IMA-SP and Security
Status of Activities & Roadmap

2nd November 2010

James Windsor TEC-SWS

IMA-SP Programme Philosophy

1. The roadmap shall implement the technology maturity steps required to prepare TSP for deployment into space applications
2. Programme Phase-1: "getting it to work"
    a. Minimal or no change to existing computer design
    b. Getting the segregation principle ready for full scale project implementation within the short term
    c. Make TSP System Executive software and support tools available for the LEON architecture
    d. Get experience in the process and TSP architecture by prototyping of S/C representative case-studies
    e. Define Phase 2
3. Programme Phase-2: "optimise a working system"

Programme Phase-1
Overview

Objective 1:

Secure availability of a TSP System Executive (SE)

1. Porting and re-qualification of commercial ARINC653 compliant SE to the SPARC computer architecture.
2. Upgrading and qualifying of existing open source RTOS to become TSP and ARINC653 compliant.

Objective 2:

Get hands-on experience with TSP in the Space context.

Prototyping and Trade-off studies:

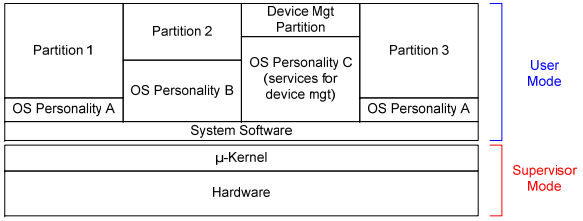
1. Spatial protection strategy
    a. Using either MMU, BPU or Fence-registers
    b. Characterise constraints, performance
2. I/O handling
    a. Study implementation of the I/O handling under the constraint of the TSP and based on re-use of existing hardware (Mil1553, SpaceWire, serial links)
    b. Characterise constraints and performance.
3. Prototyping full scale on-board software by re-implementing existing S/C platform software(s) as a partitioned implementation
    a. Re-use existing project SVF to perform re-validation
    b. Demonstrate that Hosted applications can be validated incrementally.

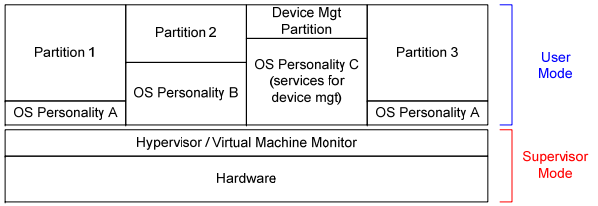
Programme Phase-1
Current ESA activities: Security & IMA-SP

1. Securely Partitioning Spacecraft Computing Resources (SecPar)
    a. Investigating the application of secure time and space partitioning technologies to enable multi-use missions from a single platform

2. Integrated Modular Avionics for Space (IMA-SP)
    a. Define, develop and demonstrate an "IMA for Space" system
    b. Using three viewpoints
        - IMA-SP System Definition & Architecture
        - IMA-SP System Life Cycle
        - IMA-SP Software Building Blocks
    c. Build on existing standards and components
        - ARINC653
        - State-of-the-art Space-grade processors: Leon3/MMU, Leon2/MMU
        - Avionics data links: 1553, Spacewire
        - Existing OBSW and related validation facilities

Securely Partitioning Spacecraft Computing Resources (SecPar)





1. Two parallel activities
    a. SciSys (UK), Astrium (F), Sysgo (D)
    → PikeOS microkernel
    b. Astrium (F), Teletel (Gr), UPV (E)
    → Xtratum hypervisor
2. Define an operational scenario for dual-use spacecraft
3. Establish the functional, operational and resources requirements based on the high robustness SKPP
4. Select separation kernel for use in secure on-board software based on:
    a. conformity to the security requirements
    b. technological maturity
    c. evaluation assurance (CC + EAL)
    d. access to source code
    e. support for the provision for in-orbit maintenance and support
    f. qualification effort at the level of on-board software criticality category B
5. Port technology to a LEON3 processor
    a. PikeOS and XtratuM ported to LEON 3
6. Produce a Secure Partitioning Test Bench to validate the security requirements
7. System demonstration of the separation kernel technology (on a virtual spacecraft simulator)

Integrated Modular Avionics for Space (IMA-SP)

1. Activity Phase 1 – System Assessment
    a. IMA-SP system definition, architectural design and component specification (software system engineering)
    b. SEP products design specification
    c. Findings consolidated through industrial review

2. Activity Phase 2 – Preparation of the Software Building Blocks
    a. Development and pre-qualification of SEP's
    b. Prototyping of I/O handling software and demonstration with representative hardware (RASTA systems, 1553 and Spacewire links)

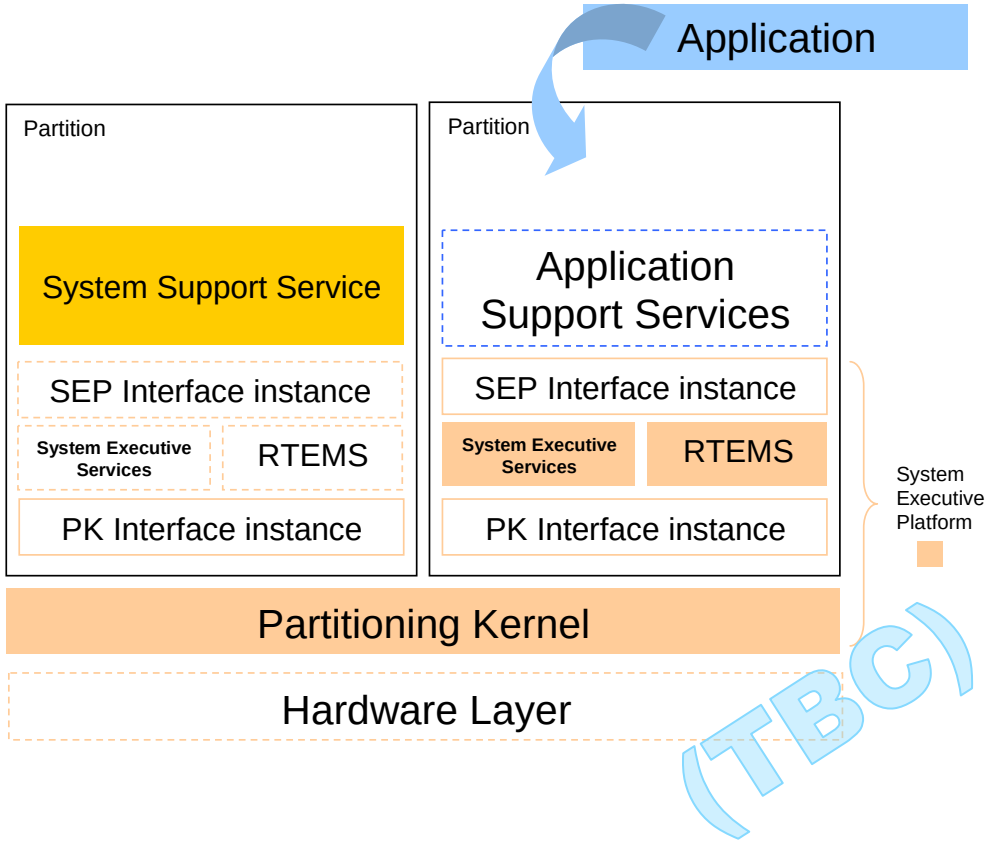
3. Activity Phase 3 - Implementation
    a. Platform software use case
    b. Payload software use case

4. All documents are publically available

ASTRIUM AN EADS COMPANY
gmv INNOVATING SOLUTIONS
SYSGO EMBEDDING INNOVATIONS
ThalesAlenia Space A Thales / Finmeccanica Company
UNIVERSITAT POLITÈCNICA DE VALÈNCIA
gtd
scisys
SPACEBEL
European Space Agency

IMA-SP System Executive Platform
Selected Partitioning Kernel Products

1. pikeOs
   a. Commercial product
   b. Aeronautics background (e.g. selected for A350)
   c. Certification package
   d. Primary hw platform: non Leon
2. XtratuM
   a. Open Source Software (OSS product)
   b. Space background (CNES LVCUGEN program)
   c. Primary hw platform: Leon
3. AIR
   a. RTEMS evolution
   b. Primary hw platform: Leon



Future Activities & Roadmap

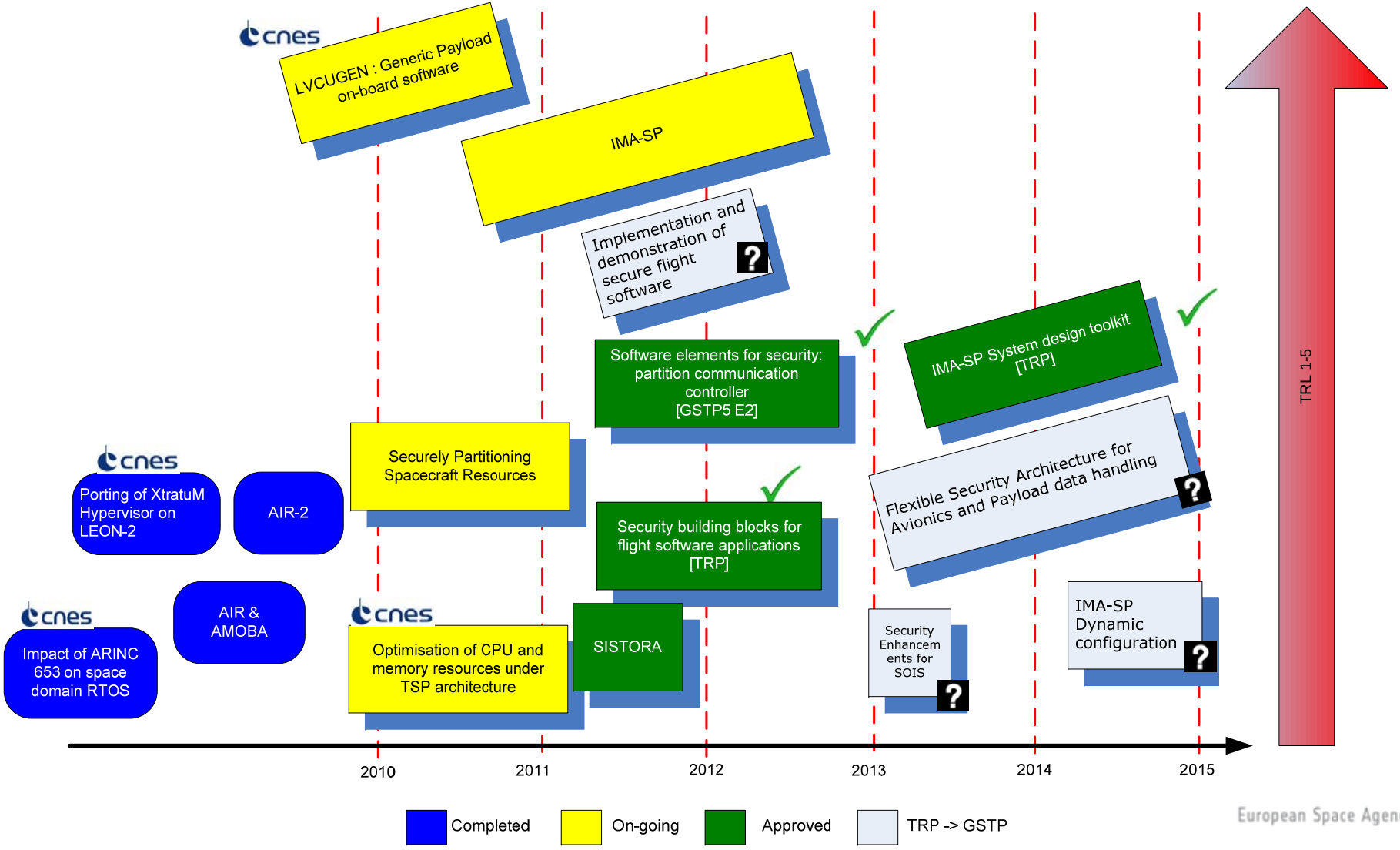
Programme Phase-1
Approved IMA-SP and Security activities

Topic	Title	Prog	Notes
Security	Software elements for security: partition communication controller	GSTP Period 5 Elem 2	Develop a partition communication controller for use in a partitioned avionics system. The controller is effectively an inter partition firewall which allows IPC only as explictly expressed in its configuration. Establish mechanisms to allow the secure re-configuration of the allowed communication paths in flight. See EMITS IITT 09.132.29
IMA-SP	IMA-SP System design toolkit	TRP	A toolkit is needed to enable the system level design, modelling, verification, schedulability analysis, and allocation of system resources (e.g. IO bandwidth and devices, permitted communication channels, CPU load, health monitoring, memory, latency) to spacecraft applications executing on a partitioned avionics platform. The toolkit shall be based on an avionics architectural language (e.g. AADL) and shall enable the iterative development of the spacecraft system.
Security	Security building blocks for flight software applications	TRP	Analyse existing spacecraft systems to identify critical applications that can be integrated together on to a common computing platform (possibly the central OBC) to reduce the number of on-board modules. In addition, the migration of functionality from hardware into the software shall allow the update of these applications while in-flight.
IMA-SP	SISTORA	-	Harmonise the CorDer Reference Architecture and the IMA-SP concepts

Programme Phase-1
Submitted Activities (awaiting approval…)

Topic	Title	Prog:	Notes
Security	–Assessment of the security properties of the hardware supporting avionics and payload data handling –Flexible implementation of Avionics and Payload data handling security functions –MILS architecture for Avionics and Payload data handling (Flexible Security Architecture for Avionics and Payload data handling)	To be submitted for GSTP E3	Identify critical spacecraft applications (e.g. based TM/TC encoders, dedicated navigation security encoders, sensors, actuators), that must for functional or security concerns be isolated from other applications (either in software or firmware) to form security functions which can be integrated together on a common computing platform using secure partitioned avionics. Perform the consolidation needed at the hardware, software and communication bus levels to build into the spacecraft avionics a complete security architecture to enforce integrity, confidentiality and availability of data for untrusted and trustworthy components including the safe and secure update of the software or firmware based security functions.
Security	Security Enhancements for SOIS	TRP (to be re-submitted for GSTP E3)	Add security enhancements (e.g. ensuring data integrity, providing confidential classification to messages, while maintaining availability) to the SOIS communication services used across a distributed avionics platform.
Security	Implementation and demonstration of secure flight software	TRP (to be re-submitted for GSTP E3)	This activity will take the secure partitioning technology, deploy it in a flight representative environment, and demonstrate that the system is resilient to selected types of security / safety threats.
IMA-SP	IMA-SP Dynamic configuration	TRP (to be re-submitted for GSTP E2)	This activity shall define and demonstrate a reconfigurable IMA-SP system to support multiple computing nodes

IMA-SP and Security Programme Roadmap (conceptual)



Progress of the roadmap

1. Phase 1 underway
    a. SecPar
    b. IMA-SP
        – Open invitation to the System Assessment Workshop (≈30/03/2011 @ ESTEC)
    c. Software elements for security: partition communication controller *(IITT GSTP)*
    d. Security building blocks for flight software applications *(approved TRP activity)*
2. Phase 2 preparatory activities (2013 target):
    a. IMA-SP System design toolkit *(approved TRP activity)*
    b. Flexible Security Architecture for Avionics and Payload data handling *(to be submitted to GSTP)*