AMIS

Application of Multiple and Independent Levels of Security (MILS) to SDR - EDA Study Conclusions

Wireless Innovation Forum European Conference 2014
November 4th, 2014 – Rome (Italy)

Overview

- **AMIS: "Application of Multiple and Independent Levels of Security (MILS) to SDR"**
- Contract 12.ARM.OP.303 (AMIS) is awarded by EDA in **November 2012** to an Industrial consortium formed by 7 SDR leading companies
  - Elektrobit (Finland)
  - Indra (Spain)
  - Radmor (Poland)
  - Rohde & Schwarz (Germany)
  - SAAB (Sweden)
  - Selex ES (Italy)
  - Thales (France)

- Study finalized in **December 2013**

- Any results or rights obtained in the performance of Contract 12.ARM.OP.303 are EDA property

Objectives

- **Goal**: *Establishment of a common understanding, among the relevant EU stakeholders, on the application of MILS to SDR*

- **Outcome**:
  - Common set of operational and security requirements
  - Impact analysis of MILS applicability in conventional SDR systems
  - Design and evaluation of candidate SDR architectures implementing MILS

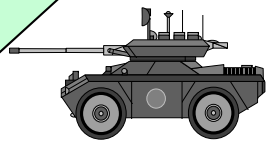
- **Expected impact**:
  - Provide referential requirements and designs for future national and European developments
  - Feed key SDR working groups and initiatives with project's technical findings

Scope

LOWER ECHELONS
- Highly mobile
- Compact solutions (space, weight , power consumption issues)

HIGHER ECHELONS
- High speed comms
- Based on wire, microwave or satellite
- Separated crypto equipment
- Posts' infrastructure issue

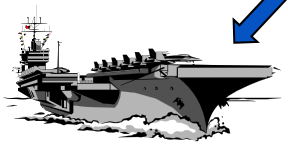
ARMY




MILS in SDR


- AMIS will focus on **Army Tactical environment up to battalion level**
- Considered the stringent scenario in terms of SWAP implications
- Easily adapted to Navy and Air Force contexts



NAVY

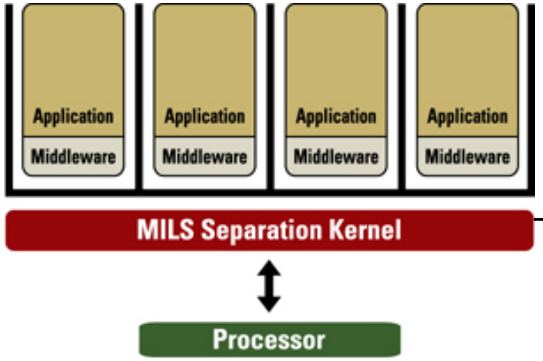
COMPARISON WITH ARMY
- In principle, same reqs for information processing
- Different crypto algorithms
- Less hierarchical interaction

AIR FORCE

Base Concepts

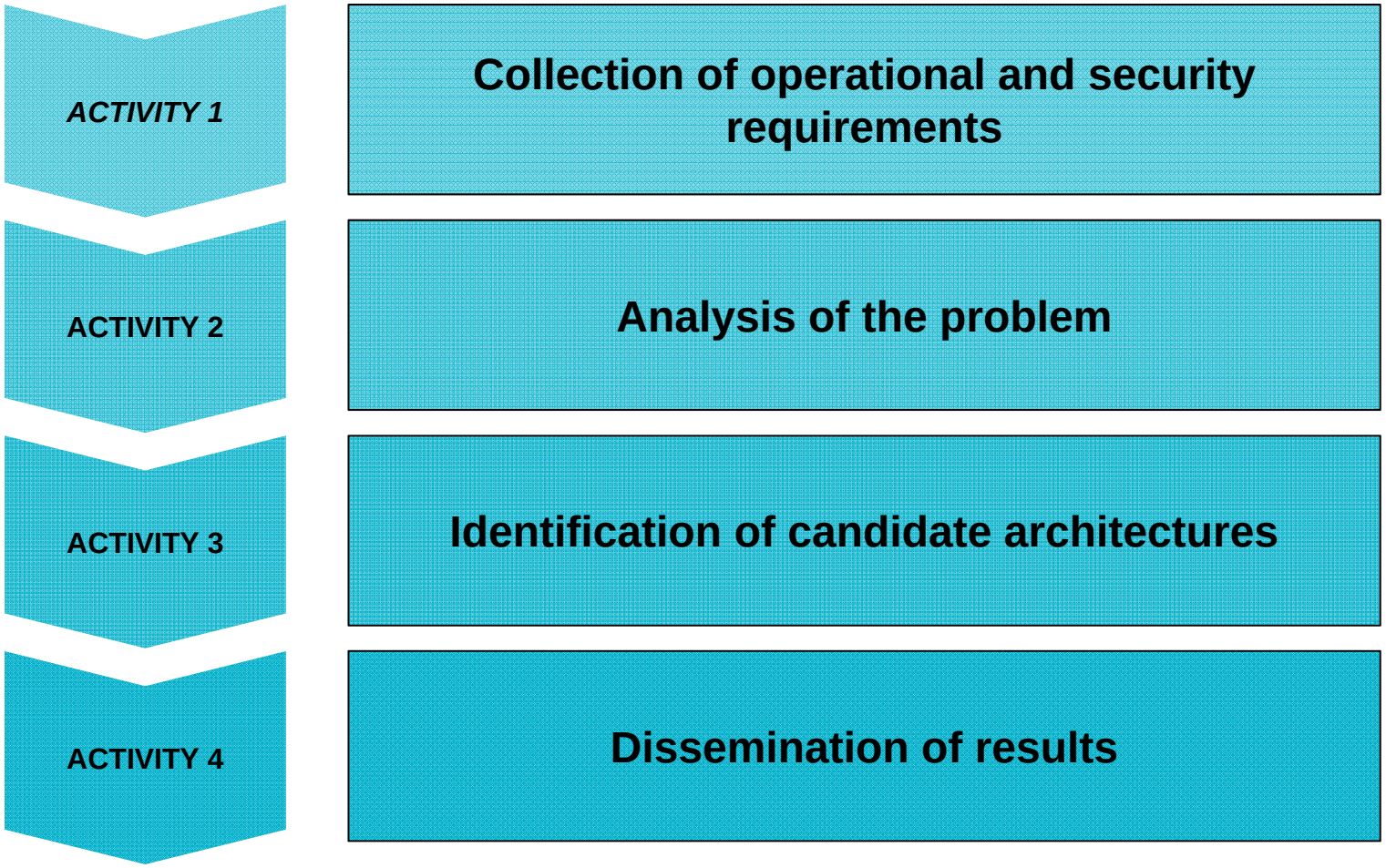
- MSLS: Multiple Single-Level Security
  - **System that securely separates data of differing classifications, one level at a time (e.g. communications platforms and infrastructures).**
- MLS: Multi-Level Security
  - **System that securely process data of differing classifications (e.g. guards, downgraders, firewalls, data fusion, databases).**
- MILS: Multiple Independent Levels of Security
  - **Layered software architecture (kernel, middleware and applications)**
  - **Supports multiple, separated entities, each operating at a different classification level (safety/security/domains). Enforces:**
    - SW architecture that support MLS and MSLS
    - Robust time and space partitioning scheduler
    - Secure information flow, data isolation, periods processing and damage limitation (mathematical verification is possible!)

AMIS target

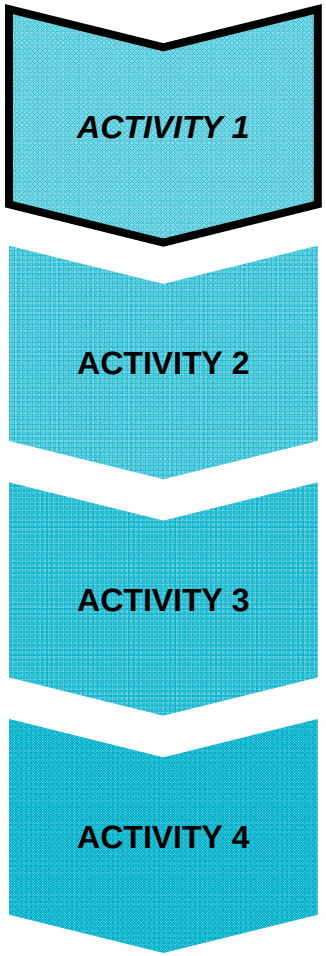


Its security functions are:
- **N**on-bypassable
- **E**valuable
- **A**lways invoked
- **T**amperproof

Organization of the Study



AMIS Study Activities



Collection of operational and security requirements

- **Provide a common basis for elaboration of the other work packages**
- **Focus on user aspects**
- **Elaboration of threats applicable to tactical SDR and to MILS**
- **Derive relevant security requirements**
- **Derive associated EAL and Assurance Requirements according Common Criteria**

Activity 1
Establishment of the Common Operational Picture (COP)

- Collect the operational needs and constraints in terms of classification level (SECRET, CONFIDENTIAL...) for the different kinds of information (voice, BFT/FFT, targeting...) to be transmitted by the units belonging to the different hierarchical levels (battalion, company, platoon...)
- Methodology:
  - Non classified questionnaire was used or interviews of the operational staff of EDA and the MoDs of the participant Governments
  - The responses to the questionnaire and interviews was evaluated and harmonized to provide a COP
- Areas of Interest covered:

•Basic Understanding and Interpretation

•Operational Aspects

•Relevant Information to be exchanged

•Allocation of Information to Hierarchical Levels

•Security Domain with Number of Links of Communication

•Allocation of Radio Types to Hierarchical Level

•Specific needs for Channel Reconfiguration/Reuse

•Role of Multichannel Radios

•Threats for SDR MILS

Activity 1
Establishment of the Common Operational Picture (COP) (II)

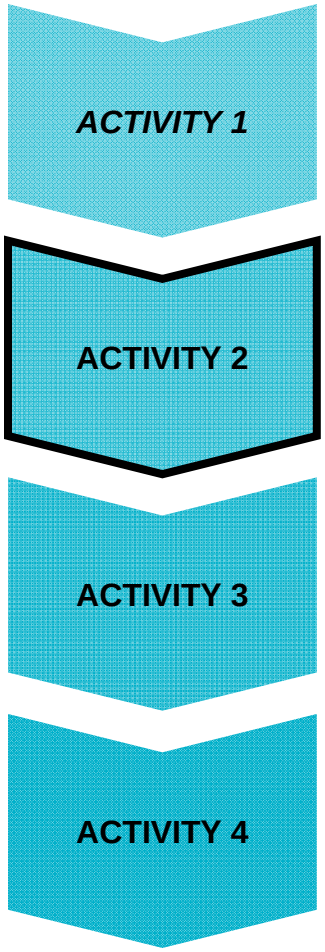
- The received answers demonstrated a shared interest on the MILS capability to SDR technology
- The survey did not lead to a single common environment, but suggested the need to explore different technical solutions, threat environments and security requirements related to MILS in different scenarios
- The outputs of the activity directed the AMIS program to propose a range of MILS technical solutions, useful for the NSAs and/or Governments to evaluate their possible applicability within the Software Radio solutions

Activity 1
Threat Analysis and Security Requirements

- An in-depth analysis was performed to Identify the threats to SDR and to information systems with MILS.
- Common Criteria was used as the common framework for the definition of the Security Requirements for SDR implementing MILS.
- AMIS does not provide a solid/strict view on SAR and EAL
  - Avoid constraining implementations to a specific MILS architecture
  - Provide freedom of choices regarding effort of design, development and evaluation.
  - Limited and diverse views from NSAs
- Suggested Guidelines
  - Security Assurance Level equivalent with EAL 3 package for the whole SDR system if handling data up to “RESTRICTED”
  - Security Assurance Level equivalent with EAL 4 package for the whole SDR system if handling data up to “SECRET”
  - Higher level of assurance (EAL 4 and over) can be considered to the following cases for extremely sensitive components of the system (e.g. separation kernel) that are essential for enforcing the security functions
    - **However, due to lack of available certified products and severe cost-impact of such a recommendation, the AMIS study does not propose a specific EAL package for these cases.**

EAL: Evaluation Assurance Level
SAR: Security Assurance Requirements

AMIS Study Activities



Analysis of the problem

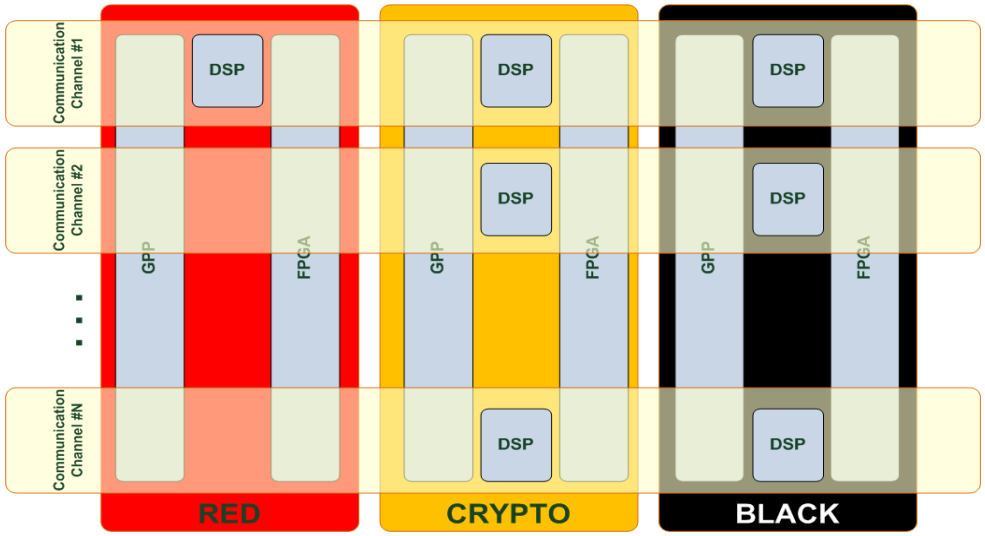
- Analyse the impact of the MILS application to the different elements composing a SDR set
- Impact analysis on SDR hardware
  - Memory, power supply, ports, buses, interfaces
  - Processing elements (GPP, DSP, FPGA…)
- Impact analysis on Operating Environment
  - Survey of applicable software COTS products
  - Impact of MILS on the middleware
- Impact analysis on Platform and Waveform components deployment and interactions
- Global impact analysis on MILS application to SDR

Activity 2
Analysis of the problem

- Identification of the impact of MILS in the different components of an SDR Architecture
  - Hardware (processors, external interfaces, power supply and internal buses)
  - Operating Environment (OS/ separation kernel, middleware, SCA Core Framework)
  - PTF and WF components

Activity 2
A Simple Example

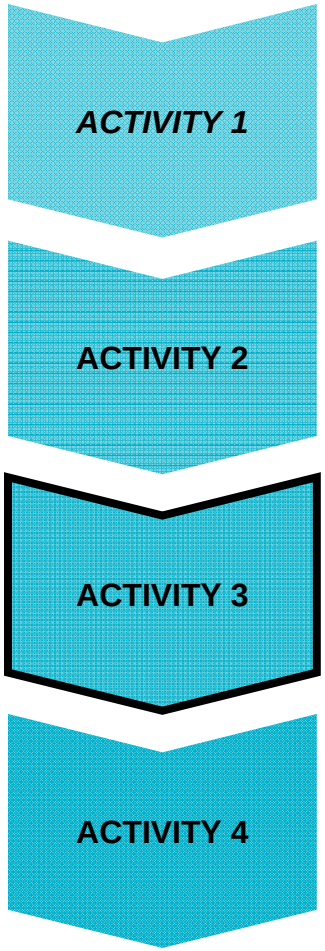
- **Impacts on processors**
  - GPP: separation kernels / hypervisors enable to host different waveforms with independent security levels
  - FPGA: isolation and partial reconfiguration mechanisms enable to host different waveforms with independent security levels
  - DSP: no solution, different DSP for different waveforms



Activity 2 Summary

- Physical and logical separations are possible to ensure MILS application
  - Physical or logical separation for red area
  - Physical separation for CS/S
  - No specific separation is necessary for MILS in black area
- Logical separation is only possible for GPP and FPGA
- Security evaluations are necessary for mechanisms which ensure the independence of waveforms with different security levels
- Downgrading of performances is expected because of the insertion of security mechanisms relative to MILS
- Deployment of SCA CF component in a MILS architecture is a complex topic which deserves further studies

AMIS Study Activities



Identification of candidate architectures

- **Identify possible solutions that could meet MILS characteristics and constraints**
- **Highlight solutions to be applied to an SDR platform in order to satisfy MILS requirements**
- **Provide suggestions and best practices to be adopted when designing an SDR Architecture implementing MILS**

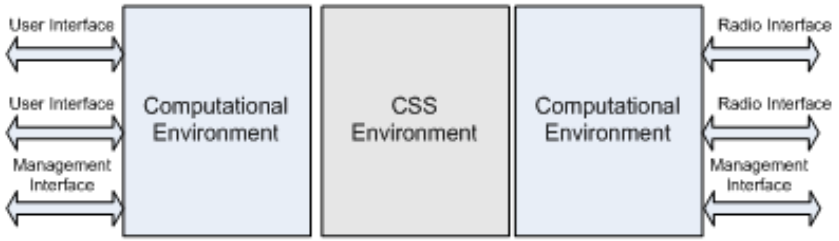
Activity 3
Design Considerations

- WF applications are SCA-allocated to each single channel
- Multiple WF applications are SCA-allocated to the same channel at different periods of time
- Cryptographic capabilities are associated with each single channel
- Specific crypto capabilities are confined in one separated CSS
- Each single channel is associated with one separated Sec Domain
- MILS capabilities in AMIS design solutions result from the combination of separation layouts and technologies encompassing at-the-state-of-the-art hardware and software paradigms
- AMIS design solutions are to undergo a security evaluation process, assessing the overall robustness of MILS capability against some specific criteria

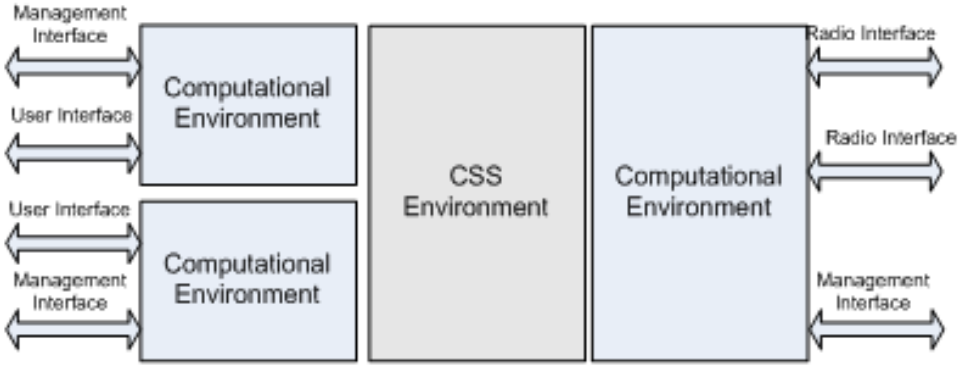
Activity 3
Candidate Architectures

- Single computational environment for single interfaces - SCE4SI

- Single computational environment for multiple interfaces - SCE4MI



- Multiple computational environment for multiple interfaces - MCE4MI



Activity 3
Key Design Drivers / Evaluation Criteria

- Form factor (PRR, Handheld, Manpack, Vehicular)
- SWaP (Size, Weight and Power)
- Estimated Cost
- Complexity
- Scalability
- Security Certification

	Metric = 1	Metric = 2	Metric = 3
Form Factor	Large	Medium	Small
SWaP	Increased	Regular	Reduced
Cost	High	Affordable	Basic
Complexity	High	Moderate	Minimum
Scalability	Difficult	Moderate	Easy
Certification	Large Effort	Moderate Effort	Straightforward

Activity 3
Assessment Table

- For each design a score is assigned based on industrial evaluation

	SCE4SI	SCE4MI	MCE4MI
Form Factor	Small	Medium	Large
SWaP	Reduced	Regular	Increased
Cost	Basic	Affordable	High
Complexity	Minimum	High	Moderate
Scalability	Moderate	Moderate	Moderate
Certification	Straightforward	Large effort	Moderate Effort

Activity 3 Summary

- SCE4SI, SCE4MI and MCE4MI has been collectively identified as "**AMIS design solutions**".
- Evaluation of AMIS design solutions preserve **industrial neutrality** regarding commercial products or existing companies' solutions.
- AMIS Design solutions candidates fit specific **operational contexts and scenarios**
- The intended goal for the involved EU stakeholders **has not been of electing or voting a specific solution**, but simply identifying:
  - drawbacks and advantages for each candidate solutions,
  - functional relationship,
  - scalability properties.

Conclusions (I)

- AMIS has thoroughly analyzed MILS application to SDR
  - "MILS in SDR" problem understanding:
    - **Common Operational Picture**
    - **Security threats**
  - Operational and security requirements well extracted
  - Impact analysis on several SDR subsystems
    - **Hardware**
    - **Operating Environment**
    - **PTF & WF components**
    - **System level impact analysis**
  - Design of candidate solutions for MILS in SDR
  - Evaluation of AMIS candidate architectures

Conclusions (II)

- AMIS provides a **neutral perspective** in the identification and evaluation of AMIS candidate architectures
  - Building blocks categorized according to their functionality or performance
  - No specific vendors' solutions are referred
  - The study proposed an evaluation methodology to measure and score candidate solutions
  - No "golden solution" is proposed
    - **Benefits and drawbacks of each AMIS candidate solution are detected**
    - **Recommendations depending on the operational context are given**

Conclusions (III)

- **AMIS constitute a new reference basis** for future implementations of MILS in EU SDR systems, providing both guidelines and recommendations
- However, **AMIS can be only considered the 1st step of the R&D EU roadmap** for a commonly agreed implementation of MILS capabilities in SDR systems.
- Future challenges:
  - **Framework for cooperation between EDA, national MoDs and NSAs** to provide a consolidated and agreed specification of the operational and security requirements for EU military MILS-capable SDRs, starting from AMIS results and supported when needed by the SDR industrial players
  - To reach an **alignment between AMIS output and European SDR reference architectures** defined by the on-going programs, such as ESSOR or SVFuA
  - To **analyze possible waveform combinations** deployed on MILS-capable SDRs to work on different operational scenarios
  - To **exercise and validate AMIS candidate designs** by means of SDR prototypes, controlled test-beds or on-field trials

Questions?