - Responsible: AIRBUS DEFENCE & SPACE (France), THALES ALENIA SPACE (France), CNES (France)
  - Background: Wide experience in IMA technology, On-board Software Development, validation and qualification, having successfully executed various related ESA and CNES studies

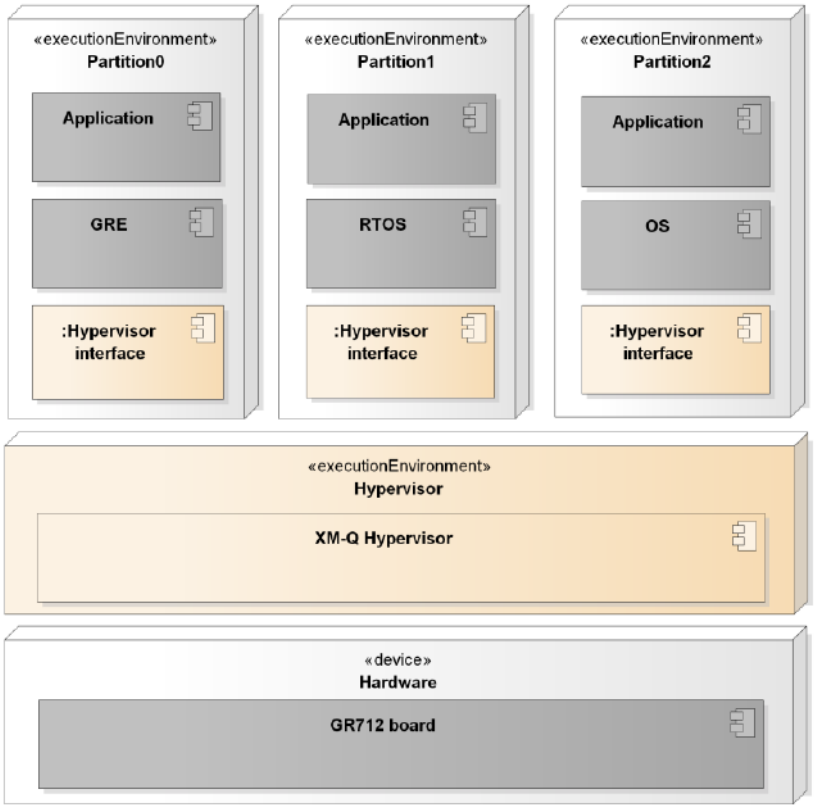
The XtratuM Hypervisor (1/3)

- Bare metal efficient hypervisor for safety critical **time and space partitioned systems**
- It supports SPARC/LEON architectures (**LEON2, 3, 4**) and ARM architectures (**Cortex-R4/R5, A9**)
- It provides **guest run-time systems** developed by **FENTISS** and other third parties
- Space qualified (aiming for **ECSS level B**) for LEON3 (monocore)



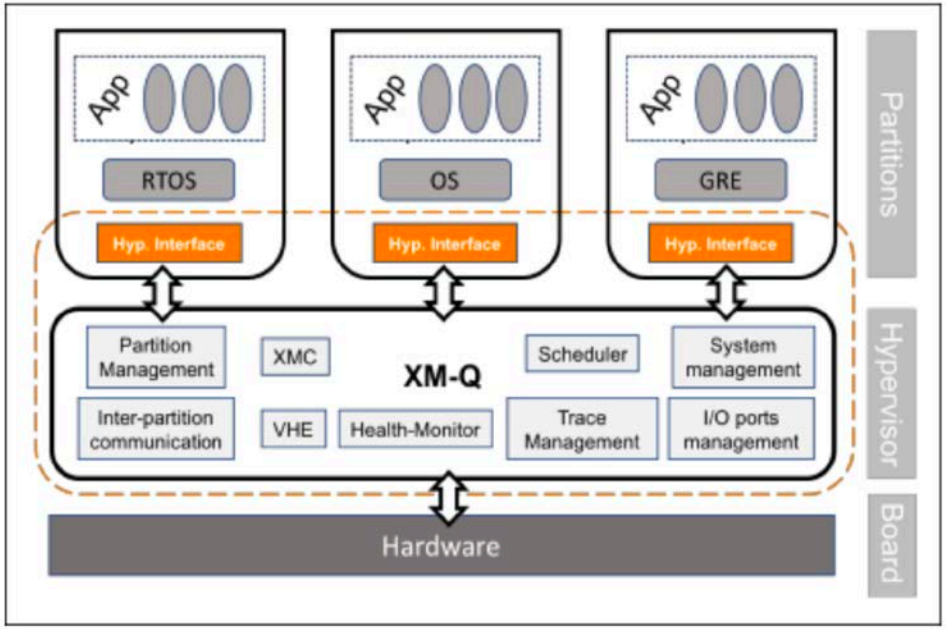
The XtratuM Hypervisor (2/3)

- XtratuM Q (**XM-Q** for short) is the **qualified version** of the XtratuM hypervisor for SPARCv8 (LEON3 monocore).
- **XM-Q qualification campaign** used as target the GR712RC processor-based board.
- **XM-Q** qualification increased the **quality** of the software and improve the **reliability** and **confidence** of the product.
- The **XM-Q** design is based on the following main pillars:
  - Fault isolation and management
  - Spatial isolation
  - Temporal isolation
  - Confidentiality
  - Configurability
  - Deterministic execution



The XtratuM Hypervisor (3/3)

- **XM-Q** capabilities can be summarized in the following services:
  - System management: state and operation of the hypervisor.
  - Partition management: state and operation of the partitions.
  - Partition scheduling: schedules partitions in a fixed, cyclic basis.
  - Health-monitor: confine the faulting subsystem and monitor the operation.
  - Memory management
  - Interrupt management
  - Inter-partition communication
  - Trace management
  - Virtual hardware environment
  - I/O management
  - GR712RC devices support



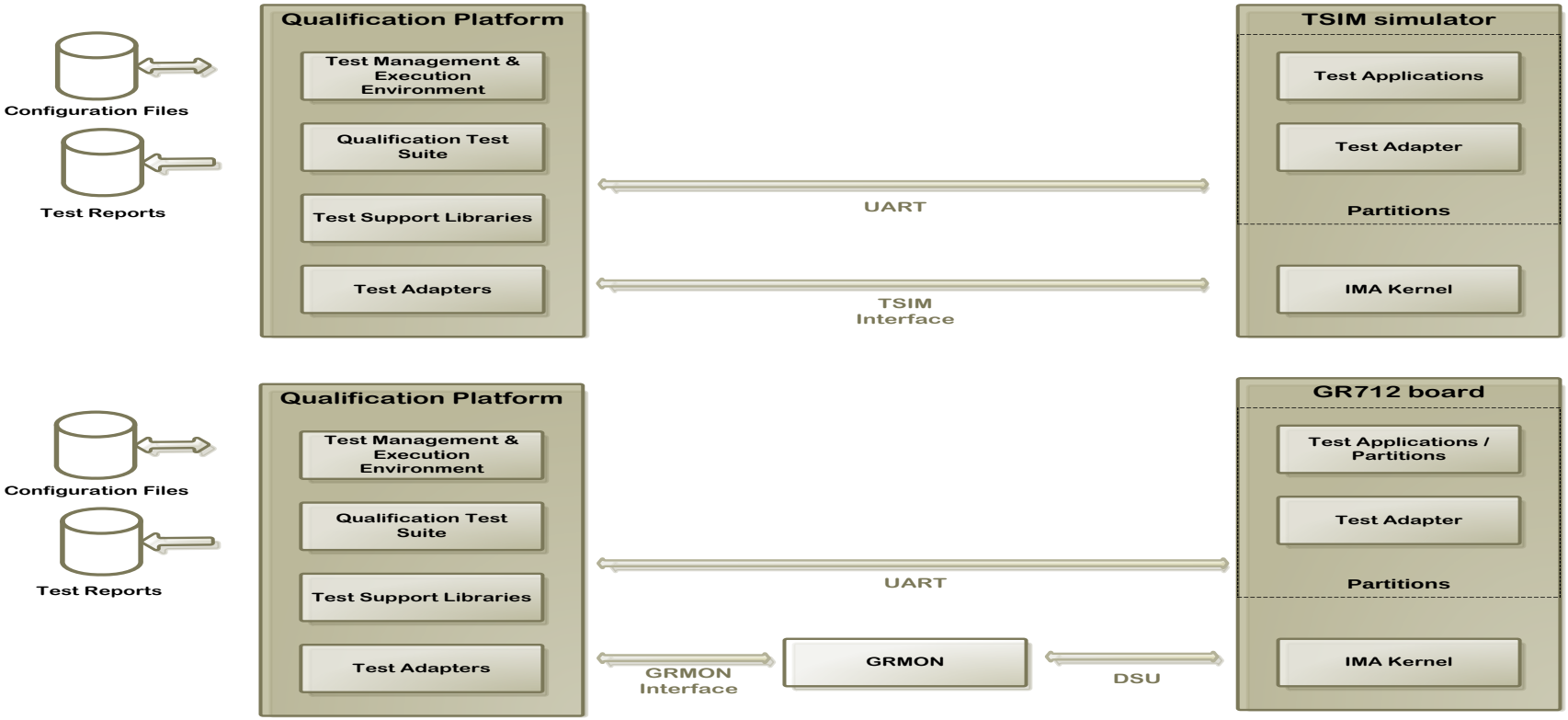
Qualification Platform & Test Suite – Introduction

- The Qualification Platform is used to execute the Qualification Test Suite for the validation of XtratuM with respect to the baseline requirements.

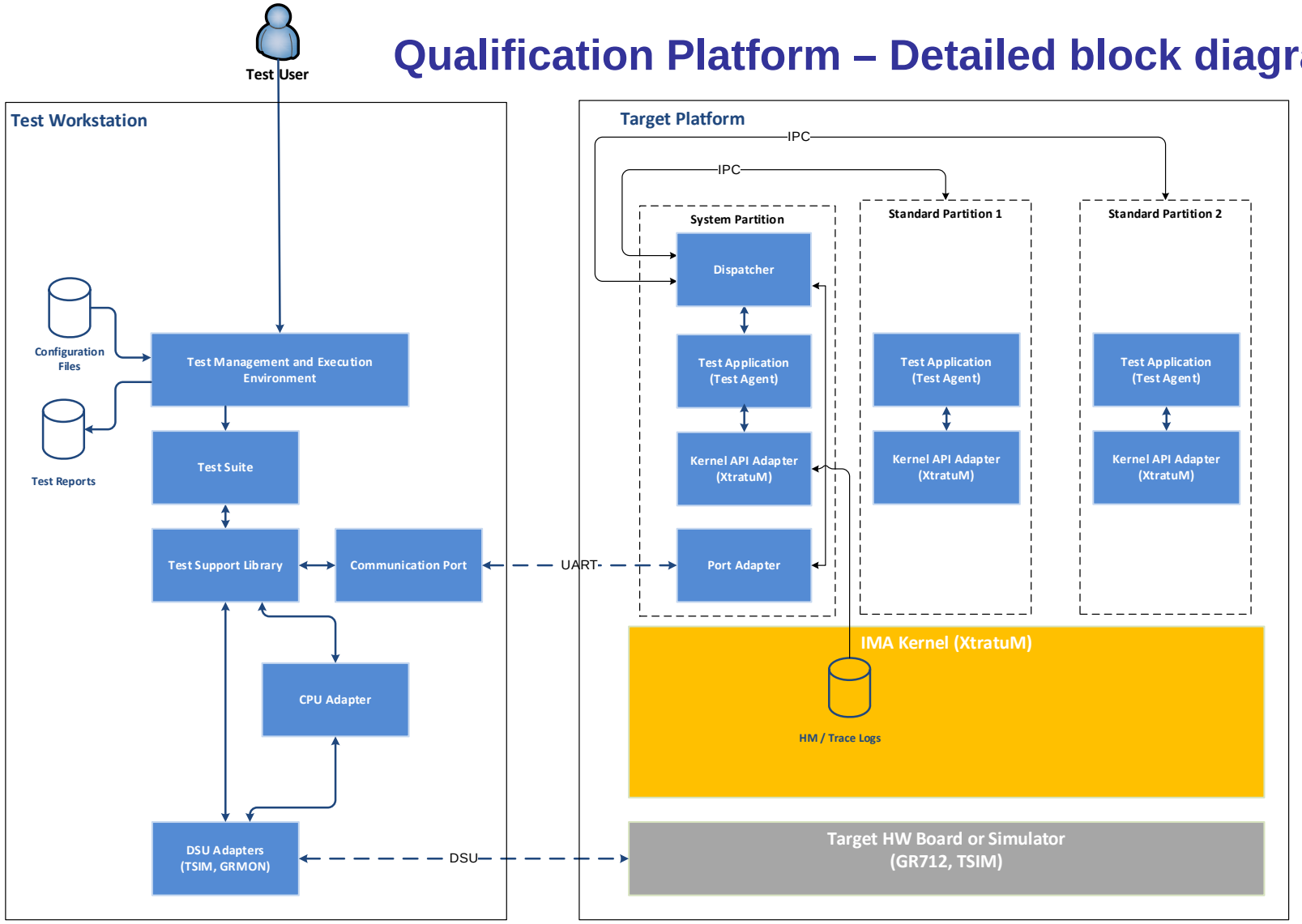
- Why TELETEL: Testing & Validation Experts
  - Supplier of EGSE for flight equipment
    - Recent References: Euclid ADPME EGSE, Microcarb Instrument EGSE, IASI-NG MDE EGSE
  - Specialization in on-board data handling technologies, with special emphasis in the validation of satellite/spacecraft on-board data networks
    - iSAFT product Line: Network Interface Cards, SW, Simulator/Recorders for SpaceWire, SpaceFibre, MIL-STD-1553, CAN, Time-Triggered Ethernet etc.
  - OBSW development
    - Recent References: JUICE on-board (and ground) CFDP development, EUCLID ASW development

Qualification Platform – High level architecture

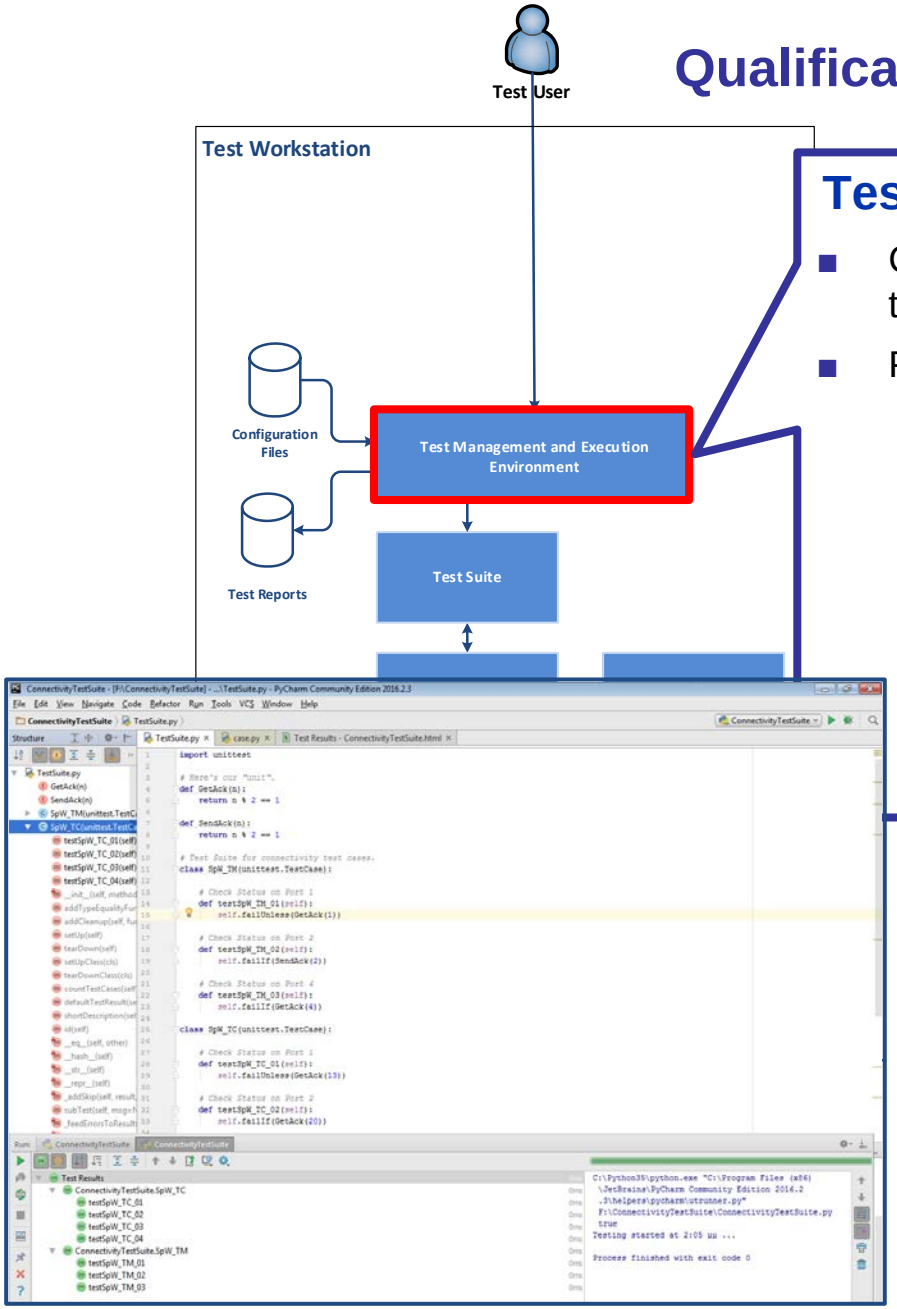
- SW components of the Qualification Platform are executed at both Test Workstation and Target Platform.
- Qualification Platform separates test implementation from the underlying hardware platform and Hypervisor API
  - allow maximum re-use of the test code with different Hypervisors & HW platforms



Qualification Platform – Detailed block diagram



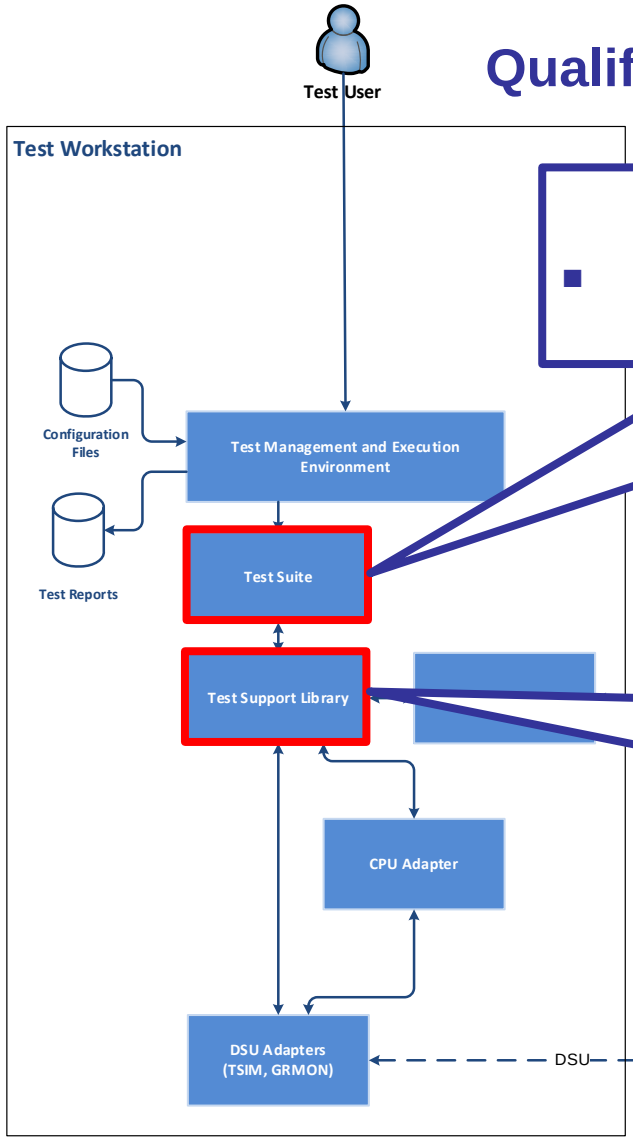
Qualification Platform – Detailed block diagram



Test Management and Execution Environment

- COTS application PyCharm IDE including the PyUnit unit testing framework.
- Provides:
  - Graphical environment to the user (actor) for the execution of the tests
  - Loading the Qualification Test Suite with the test scenarios and cases
  - Execution of the test suite using the PyUnit , the Test Support Libraries and Test Adapters
  - Creating the test reports after the test suite execution.

Qualification Platform – Detailed block diagram



Qualification Test Suite

- Python test scenarios (group of test cases and test steps) that validate the features of the Hypervisor

Test Support Library

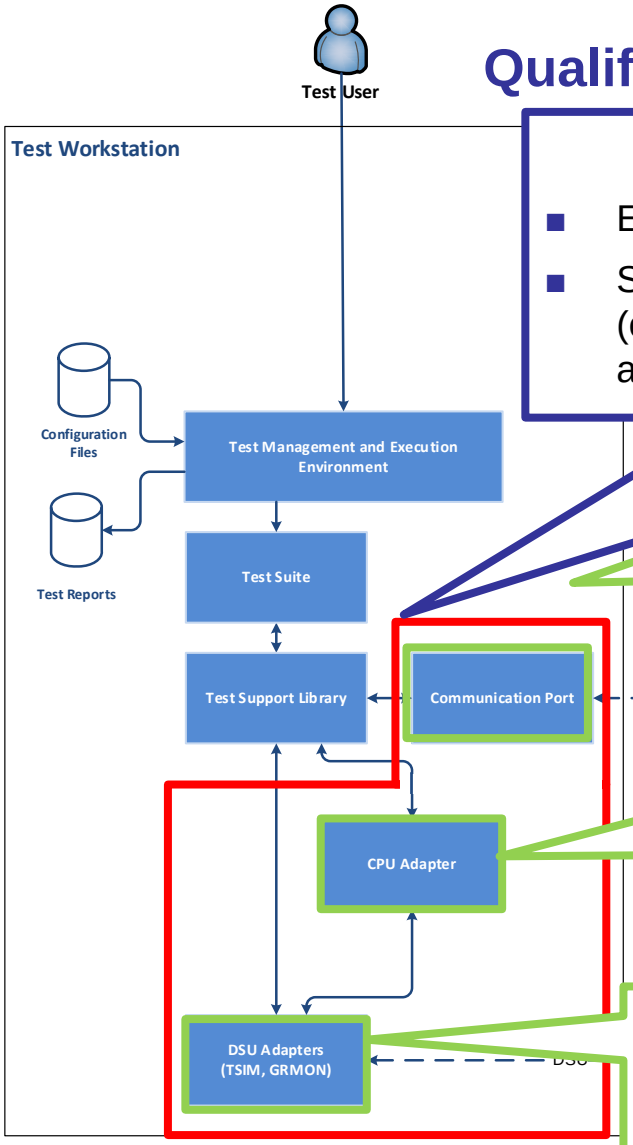
- Python utility functions that implement specific common functionalities that is used by test cases

Qualification Platform & Test Suite

IMA Kernel (SUT)

Target Platform

Qualification Platform – Detailed block diagram



Test Adapters

- Enable the communication with the target platform
- Software adapters for performing hardware-specific operations (e.g. read/write registry/memory, add watch points etc.) in an abstract way through a generic interface for the test support library.

Communication Port

- Serial communication protocol implementation between the qualification platform and the test partitions of the target platform
- Used to trigger the execution of tests (or test steps) on the target platform and collect test results.

CPU Adapter

- Set of services that are not dependent on the target CPU, e.g. check CPU HW registers and / or specific memory areas

DSU Adapter

- Debug functionality for different support DSU components, e.g. GRMON for LEON-based platforms or TSIM

Qualification Platform & Test Suite

IMA Kernel (SUT)

Target Platform

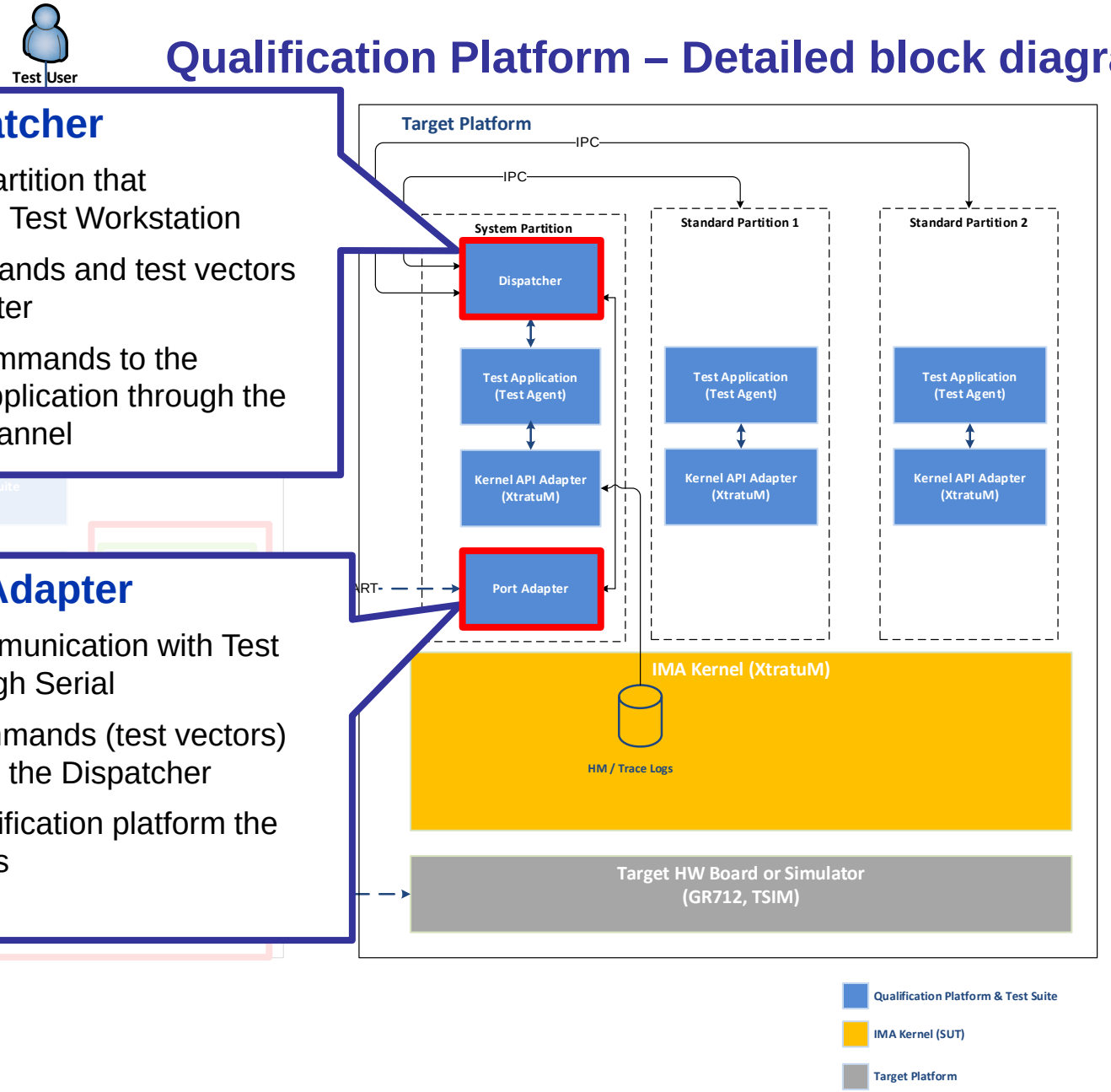
Qualification Platform – Detailed block diagram

Dispatcher

- Part of a system Partition that communicates with Test Workstation
- Retrieve the commands and test vectors from the Port Adapter
- Dispatches test commands to the appropriate Test Application through the appropriate IPC channel

Port Adapter

- Synchronous communication with Test Workstation through Serial
- Receives test commands (test vectors) that are forwarded the Dispatcher
- Sends to the Qualification platform the test replies/outputs



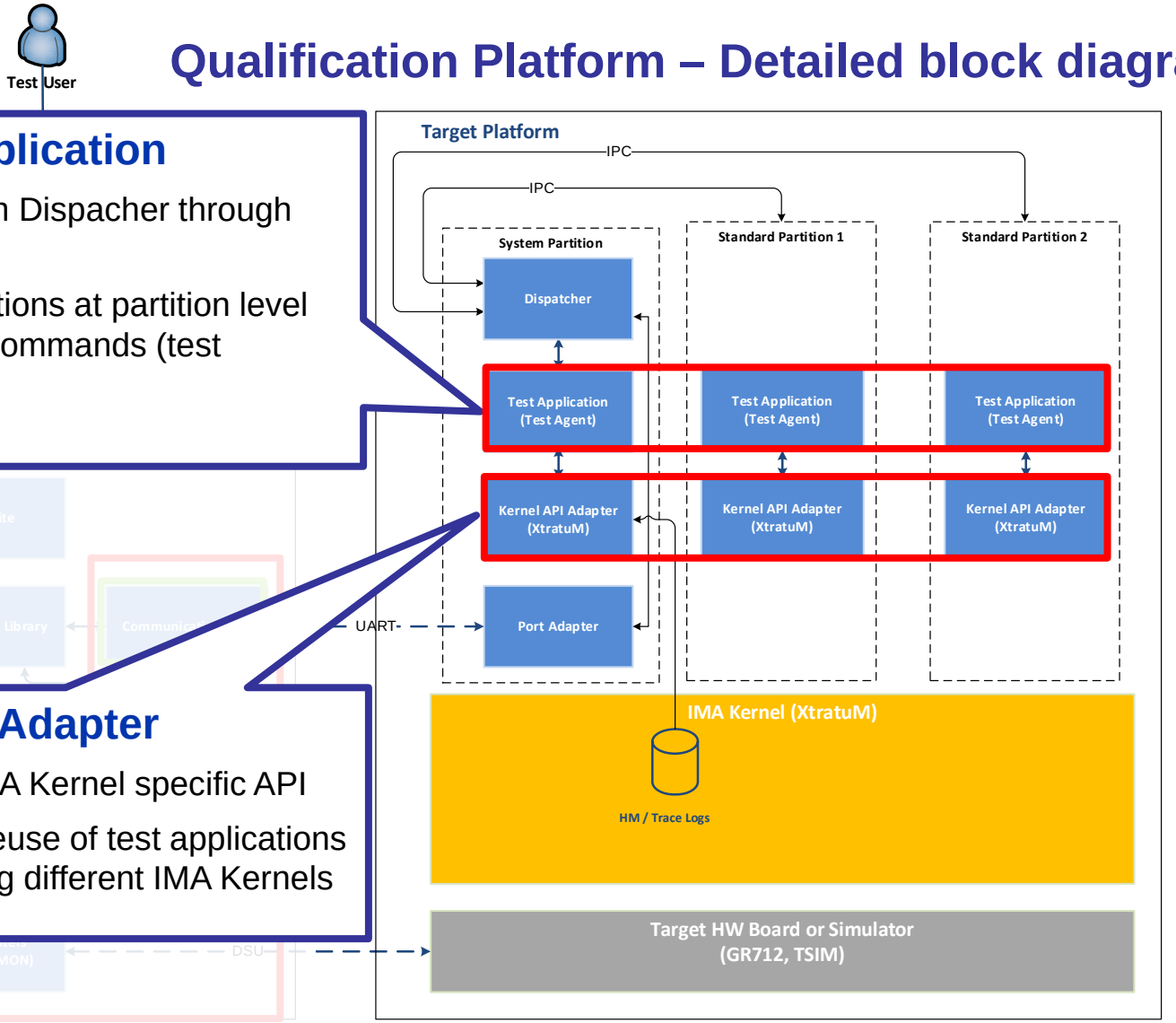
Qualification Platform – Detailed block diagram

Test Application

- Communicates with Dispacher through IPC channels
- Perform test operations at partition level based on the test commands (test vectors) received

Kernel Adapter

- Wrapper of the IMA Kernel specific API
- Enables efficient reuse of test applications and tests for testing different IMA Kernels



Test Suite - Objectives

- Validation of XtratuM hypervisor features:
  - Time Partitioning
  - Space Partitioning
  - Failure Containment and Recovery
  - Interrupt Handling
  - Initialisation
  - I/O Access to external memory mapped devices
  - Partition Services
  - Partition Management
  - Time Management
  - Inter-Partition Communications
  - Memory Management
  - Health Monitoring

Test Suite - Specification

- Specification of the test suite is provided in “D07 Test Plan for Qualification of IMA Separation Kernels” (“IMA-SP Kernel Qualification Preparation” GSTP activity):
  - Initialisation Management
  - Partition Mode Management
  - Time Partitioning
  - Inter-Process Communication
  - Health Monitoring and Trap Management
  - Time Management
  - Cache Management
  - FPU Management
  - Sizing
  - API
  - Hardware Specific Requirements
  - Dependability and Robustness

XM-Q detailed activities (1/2)

During the study a set of activities were performed in XM-Q hypervisor in order to reach a qualification ECSS level B:

- Technical specification: a complete software requirements specification.
- Architectural design: upgrade the design and improve the portability. Integration testing plan.
- Detailed design and implementation:
  - Source code refactoring to comply with the upgraded technical specification, design and quality requirements.
  - Unit and integration tests campaigns.
  - Software user documentation
- Product assurance activities
  - Software product assurance plan
  - Software product assurance report: metrics, coding standards, etc.

XM-Q detailed activities (2/2)

- Validation activities
  - Software validation strategy (plan)
  - Software validation specification
  - Implementation of test-suite
  - Validation campaign
- Verification activities
  - Software verification plan
  - Software verification reports
- Support and maintenance
  - Provide support during the qualification campaign.
  - Management of the problems detected during the campaign: update documentation and software.

Qualification Platform and Test Suite detailed activities (1/2)

- Qualification Platform activities
  - Design and implementation of test workstation software components to perform:
    - specific test functionalities
    - hardware-specific operations
    - low level communication interface
    - debugging operations with the target hardware using a generic interface (DSU adapter)
  - Implementation of TSIM-specific DSU adapter
  - Design and implementation of communication protocol between the test workstation and the target platform based on serial communication protocol.
  - Design and implementation of target platform test infrastructure software components:
    - Test dispatcher
    - Generic Kernel API wrapper
    - Partition test application for test commands execution

Qualification Platform and Test Suite detailed activities (2/2)

- Test Suite activities
  - Design and implementation of test scenarios in Python in compliance with “D07 Test Plan for Qualification of IMA Separation Kernels”
  - Design and implementation of Unit Test Simulator for unit test evaluation of Test Suite
  - Execution of Test Suite against XtratuM IMA Kernel using TSIM simulator environment.
  - Supported the execution of the test suite against XtratuM by TAS-F and ESA.

TS validation activities results

- During the validation campaign with respect to TS several results were obtained that can be summarized as follows:
  - Building a test suite covering different aspects: functional, robust, correctness and performance.
  - Complete traceability against TS requirements.
  - Definition of regression testing strategy
  - Qualified configuration parameters to be used in future missions.
  - Coverage obtained by all testing activities is greater than 95%.
  - Robust XM-Q kernel against processor errata and technical notes reported by the manufacturer (Gaisler).
  - Improve of the quality, reliability and confidence of the XM-Q hypervisor

RB validation activities results (1/3)

- Two independent RB validation executions have been performed: by TELETEL and by TAS-F
- Overall results are summarized as follows:

	TLT Results		TAS-F Results	
	#	Ratio	#	Ratio
PASS	**33**	**71.74%**	**28**	**60.87%**
FAIL	**13**	**28.26%**	**18***	**39.13%**
Total Test Scripts	**46**		**46**	

- **Note*:** Discrepancy between TLT's and TAS-F results due to:
  - (4 out of 46 tests) Incompatible version of TSIM simulator,
    - i.e. use of TSIM 2.0.51 instead of the required TSIM 2.0.61
  - (1 out of 46 tests) Issues with serial link, unexpected serial timeouts when external synchronization was used

RB validation activities results (2/3)

- Justification for all the detected failures (well elaborated and documented in the qualification report):

1) Inconsistency between Test Plan (D07 SSL/10254/DOC/007) and XM technical specification (SRS) [*11 out of 46 tests*] **– Accepted by the consortium**

- *Affected scenarios:*
  - DR-4, Invalid API Calls (DR4_B)
  - FM-1, FPU Configuration and Context (FM1)
  - HMTM-4, Errors and Health Monitoring Events (HMTM4_B, HMTM4_C)
  - HMTM-5, Health Monitoring Log Behaviour (HMTM5_A)
  - IPC-1, Sampling Ports (IPC1)
  - IPC-2, Queuing Ports (IPC2)
  - MM-2, Partition Mode (MM2)
  - SP-1, Memory Region Access (SP1_E)
  - SP-2, Bit Level Access (SP2)
  - MBT_IPC_001, Port Status (MBT_IPC_001)

XtratuM API call to reset a partition with invalid reset mode parameter returns NO_ERROR message while Test Plan expects an INVALID_PARAMETER error message

XtratuM is using FIFO policy on HM Log while Test Plan is expecting LIFO policy HM Log

Test Plan assumes the usage of an "execution-only" memory area while XtratuM SRS specification does not support it

2) Supporting tools limitation, e.g. usage of LEON simulator (TSIM) for accessing system registers [*2 out of 46 tests*]

- *Affected scenarios:*
  - CM-1, Cache Support (CM1_A)
  - HMTM-6, Kernel Errors (HMTM6)

Hardware register CCR value changes (CCR.ip and CCR.fi) cannot be detected when expected with TSIM usage

RB validation activities results (3/3)

- Overall validation activity conclusions:
  - Validation campaign was successful
  - No functional issues were detected from the validation against technical specification (SRS) of XtratuM hypervisor
  - Detected failures on specific test steps are **expected to happen** considering
    - *the differences between the Test Plan Specification (D07 SSL/10254/DOC/007) and actual XtratuM hypervisor technical specification (SRS);*
    - *supporting tools limitation (TSIM usage)*
- Follow-up activities
  - Synchronisation of Test Plan Specification with technical specification of the hypervisor
  - Extend validation supporting tools to additional Debug Support Units (DSU), e.g. GRMON, to cover all test cases. (on-going activity)
  - Maintain validation test suite accordingly.

Verification activities

- ISVV related activities on XtratuM artefacts were performed:
  - Verification of the technical specification
  - Verification of the software architectural design
  - Verification of the software detailed design
  - Verification of code
  - Verification of software unit testing
  - Verification of software integration
  - Verification of software validation with respect to the technical specifications
  - Verification of software validation with respect to the requirements baseline
  - Evaluation of validation: complementary system level validation *(out of scope)*
  - Verification of software documentation
  - Schedulability analysis for real-time software
    - *limited to worst case execution time (WCET) results of the XtratuM functions*
  - Technical budgets management
  - Behavior modelling verification *(not performed, NCR was issued)*

Main conclusions and next steps

- XtratuM hypervisor has reached a mature state for SW criticality ECSS Cat.B improving the quality, reliability and confidence of the product.
  - Validation against TS on real hardware (GR712 board) is performed
  - To complete validation against RB on real hardware (GR712 board)
- Availability of a generic Qualification Test Framework that can be adapted for different Hypervisor Kernels and hardware platforms.
- Availability of a generic Test Suite for the Qualification of IMA Separation Kernels that can be adapted for different Hypervisor Kernels.
- Follow-up GSTP activity: Multicore IMA Separation Kernel Qualification, preparation and execution

XtratuM over LEON Processors

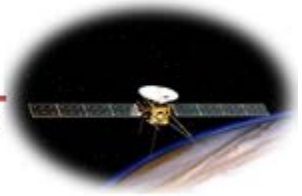
PLATiNO
(OBC)
XtratuM with RTEMS
(GR740)

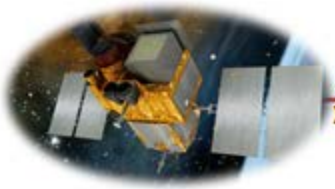
Launching Dates

2020 2021 2022 2023 2024

MERLIN
XtratuM
with RTEMS
(GR712)

JUICE
(MAJIS)
XtratuM with LithOS
(GR740)





SVOM
(MXT & ECLAIRS)
XtratuM with LithOS
(GR712 mono and
dualcore)

SWOT
XtratuM with RTEMS
(GR712)

Contact

- 124 Kifissias Avenue
- 115 26 Athens, Greece

- Tel: +30 210 6983393
- Fax: +30 210 6983391

- email: rtd@teletel.eu
- http://www.teletel.eu

- Ciudad Politécnica de la Innovación, Edificio 9B Despacho 3
- Camino de Vera s/n, 46022 Valencia, Spain
- Tel: +34 963 294 704

- email: info@fentiss.com
- https://fentiss.com