55th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cybersecurity in space systems, risks and countermeasures (4)

Author: Mr. Marcus Wallum
ESA - European Space Agency, Germany

Dr. Daniel Fischer
European Space Agency (ESA), Germany
Mr. Matteo Merialdo
RHEA System B.V., Italy
Mr. Danilo Ingami
Rhea Group, Italy
Mr. Peter Hagström
Rhea for ESA, Belgium
Mrs. Gabriela Mihalachi
Rhea System S.A., Italy

SECURE SYSTEMS ENGINEERING FRAMEWORK FOR SPACE MISSIONS

Abstract

Space systems and the data, products and services they provide are increasingly relied upon for supporting critical infrastructures and services, communication, scientific study, exploration, policy and decision making. This increased reliance of society on space assets also increases their attractiveness as targets for adversaries. Together with lower entry barriers, increasing complexity and tight coupling between space and terrestrial-based systems, it is apparent that the effective management of security of space systems has never been more important.

Standardisation bodies have developed comprehensive generic and industry-specific standards to aid the implementation, management and assurance of security for information systems. Today there is no similarly generic approach to support secure system engineering processes for space systems. This gap is especially problematic for civilian and unclassified space missions, which may lack an imposed Program Security Instruction or adequate security-dedicated expertise or budget.

There is therefore a pressing need to analyse and evolve space system engineering, quality and management standards, which govern and guide the development of space systems to account for security aspects throughout the System Development LifeCycle (SDLC). In order to realise an efficient and effective application of the revised approach, the development of a framework of supporting methodologies, tools, and datasets is necessary. This paper introduces the Secure Systems Engineering for Space Missions (SSE4S) Framework currently under development at the European Space Agency (ESA). The framework builds upon and extends existing standards and software and consists of the following components:

- Methodology – guided SSE processes embedded in the SDLC, integrated in particular with existing and to-be-revised European Cooperation for Space Standardization (ECSS) standards.
- Vocabulary / Data model – formal definition of any entity used within the framework, supporting a digital engineering approach and integration with the Model Based System Engineering paradigm.
- Data – Reusable constructs and information, including catalogues of security requirements and controls and associated profiles adapted to specific contexts (e.g. mission, system, organisational),

repeatable assurance cases for certification or accreditation and space system specific threat and vulnerability taxonomies.

- Tools – software to form a complete capability to implement the framework. Tooling shall support the Security Threat and Risk Assessment, Security Requirements Engineering, Security Testing and Security Certification and Accreditation processes, providing workflows across all and utilising automation wherever possible.
- Products – Templates for generated documents and reports (e.g. System Security Requirements Statements, Security Operating Procedures, Risk Assessments, Residual Risks, test reports).