Integrated Modular Avionics for Space

IMA4Space

ADCSS 2012

J.Windsor
ESTEC

23-10-2012

European Space Agency

Agenda

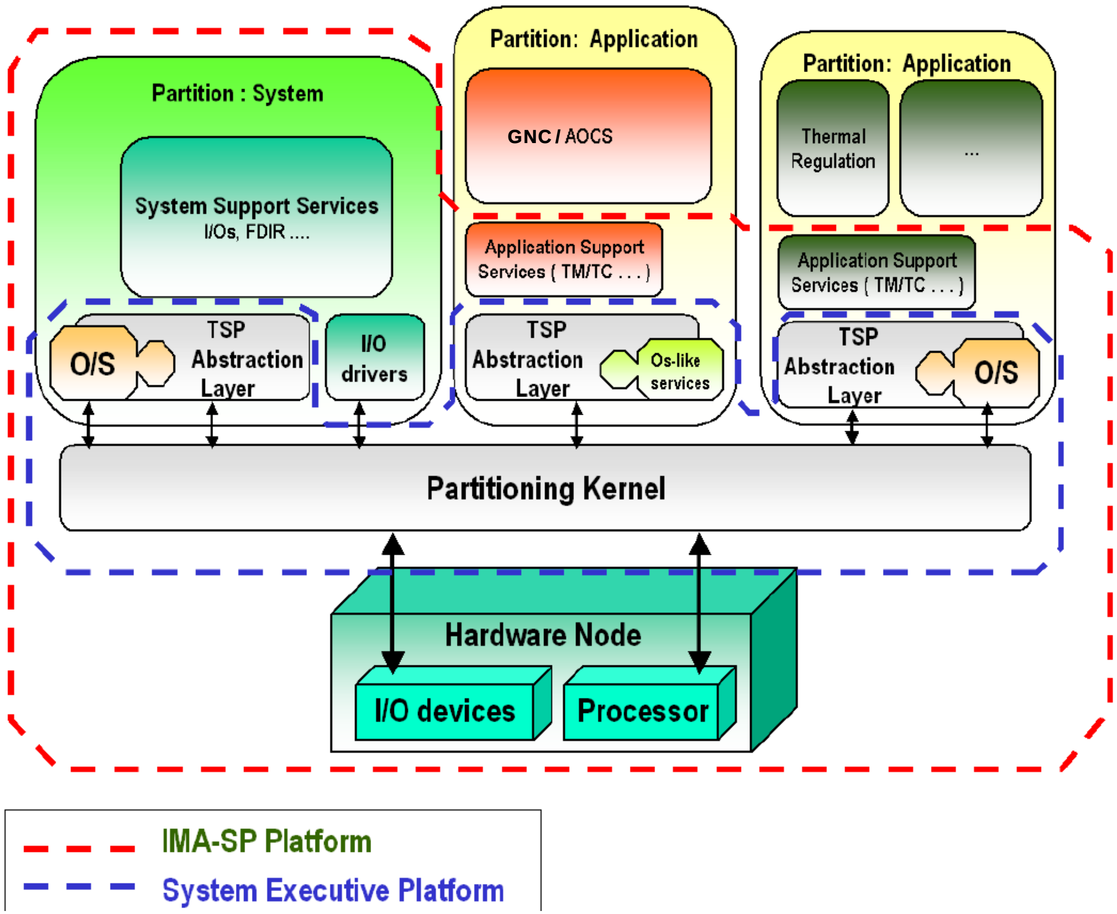
1. Introduction
2. Architecture
3. Implementation Status of System Execution Platforms (SEPs)
4. Use Case: (Platform Software) Astrium
5. Use Case: (Platform & Payload) Thales/SCISYS
6. Use Case: (IO) GMV
7. Conclusion of the use cases

Introduction

- Kick Off (July 2010)
- Activity Phase 1 – System Assessment
  - IMA-SP system definition, architectural design and component specification (software system engineering)
  - SEP products design specification
  - Findings consolidated through industrial review
- Activity Phase 2 – Preparation of the Software Building Blocks
  - Development and pre-qualification of SEP's
  - Prototyping of I/O handling software and demonstration with representative hardware (RASTA systems, 1553 and SpaceWire links)
- Activity Phase 3 - Implementation
  - Platform software use case
  - Payload software use case
  - I/O use case
- Final Presentation (5th/6th December 2012)
- All documents shall be publically available

IMA-SP Architecture

- Hardware node(s) → LEON2/3 + IO devices
- System Executive Platform (SEP)
  - Partitioning kernel – executes independent partitions with static cycle
  - TSP Abstraction Layer (derived from ARINC 653 APEX)
  - RTEMS Guest OS - executes processes within partition
- System support services
  - system middleware e.g. I/O handling, FDIR, OBSM
- Application support services
  - application middleware e.g. TM/TC interface, access to on-board parameters



Implementation status of System Execution Platforms (SEPs)

- XtratuM (XM) SEP
  - LEON2 MMU and LEON3 MMU
  - Compliant to SSS & TSP Services API document
  - XM and RTEMs modification for performances and mapping requirements from experimentation
  - Test suite for TSPAL/XtratuM (LEON3 and LEON2)
  - Test suite for TSPAL-RTEMS/XtratuM (LEON3 and LEON2)
- Pike OS SEP
  - rtems-tsal and ReleaseNotes compliant SSS & TSP Services API document
  - Pike OS SEP on LEON2 MMU and LEON3 MMU
  - SEP RTEMS personality Validation Suite
- AIR SEP
  - Fixing the interrupt virtualisation race conditions
  - Leon 2 implementation
  - Partition restart implementation
  - Completing the remaining tests and documentation

IMA-SP Stakeholders

Use Cases A + B

Actor:	System Architect	System Integrator (early phases)	IMA-SP Platform Supplier	Application Suppliers	System Integrator (later phases)
is provided with…	- Customer needs	- High level requirements - General architecture design - Standards	- IMA-SP Platform requirements - Configuration of the IMA-SP Platform - Standards	- Application requirements - Resource allocation - Toolset and IMA-SP Platform simulator - Pre-qualified configured IMA-SP Platform - Standards	- Pre-qualified configured IMA-SP Platform - Pre-qualified applications
has to provide …	- High level requirements - Standards - General architecture design	- Verified requirements - IMA-SP Platform requirements - Configuration of the IMA-SP Platform - Application requirements - Resource allocation for the applications	- Pre-qualified configured IMA-SP Platform - SEP supplier & guest RTOS - System / Application Support Services - Toolset and IMA-SP Platform Simulator	- Pre-qualified applications - Partition Emulator for qualification of dependent applications	- IMA-SP Platform requirements - Configuration of the IMA-SP Platform - Resource allocation for the applications - Application requirements - Integrated qualified system

IMA SP : Use Case A Platform Software

23 10 2012

All the space you need

ASTRIUM
AN EADS COMPANY

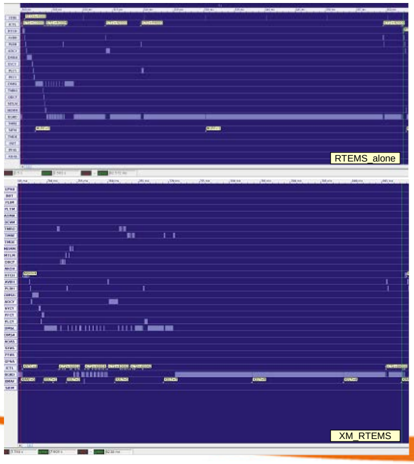
Use case A : Architecture

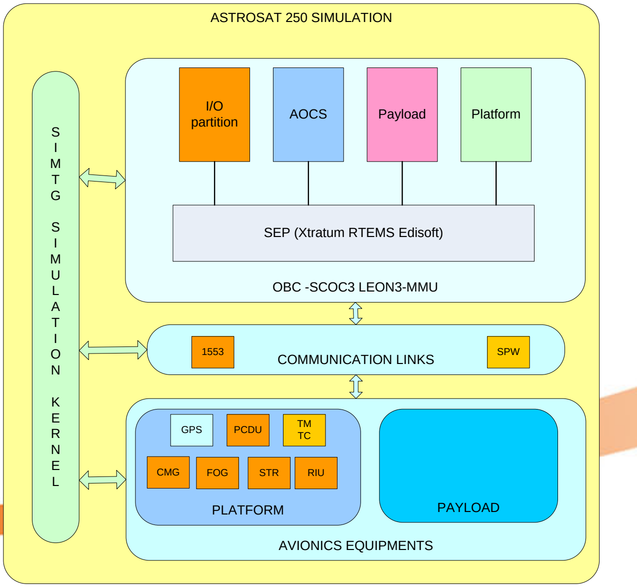
- Operational test scenario on NSVF
  - ***IMU equipment management :*** TM/TC management and 1553 exchange in an open loop configuration.
  - ***AOCS functional*** AOCS behaviour in close loop (MAN and CAP algorithm).

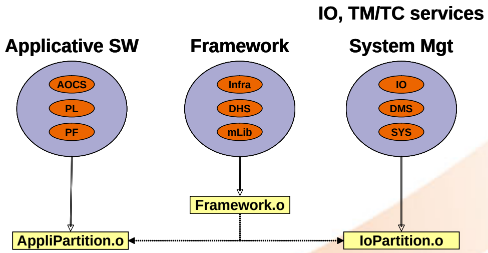
- First step AS250 Partitioning in two partitions on XtratuM SEP
  - One I/O partition for DHS, I/O and system
  - One partition for AOCS, platform and payload

- Second step AS250 Partitioning in four partitions on XtratuM SEP
  - I/O partition for DHS, I/O and system
  - AOCS,
  - platform
  - payload

- Metrics for performances



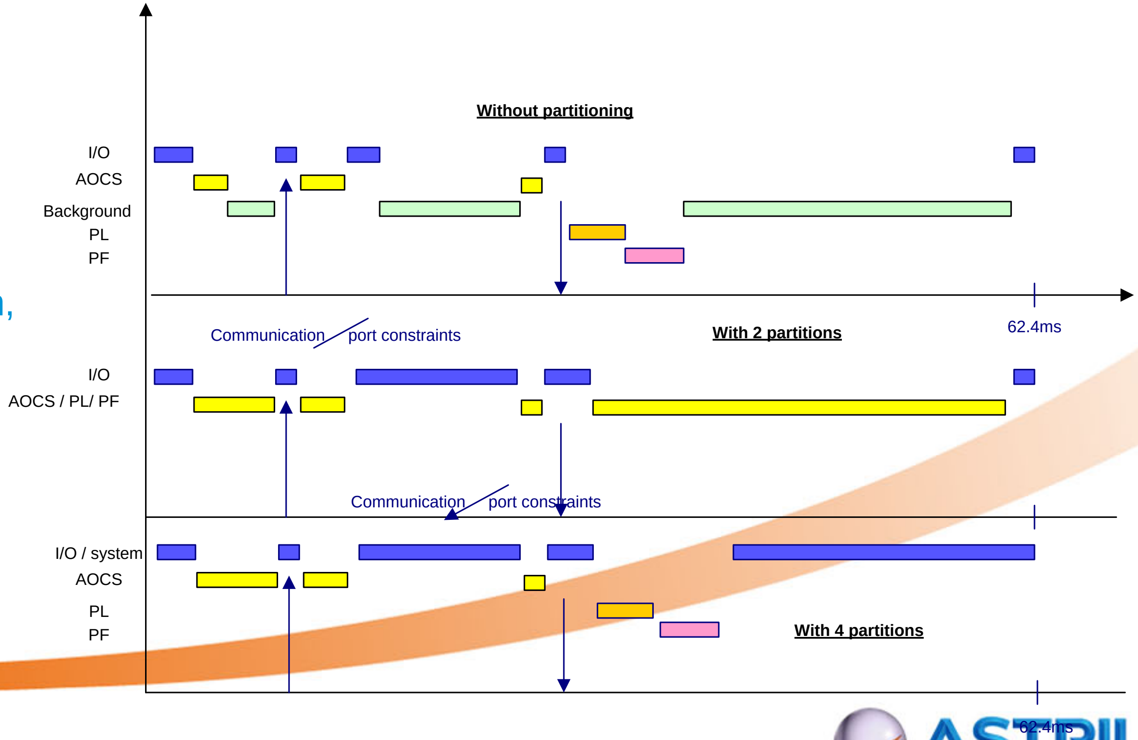


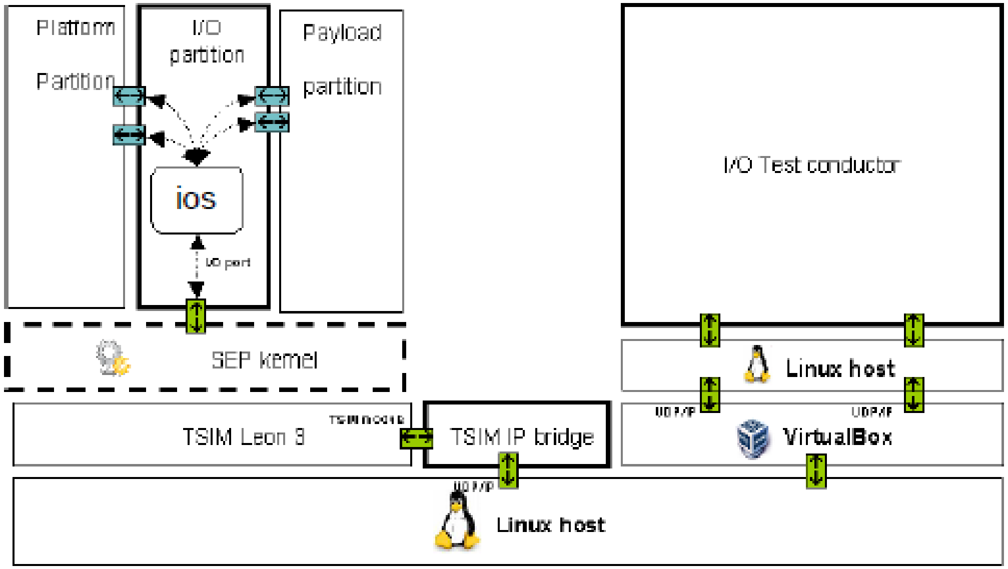


Use case A : Status

- Redesign and configuration (communication, interrupt, space partitioning)
- End to End flow model for computation time characterization and management of virtualised interrupt
- Development of automatic code generator to redesign automatically the interface between partitions using ARINC 653 communications ports from messages data base
- I/O management by communication port with operational constraints (device exchange through 1553 buses)
- Management of TM/TC : software buses encapsulated in communication port

- Development of a framework (libraries, TM/TC services, events) to be part of partition container.
- Scheduling plan for initialisation, synchronisation by On Board Time and change to an operational scheduling plan.
- Design for 4 partitions (I/O, AOCS, PL, PF) using the automatic code generator





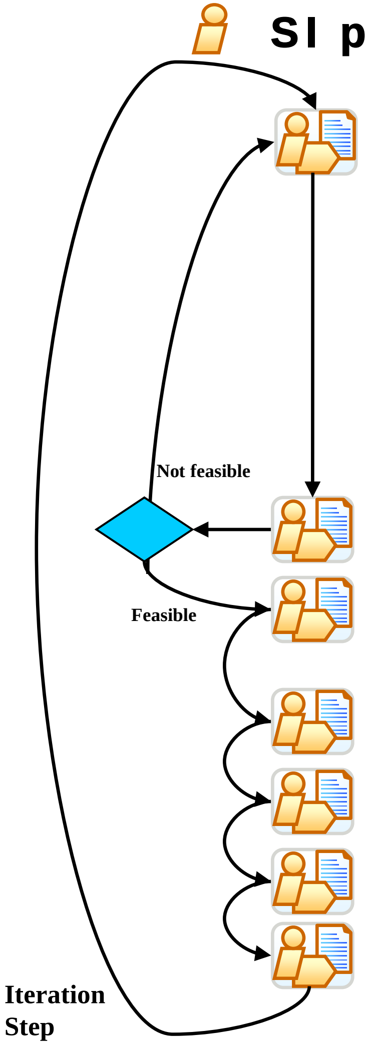
Platform & Payload

USE CASE B

Use-Case B : TAS and SCISYS

System Integrator perspective (TAS)

SI perspective: Iterative Design / Development / Integration process:



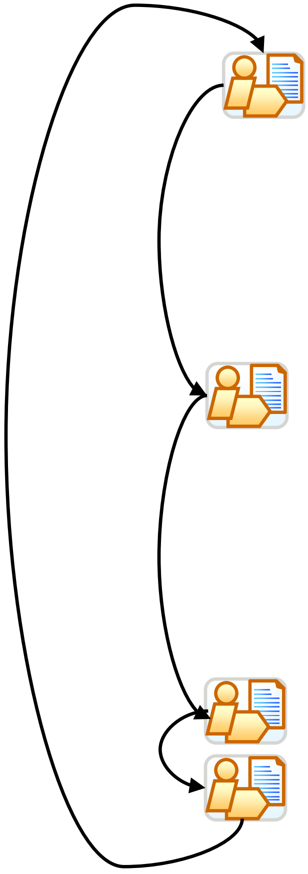
- Negotiation point with Partition Suppliers
  - I/O management:
    - Decide I/O strategy (I/O partition for TM/TCs / Eqt. Com)
    - Specify inter-partition communications (Ports, Channels, Message Types)
  - Specification of system management issues:
    - Specify boot and maintenance strategy (module schedules, patch mechanisms)
    - Specify FDIR strategy (software Watchdog, Health Monitoring Strategy)
  - Resource allocation:
    - Specify allocated resources to each partition (memory, time, …)
- Feasibility analysis
- Configuration of the platform:
  - PikeOS kernel configuration
  - I/O development / update
- Tests and validation of the platform
- Delivery of the “use-case environment” to partition suppliers (PLATFORM and MIRAS)
  - Issue : who provides the partition stubs ? → for use-case B : System Integrator
- Individual partition acceptance
- Partition Integration and validation

Status: 1 successful iteration. Still remains 3 iterations.

Use-Case B : TAS and SCISYS

Partition Supplier perspective (TAS)

PF perspective: Iterative Design / Development / Validation process:

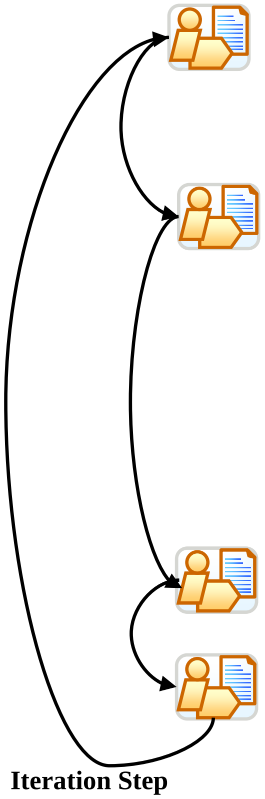


- Negotiation point with System Integrator
  - I/O management: all TM/TC and Equipment communications via IPC and I/O partition
  - Boot, Maintenance and FDIR strategies → many impacts on the original project
  - Resource allocation:
    - » MAF = 125 ms, frame execution time : 50ms
    - » no major changes in scheduling and memory from original project
- Partition Development (port of original project into PLATFORM partition)
  - Replace OSTRALES RTOS by RTEMS
  - Port Hardware Dependant Software on top of TSP-Abstraction Layer communication ports
    - » TM / TC completed
    - » Equipment communication (in progress)
  - Port System Management Software library & Applications
- Test and Validation of the Partition
- Delivery of the Partition Binary Image to System Integrator
- **Status**:
  - Development on-going with the porting of the PLATFORM applications
  - Early Results: scheduling and TM / TCs are validated.

Use-Case B : TAS and SCISYS

Partition Supplier perspective (SCISYS)

MIRAS perspective: Iterative Design / Development / Validation process:



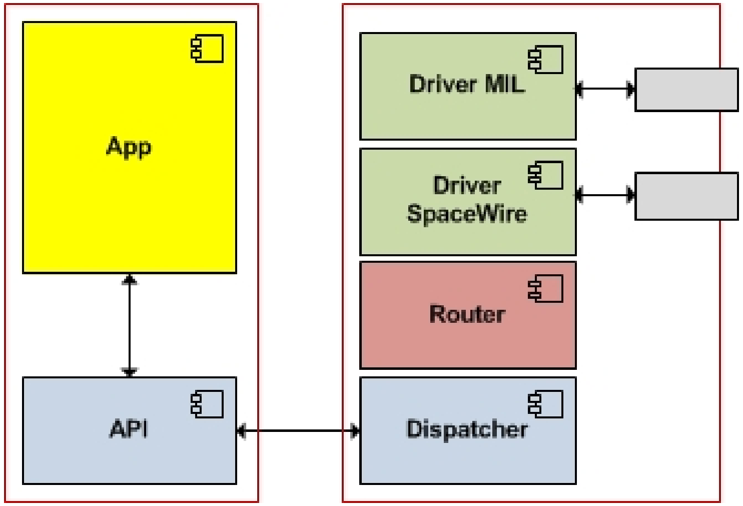
- Negotiation point with System Integrator
  - Scheduling: MIRAS needs to be modified to fit with the MAF
  - Impact: replacement of the LLSW and removal of some functionality from MIRAS, e.g Memory Scrubbing
- Partition Development
  - Low Level Software (LLSW) Port:
    - Removal of all software which interacts/controls the hardware
    - Replaced with IPC channels which communicate with the SVF via the IO partition
  - MIRAS Port:
    - Architecture design changes : Direct communication with the hardware replaced by:
      - request data from the SVF in one execution window and receive it in a subsequent execution window.
    - Removal of unnecessary code e.g. Memory scrubber
- Test and Validation of the Partition
- Delivery of the Partition Binary Image and SVF to System Integrator
- **Status**:
  - LLSW IPC port & MIRAS TM/TC Manager completed
  - SVF tool framework complete, development on-going with the porting of MIRAS
  - Early Results: data successfully between SVF and the MIRAS partition

Generic I/O Component

USE CASE C

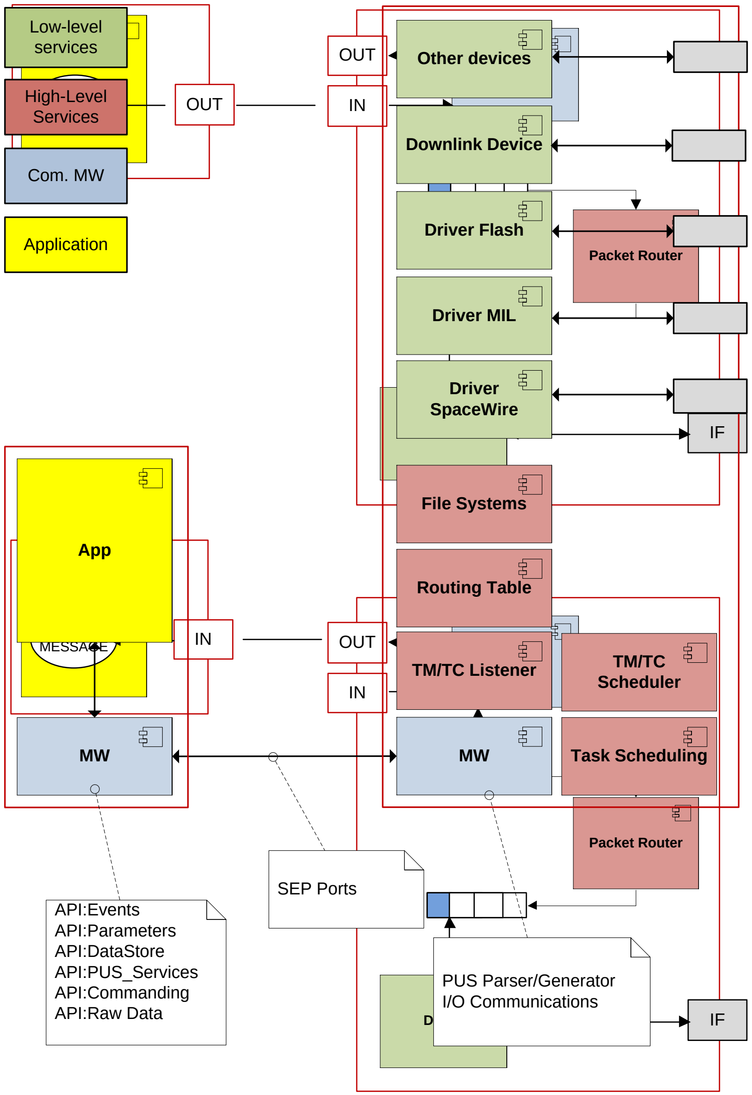
GENERIC I/O COMPONENT

- Interacts with other applications through ARINC 653 Ports...
- ... or shared memory
- Allows for higher level abstraction of hardware devices and data buses, through specific Middleware
- Interruptless, it is based on polling and, hence, deterministic
- Provides drivers for:
  - MIL-STD-1553B (Cores: GR1553B and B1553BRM)
  - SpaceWire (GRSPW2)
  - Ethernet (GRETH) with UDP/IP stack
  - UART (APBUART)



I / O COMPONENT INTERFACES

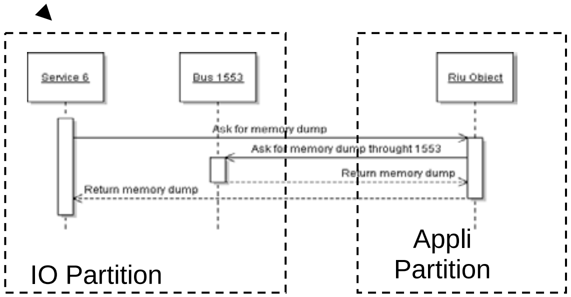
- Current API (Middleware)
  - **io_init**
  - **send_read_request**
  - **get_reply**
  - **send_data**
- Remote ports
  - **Subscribe option**
- Shared memory

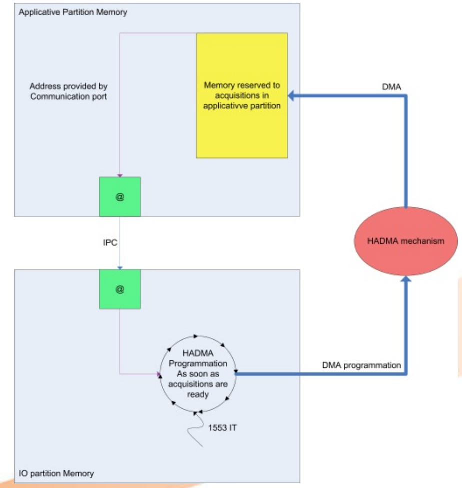


Use Case Feedback

Use case A : design contraints and solution

- Operational application with interrupt synchronisation
  - Solution : scheduling plan adapted to the interrupt synchronisation
- Operational application with object design
  - Solution for the use case : multiplication of communication port
- Operational software with enable/disable interrupt
  - Solution for the use case : Xtratum services
- On Board Time interrupt multiplexed
  - Solution for the use case : wait on the first one, no timers drift on the NSVF
  - Solution for the future : dedicated line or interrupt handler in BSP
- Operational application with complex data structure (1ko of industrial data / MIF => 200ko of structured data /MAF to be transferred from I/O partition to application partition in 3ms in order not to redesign completely the software)
  - Solution for the use case : shared memory or DMA mechanism (already designed to be tested)
- The snooping on the leon3 cache does not work with MMU
  - Solution for the future : memory sectors used with DMA should be set uncacheable




Applicative Partition Memory
Address provided by Communication port
Memory reserved to acquisitions in applicativve partition
DMA
@
IPC
HADMA mechanism
@
HADMA Programmation As soon as acquisitions are ready
DMA programmation
1553 IT
IO partition Memory

Use Case B Feedback (1/2)

- Porting an existing application to a partitioned system is not a straight forward process
  - In depth knowledge of the application/design/software is required
  - Architecture/implementation changes are required
- Role / responsibilities definition and contract / licenses issues are important
  - System integrator relies on Partition Suppliers who rely on Platform Supplier who relies on SEP supplier and HW/Simulator suppliers
    - who is responsible if there is a problem ?
- I/O management changes from traditional practices
  - Generally cannot directly read from hardware →communication buses are shared resources managed by an I/O partition
  - New I/O management introduces latency
  - IPC communication is limited and not efficient when big amount of data is exchanged
    - Need to use other mechanisms (DMA or shared memory)
    - Trade-off for I/O mechanisms is not straight forward

Use Case B Feedback (2/2)

- Scheduling of application activities is more complex
    - Take into account other partitions' needs implies to change frame execution time, and/or MAF → impact on traditional practises
        - Schedule of the system drives the schedule of the application
        - If a task needs to execute at a certain frequency this must be accounted for in the system & application schedules
    - Task scheduling has to be synchronised with partition scheduling
        - ensure all critical tasks are completed before context switch
- Using an SEP is not an easy job
    - Need a strong support all along the project !
    - Tool support
- Compatibility of all actors' SVF is an important topic
- Concurrent availability of several test benches / hardware representative environments is required to achieve parallel qualification of partitions

System Executive Platform Feedback

- XtratuM SEP for use case A
  - Pro : product maintenance & adaptability – good level of maturity – OBT synchronisation
  - Cons : Missing GDB debug tool – bootloader
- Pike OS SEP for use case B
  - Pro : Extensive documentation – Development tools very good – Easily configurable – Debug available on TSIM
  - Cons : No tracing mechanism – Missing GDB debug tool – RTEMS interrupt management not implemented
- Edisoft RTEMS para-virtualised for all SEP kernels

Conclusion

- Existing flight software has been re-factored into partitions with partial re-validation on SVF platform
  - Astrium Astrosat AS250
  - TAS-F Sentinel 3 Central Software
  - SCISYS MIRAS payload application
- AIR, PikeOS and XtratuM have been ported to LEON2/3 and pre-validated
  - PikeOS offers DO-178 certification datapack
- Lessons learnt from Use Cases
  - Mastering role definition and process is key to success
  - IO management with current HW is challenging but not impossible
  - Execution Platform support tools & test bench needed
  - HW improvements have been identified

Reminder: Final Presentation

Please join us for the IMA-SP Final Presentation

5th / 6th December 2012 at ESTEC