Effective Security Engineering for the Ground Segment

GSAW 2017
Daniel Fischer, Mariella Spada

14/03/2017
Information Security: A Strategic Objective

- ESA is responsible for assets of very high tangible and intangible value
- Information security has emerged as a strategic objective for ESA
  - Stringent security requirements, mainly due to safety and/or dual aspects (Galileo, Copernicus, SSA..)
  - Changing Security Environment

- Strong executive commitment by ESA towards information security
- Agency level endorsement of security engineering practices
  - Enforced top level security policies in the form of regulations and directives
  - Management commitment to improving security practice throughout the Agency at all levels
  - Moving towards security certification
Ground Segment Systems Engineering

- Mission Requirements
- Mission Integration

Ground Segment Systems Engineering

Subsystem Engineering
Systems Engineering Processes

- Requirements Engineering
- Design
- Implementation
- Testing
- Deployment & Operations
- Maintenance

Information Security?
Secure System Engineering Focus

Requirements Engineering
Design
Implementation
Testing
Deployment & Operations
Maintenance

Requirements Engineering Framework
Requirements Catalogue
Penetration Testing
Code Scanning
Risk Assessment Integration
Security Requirements Engineering

Mission Higher Level Security Requirements

Security Strength
Environment Specification

Security Requirements Engineering Framework

Engineer

Penetration Testing
Code Scanning
Risk Assessment Integration

Security Requirements
- Functional
- Assurance
- Documentation
- Contractual

NIST, ISO, Etc.

Security Requirements Catalogue
Requirement Templates Repository

ESA UNCLASSIFIED - Releasable to the Public
Security Requirements Engineering Framework

GASF Tool

Template A

Template B

Project view

Export

DOORS

Compute recommendations

Requirement Catalogue

ESA UNCLASSIFIED - Releasable to the Public
Security Validation and Testing

Static Tools

Pentesting Tools

Fully Representative Ground Segment Environment

Requirements Catalogue

Requirements Engineering Framework

Risk Assessment Integration

Certification
Risk Assessment Integration Tools

Engineer Stakeholder

Risk Assessment Integration Tools

Risks Register Engineering Tools

Risk Assessment Methodologies Threat & Vulnerability Databases

Agency Level Risks Sub System Level Risks

Requirements Engineering Framework Penetration Testing Code Scanning

Risk Assessment Methodologies

ESA UNCLASSIFIED - Releasable to the Public
The Future of Ground Segment Security Engineering

- Development of an overall security system engineering framework
  - Complete integration of the individual elements into one framework
  - Provision of engineering and exploitation interfaces with the system models

- Modular design of security engineering processes
  - Objective: Integration into the model-centric ground segment engineering approach
  - Data to be integrated into the engineering model
    - Security Requirements
    - Risk Assessment Information
    - Security validation and testing information
Thank You very much for your attention!

Effective Security Engineering for the Ground Segment
D. Fischer, M. Spada

Any questions?