SSE4SPACE

Secure Systems Engineering for Space Missions

Final Presentation

SSE4SPACE

RHEA GROUP

WMG THE UNIVERSITY OF WARWICK

GREY CONSULTANTS

OHB

«DigitalEngineering» DEKonsult

SSE4SPACE
Secure Systems Engineering for Space Missions

Consortium

RHEA GROUP

- Strong background in space, security and system engineering
- Project coordination, Requirement specification, software development and risk-assessment methodology

«DigitalEngineering» DEKonsult

- Focus on computer aided design, analysis and simulation in all its forms, the digital transformation and its infusion, aiming for effective and efficient multi-disciplinary, concurrent, model-based engineering of complex systems.
- Contributes expertise knowledge on ontologies and data modelling

WMG THE UNIVERSITY OF WARWICK

- Relevant experience and expertise in the domain of industrial best practices in secure system and software engineering relevant to all critical infrastructure sectors
- Contributes on gap analysis and process/methodology definition

GREY CONSULTANTS

- Hands-on experience in the application of systems and security engineering practices to the space sector s across the entire mission lifecycle
- Contributes to the user-requirements as well as to the future roadmap

OHB

- Specializes in the development and integration of space systems and satellites.
- Contributes with the unique industry perspective and responsible for the SSE4Space validation.

Importance of Secure System Engineering

SSE4SPACE Secure Systems Engineering for Space Missions

Reliance on space assets

- For terrestrial services such as communication and navigation
- Environmental and Research

Increased attractiveness as target for adversaries

- Dependence on space systems, high impacts
- Long life-cycles
- SDR and cheap equipment for adversaries

Changing landscape, new private actors and declining lowered barriers to access space

- Price has dropped 95% over a short period, were some say cost will be <100$/Kg within 2023.

Cost increases when security is an after thought

Need to evolve space system engineering,

Challenges in Secure System Engineering

Space Systems are complex

- Highly dependent on context
- Component interdependencies
- Multiple stakeholders involved
- Need to link the system engineering practices (such as MBSE) to the security engineering.

System Driven / Component Driven

- Prevailing methodologies component-driven
- Often neglects broader system-level view

Reuse and Interoperability

Need to consider operational risks

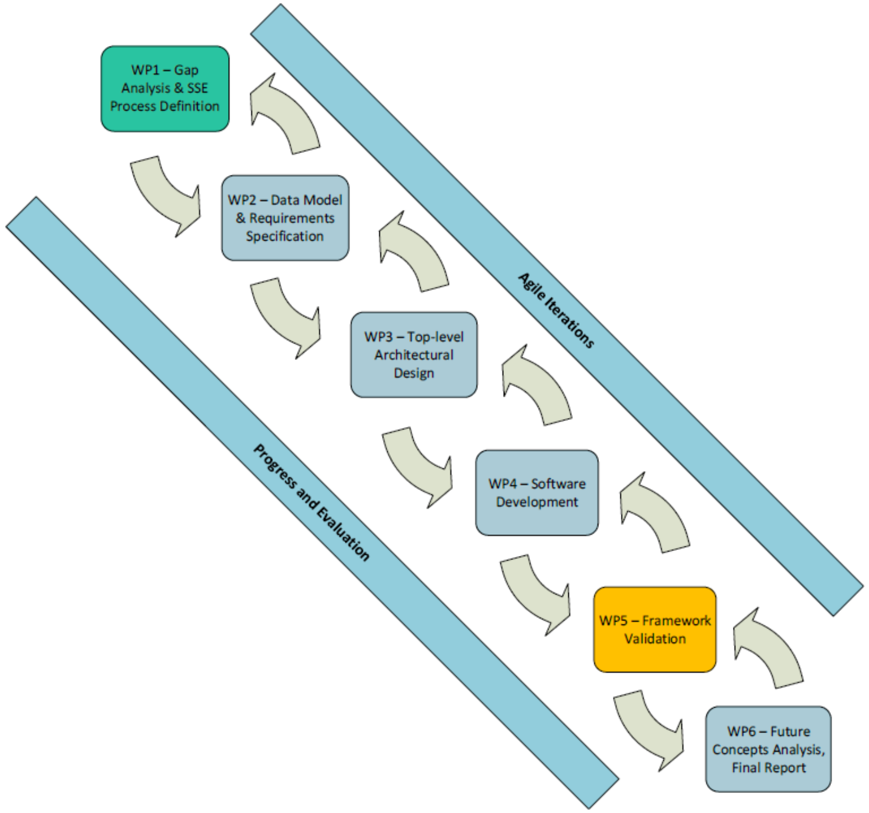
SSE4SPACE
Secure Systems Engineering for Space Missions

Work Package - Overview

1. Gap Analysis and Process Definition
2. Data model & Requirements Specification
3. Top Level Architectural Design
4. Software Development
5. Framework Validation
6. Future Concepts

Characterized by an agile methodology

- Short 2-week sprints
- High engagement from end-users


WP1 – Gap Analysis & SSE Process Definition
WP2 – Data Model & Requirements Specification
WP3 – Top-level Architectural Design
WP4 – Software Development
WP5 – Framework Validation
WP6 – Future Concepts Analysis, Final Report
Agile Iterations
Progress and Evaluation

RHEA GROUP · WMG THE UNIVERSITY OF WARWICK · GREY CONSULTANTS · OHB · «DigitalEngineering» DEKonsult

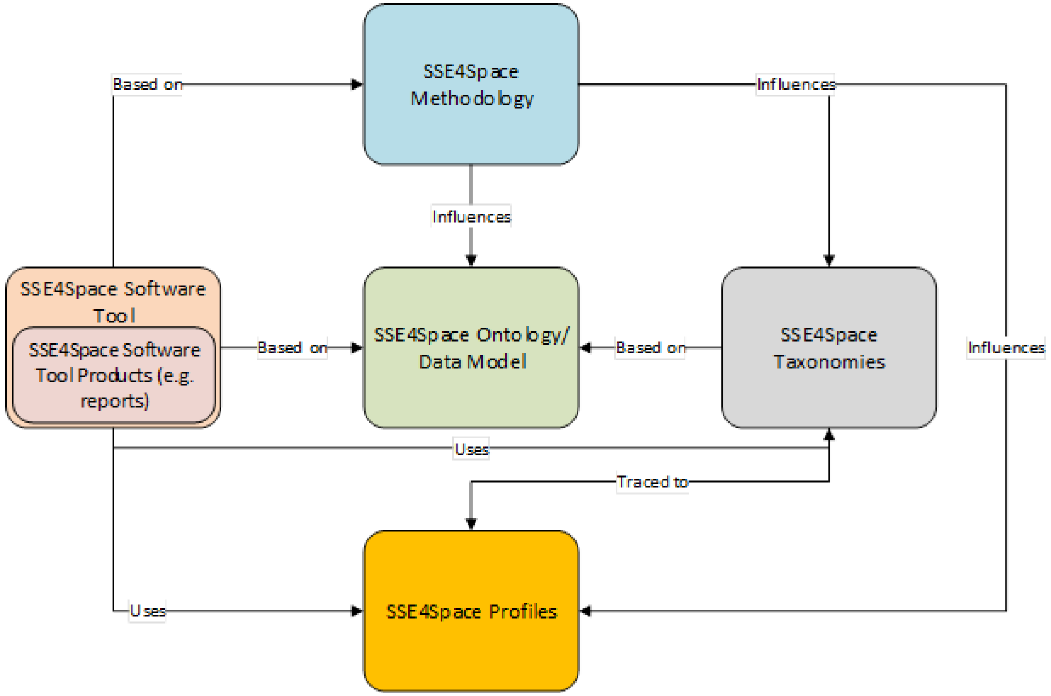
ESA UNCLASSIFIED – RELEASABLE TO THE PUBLIC

The SSE4Space Framework – Overview

Definition of the SSE4Space Methodology

Data model and Ontology

Software design and Implementation



SSE4Space Methodology

Comprehensive Methodology

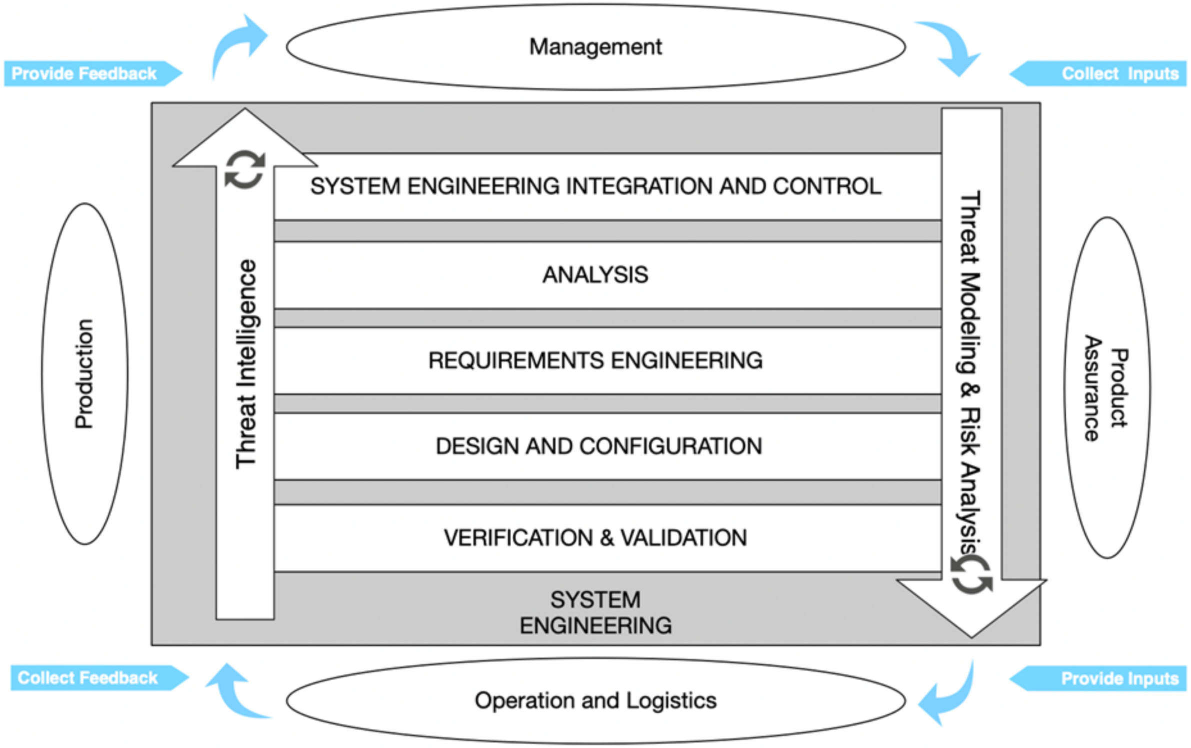
- Follows the entire life-cycle
- System driven and component driven (Top-down, bottom-up)
- Identification, Assessment, Treatment, Security Requirement Management,
- Supporting the Certification & Verification

Industry best practices

- MITRE Catalogue (CWE, CVE, CAPEC, ATT&CK)
- Custom catalogues (For instance SPACE-SHIELD)
- NIST 800-53

Draws upon established risk management frameworks

- NIST 800-30
- ISO27005



ESA UNCLASSIFIED – RELEASABLE TO THE PUBLIC

SSE4Space Data model

Glossary of Terms

- Central repository for clear definitions and standardized terminology
- Comprehensive collection with over 1300 specific terms.

Reusable Data Constructs

- Structured using the UML2 framework for consistency and integration
- Facilitates interoperability and modular design

Taxonomy/Ontology

- Defines a clear hierarchy of types, inheritance and interrelations
- Supports logical data structuring and complex system modelling

SSE4Space Software Solution

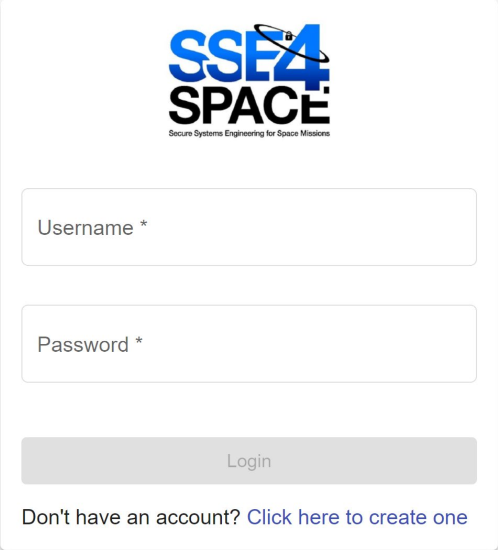
Software to implement the methodology

Catalogue management, threats, mitigations, controls …

Multi-phases and iteration

Multi-user and shared responsibilities

Sharing interfaces through HSICD and custom JSON data-format.



Don't have an account? Click here to create one

Demonstration

Gabriela to present the features of the software

Validation Demonstration

HERA is part of the Asteroid Impact & Deflection Assessment (AIDA) programme which is based on the synergy between DART and HERA missions:

- DART: Double Asteroid Redirection Test, is a Kinetic impactor to demonstrate deflection of asteroids
- HERA: Monitoring mission arriving after DART impact.

Validation Demonstration

The key mission goal of HERA is to take high resolution images of the crater made by DART.

Other high level mission objectives of HERA are:

- Increasing our understanding of how we can deflect asteroids in the future.
- Traveling to an asteroid after NASA's DART mission has flown there and impacted with it.
- Further explore the Solar System, investigating the smallest asteroid and the first binary-asteroid system ever visited.
- Using different instruments to discover more about asteroids.
- Investigating new techniques and technology for activities in deep space as autonomous proximity operations.

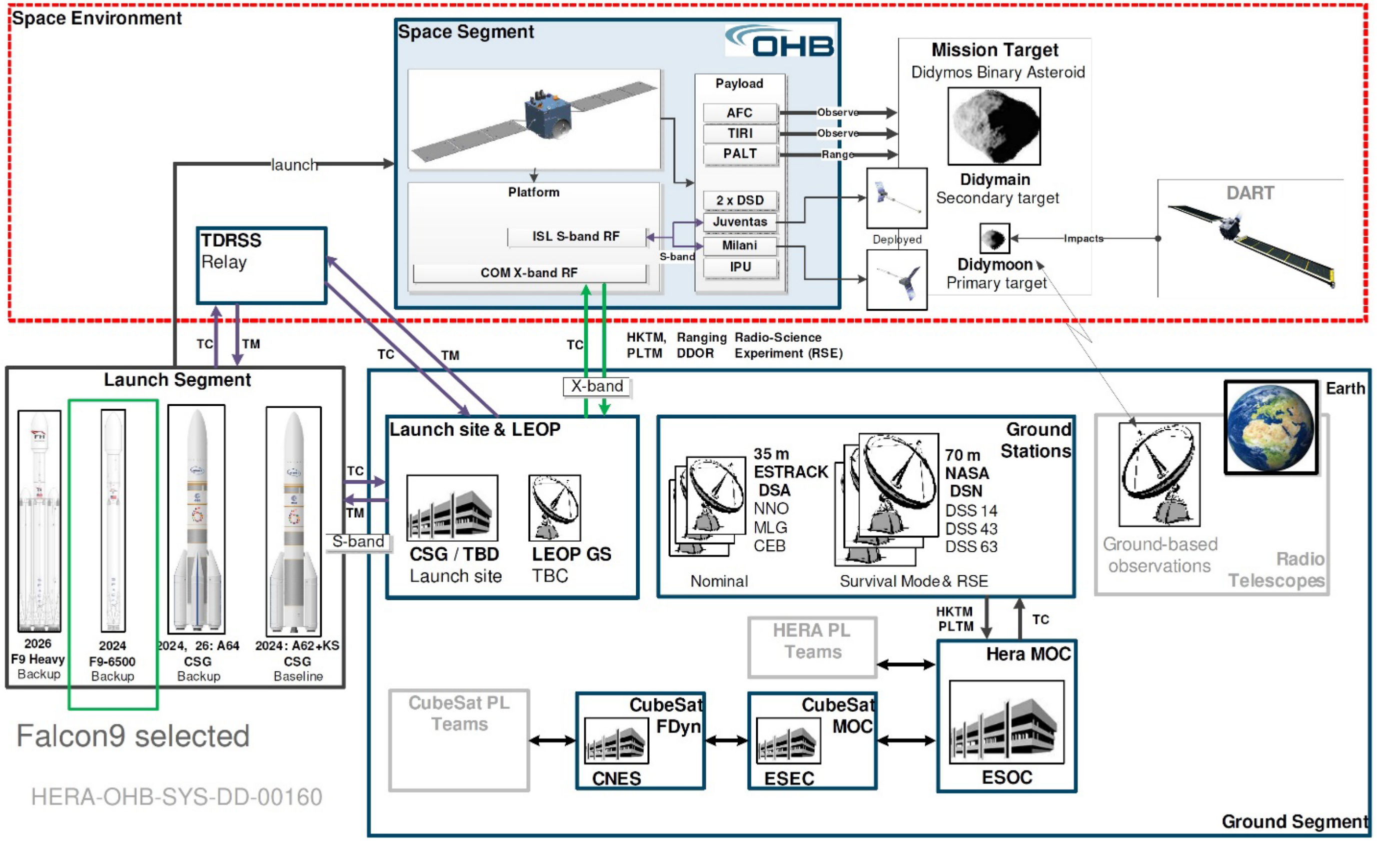
Validation Demonstration

The HERA space segment is composed by:

- The HERA spacecraft and payload
- The cubesat: “Juventas”
- The cubesat “Milani”

HERA ground segment is made of:

- The ESATRACK DSA (35 m antenna, for nominal operations) and NASA DSN (70 m antenna for survival mode) ground stations
- The HERA Mission Operations Center (MOC) in ESOC
- The cubesat MOC in ESEC
- The cubesat Flight Dynamic team in CNES



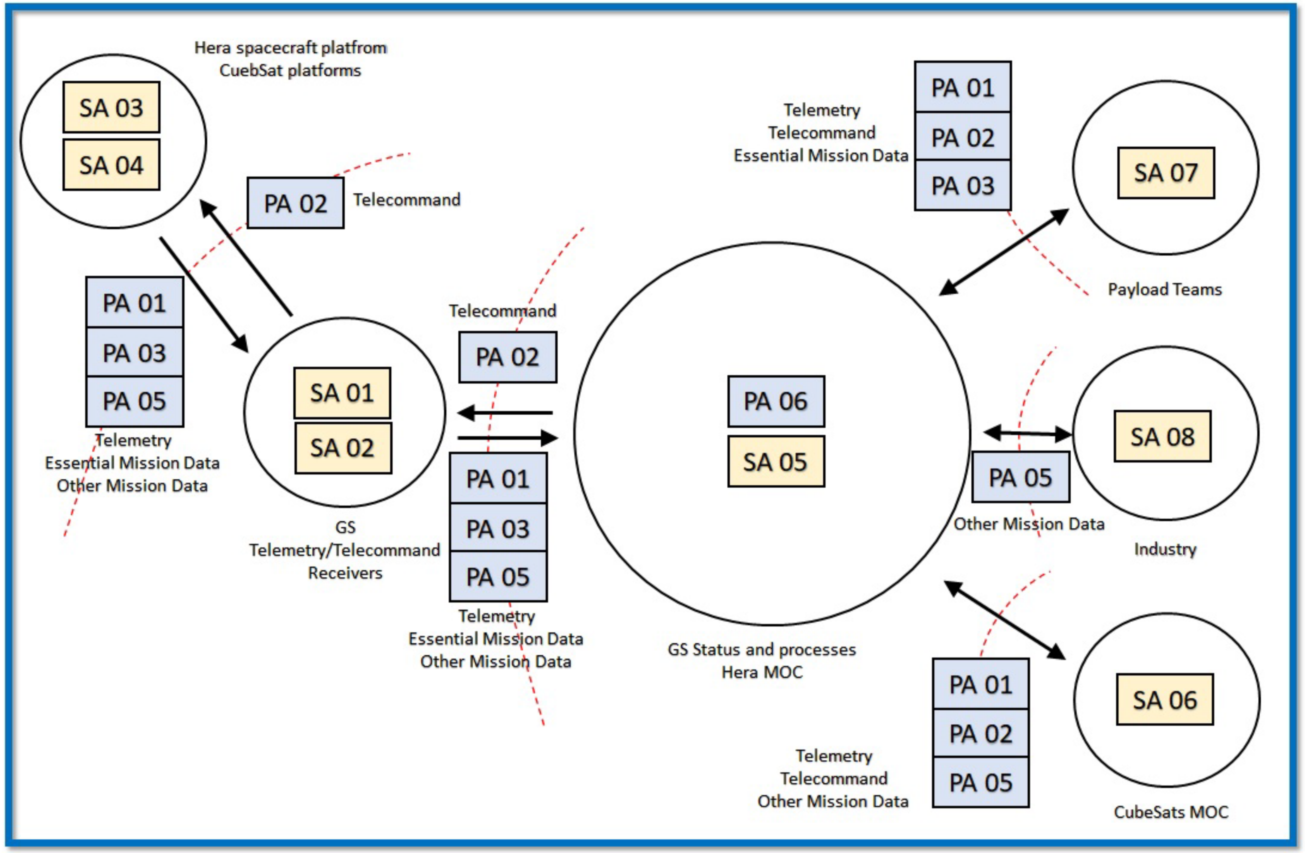
RHEA GROUP   WMG THE UNIVERSITY OF WARWICK   GREY CONSULTANTS   OHB   «DigitalEngineering» DEKonsult

Validation Demonstration

- The validation of the SSE4Space tool uses the HERA mission and utilizes data from project documents and the High Level Risk Assessment (HLRA) document
- The three mission phases A, B and C are examined and various Targets of Evaluation (TOE) are created and analyzed
- The TOEs cover the ground segment and the space segment

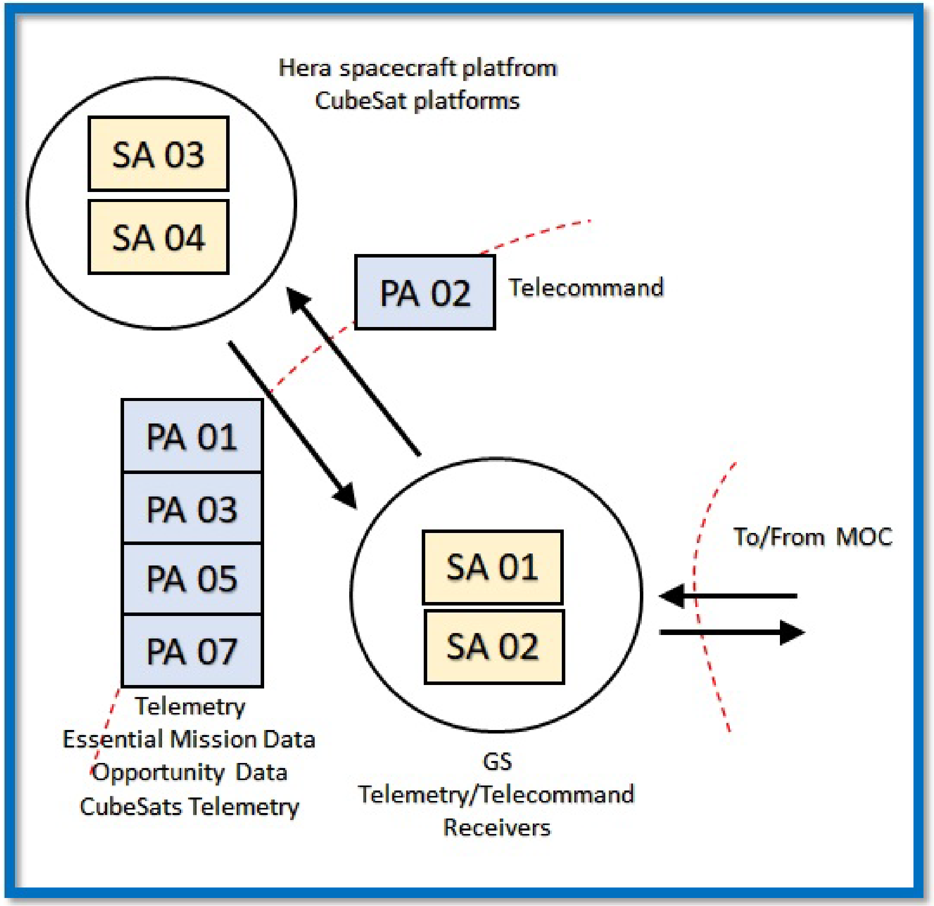
Validation Demonstration

TOE 01: HERA Overall System



Validation Demonstration

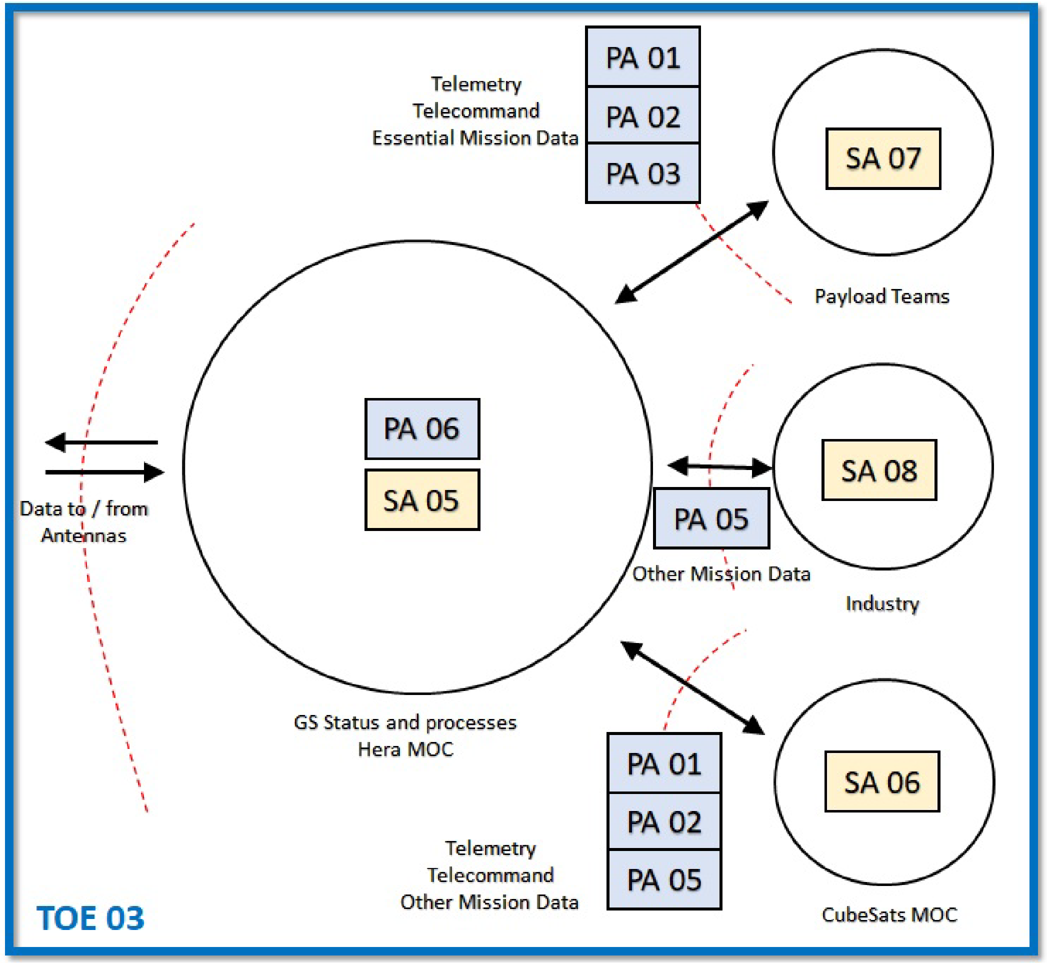
TOE 02: HERA Space platform



TOE 02

Validation Demonstration

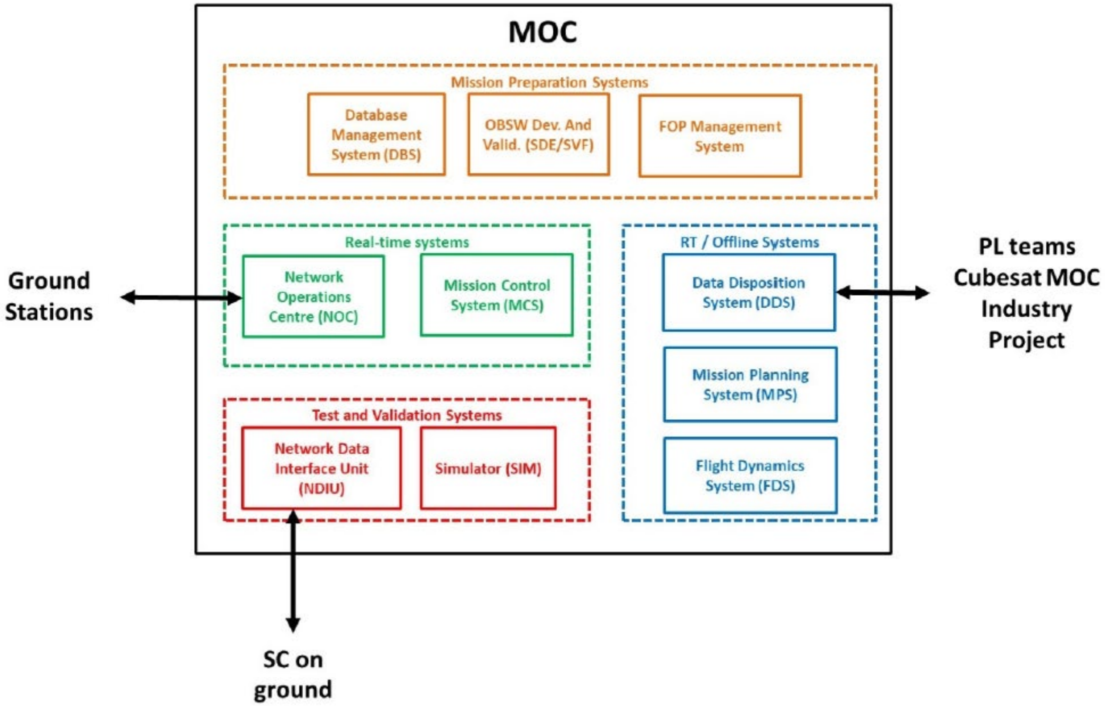
TOE 03: HERA MOC and connected facilities



ESA UNCLASSIFIED – RELEASABLE TO THE PUBLIC

Validation Demonstration

TOE 04: Flight Operations Management System



MOC

Mission Preparation Systems

Database Management System (DBS)

OBSW Dev. And Valid. (SDE/SVF)

FOP Management System

Real-time systems

Network Operations Centre (NOC)

Mission Control System (MCS)

RT / Offline Systems

Data Disposition System (DDS)

Mission Planning System (MPS)

Flight Dynamics System (FDS)

Test and Validation Systems

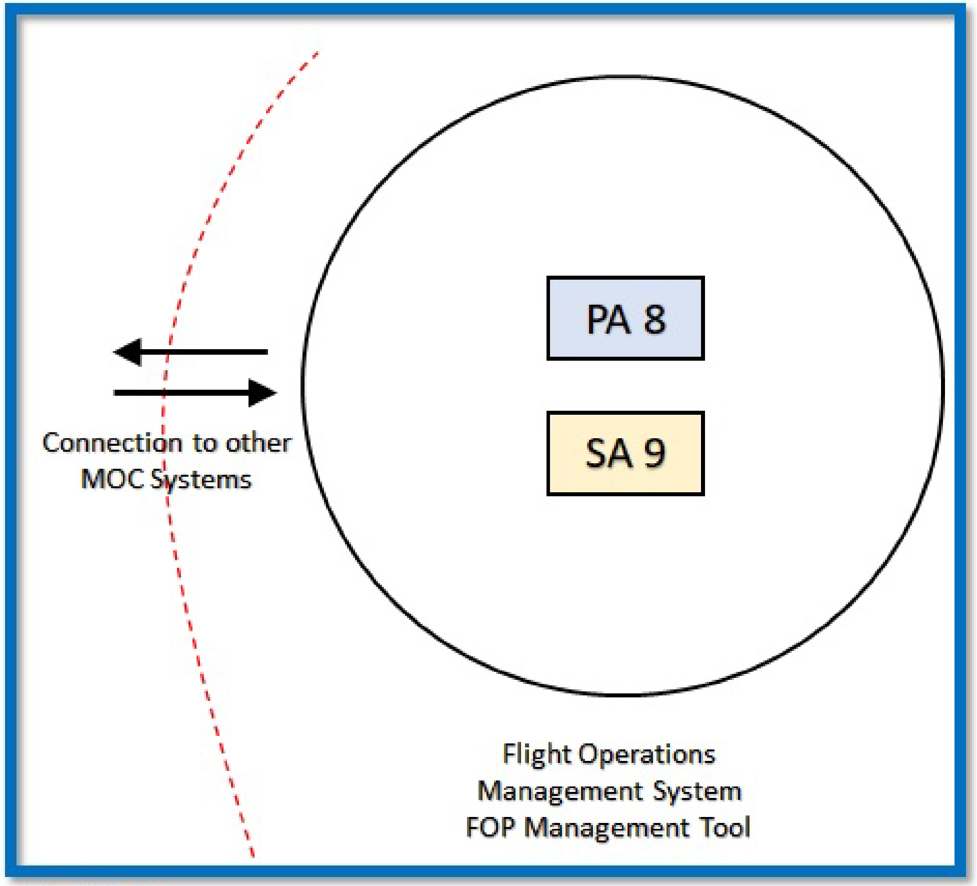
Network Data Interface Unit (NDIU)

Simulator (SIM)

Ground Stations

PL teams Cubesat MOC Industry Project

SC on ground



PA 8

SA 9

Connection to other MOC Systems

Flight Operations Management System FOP Management Tool

TOE 04

Gap analysis

External Standards to ECSS Standards

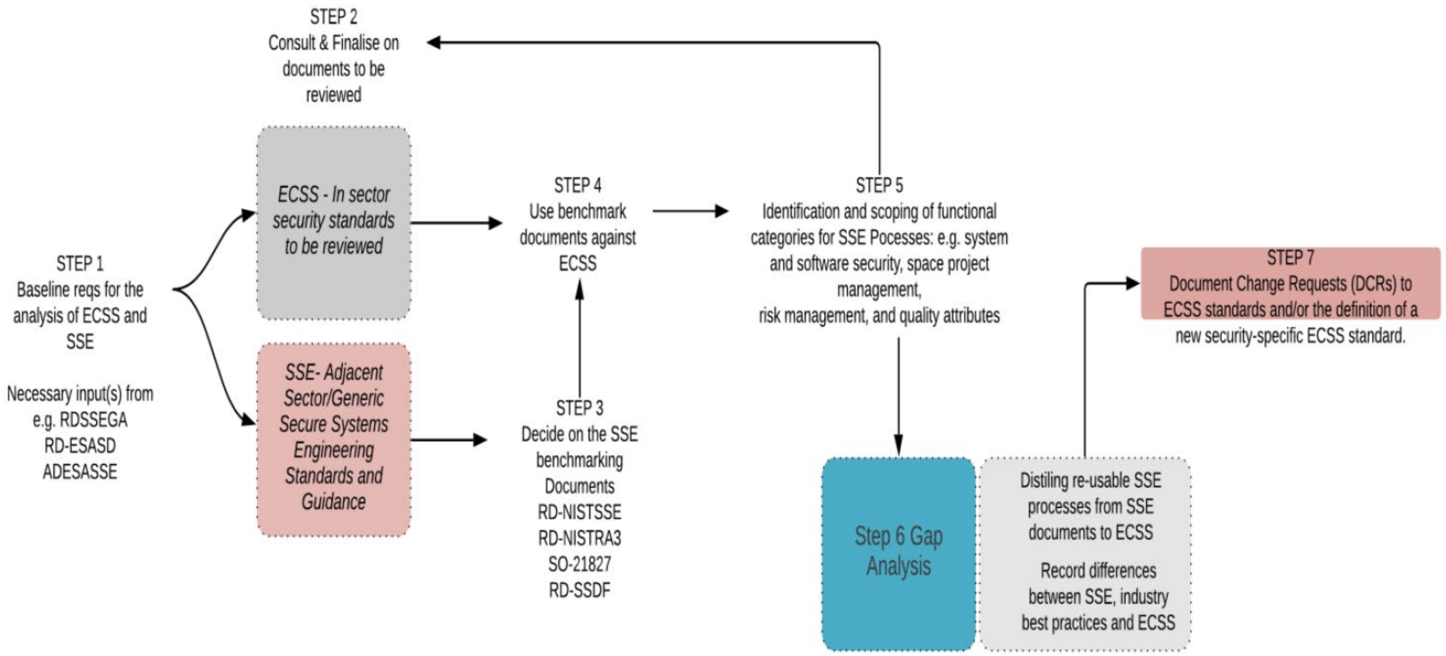
- Study reviewed 14 external standards
- From these, 10 were selected to be mapped against existing ECSS standards

Identifying Gaps

- Where ECSS does not fully cover Secure System Engineering
- Understand the lack or need of enhancements

Methodology

1. Identification of baseline requirements
2. Finalization on documents to be reviewed
3. Confirm SSE benchmark documents
4. Confirm in-sector standards
5. Functional Categories for SSE process
6. Perform Gap analysis
7. Document Change Requests



STEP 1
Baseline reqs for the analysis of ECSS and SSE

Necessary input(s) from e.g. RDSSEGA
RD-ESASD
ADESASSE

STEP 2
Consult & Finalise on documents to be reviewed

ECSS - In sector security standards to be reviewed

SSE- Adjacent Sector/Generic Secure Systems Engineering Standards and Guidance

STEP 3
Decide on the SSE benchmarking Documents
RD-NISTSSE
RD-NISTRA3
SO-21827
RD-SSDF

STEP 4
Use benchmark documents against ECSS

STEP 5
Identification and scoping of functional categories for SSE Pocesses: e.g. system and software security, space project management,
risk management, and quality attributes

Step 6 Gap Analysis

Distiling re-usable SSE processes from SSE documents to ECSS

Record differences between SSE, industry best practices and ECSS

STEP 7
Document Change Requests (DCRs) to ECSS standards and/or the definition of a new security-specific ECSS standard.

Categories for SSE Process

To aid mapping, some ECSS standards were only mapped against the engineering domains of interest

To ensure that the SSE processes were covered as fully as possible, and that the relevant standards were matched to their ECSS counterparts the cross mapping

ID PROCESS	ID PROCESS
AQ Acquisition	MS Measurement
AR Architecture Definition	OP Operation
BA Business or Mission Analysis	PA Project Assessment and Control
CM Configuration Management	PL Project Planning
DE Design Definition	PM Portfolio Management
DM Decision Management	QA Quality Assurance
DS Disposal	QM Quality Management
HR Human Resource Management	RM Risk Management
IF Infrastructure Management	SA System Analysis
IM Information Management	SN Stakeholder Needs and Requirements Definition
IN Integration	SP Supply
IP Implementation	SR System Requirements Definition
KM Knowledge Management	TR Transition
LM Life Cycle Model Management	VA Validation
MA Maintenance	VE Verification

Standards

Standard	Number of Mappable Controls	Number (%) of controls Mapped	Number (%) of controls Not Mapped
ISO 27001	52	29(55%)	23(44%)
ISO 27005	25	19(76%)	6(24%)
NIST 800-160 Vol 1	563	481 (85%)	82 (15%)
NIST 800-160 Vol2 Resilience	230	227 (99%)	3 (1%)
NIST 800-37R2	47	43 (91%)	4 (9%)
ISO 21827	130	117 (90%)	13 (10%)
NIST SSDF	37	33 (89%)	4 (11%)
Microsoft Trustworthy SDLC	90	77 (86%)	13 (14%)
CCSDS 350.7 Mission Planners Guide	162	153 (94%)	9 (6%)
OWASP SAMM	71	53 (75%)	18 (25%)
Total	1,407	1241(88%)	175(12%)

SSE4SPACE

Secure Systems Engineering for Space Missions

Key findings

Gaps within ECSS

Mapping Rate and Identified Gaps:

- Over 84% from standards were mapped to ECSS
- Significant Gaps were identified in Decision Management and Knowledge Management
- The Largest number of gaps were concentrated in the area of Risk Management and Security Operations Procedures.

Most impactful Framework

- NIST 800-160 System Engineering standard was identified as the framework producing most systems control gaps

Document Change Requests

- As a result of the gap mapping exercise, outline document change requests have been formulated to assist the incorporation of the required documentation changes for ECSS standards (179 DCRs)

RHEA GROUP

WMG THE UNIVERSITY OF WARWICK

GREY CONSULTANTS

OHB

«DigitalEngineering» DEKonsult

Recommendations

1. Develop strategies that specifically relate to knowledge management and decision management.

2. Define secure system engineering management activities to be included in systems engineering management planning. A closer definition of the levels of risk management, analysis, assessment, and treatment is required to accurately cover the Risk Management landscape.

3. Derivation of security assurance and security strength of function requirements to empower the development of resilient protection strategies and capabilities.

4. Incorporate architecture into security design activities (high-level design, detailed design) and development to give guidance on the selection of solution classes and provide reference architectures or blueprints.

5. Adopt a process to encompass security verification and validation activities.

6. Utilise the products, processes and review points identified as input to the novel SSE process.

7. Develop the system security engineering process guidance to provide process and lifecycle orchestration and enhance the pr oduction of adaptive security systems.

Methodology

PETER HAGSTROM

Development of a novel SSE-methodology

Comprehensive Approach

Developed as an augmentation of ongoing Security Initiatives

Aims to deliver SSE practices for space mission capabilities

Fundamental Processes

Threat modelling and vulnerability identification

Security Risk Assessment in business context

Analysis and management of security requirements

Support the Testing, verification, approval and accreditation processes

High-level schematic integration

Align with ECSS engineering process and integrate Risk Analysis across all lifecycle phases

Incorporate threat intelligence from operational to enhance system engineering

Balance system and component perspectives

Merge system-driven and component-driven risk analysis for holistic view

ESA UNCLASSIFIED – RELEASABLE TO THE PUBLIC

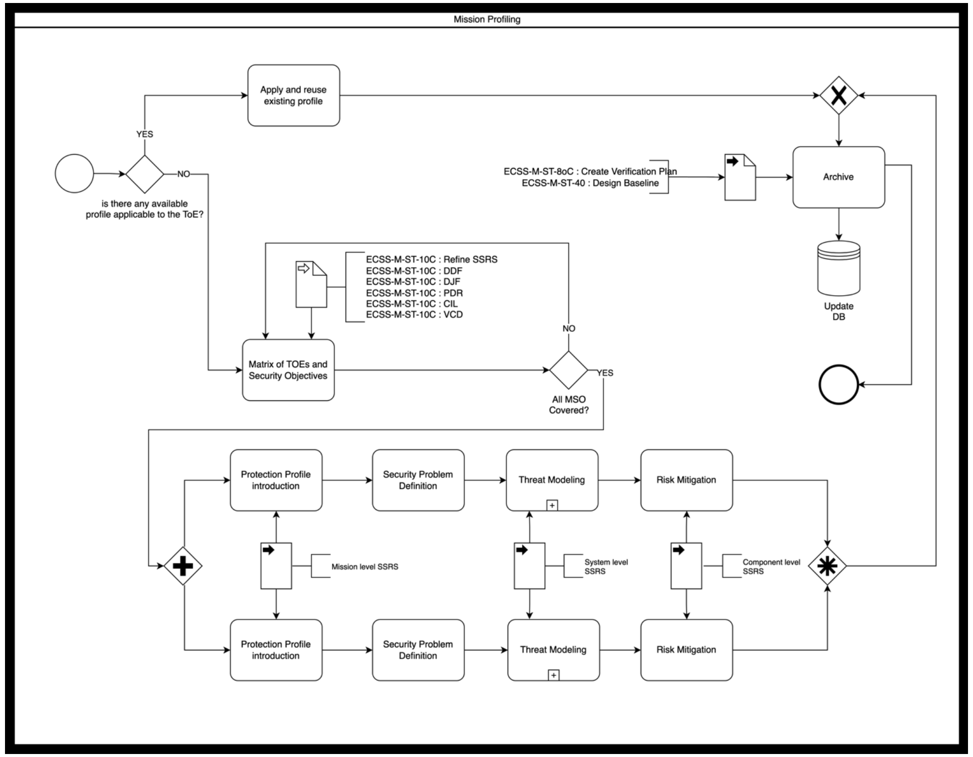
Definition of BPMN

The SSE4Space intersects with ECSS engineering

- Risk analysis
- Threat modelling
- Integrating threat information

Business process

- Activities
- Inputs and Outputs



Mission Profiling
Apply and reuse existing profile
YES
NO
is there any available profile applicable to the ToE?
ECSS-M-ST-8oC : Create Verification Plan
ECSS-M-ST-40 : Design Baseline
Archive
Update DB
ECSS-M-ST-10C : Refine SSRS
ECSS-M-ST-10C : DDF
ECSS-M-ST-10C : DJF
ECSS-M-ST-10C : PDR
ECSS-M-ST-10C : CIL
ECSS-M-ST-10C : VCD
NO
Matrix of TOEs and Security Objectives
YES
All MSO Covered?
Protection Profile introduction
Security Problem Definition
Threat Modeling
Risk Mitigation
Mission level SSRS
System level SSRS
Component level SSRS
Protection Profile introduction
Security Problem Definition
Threat Modeling
Risk Mitigation

SSE4Space - methodology for SSE

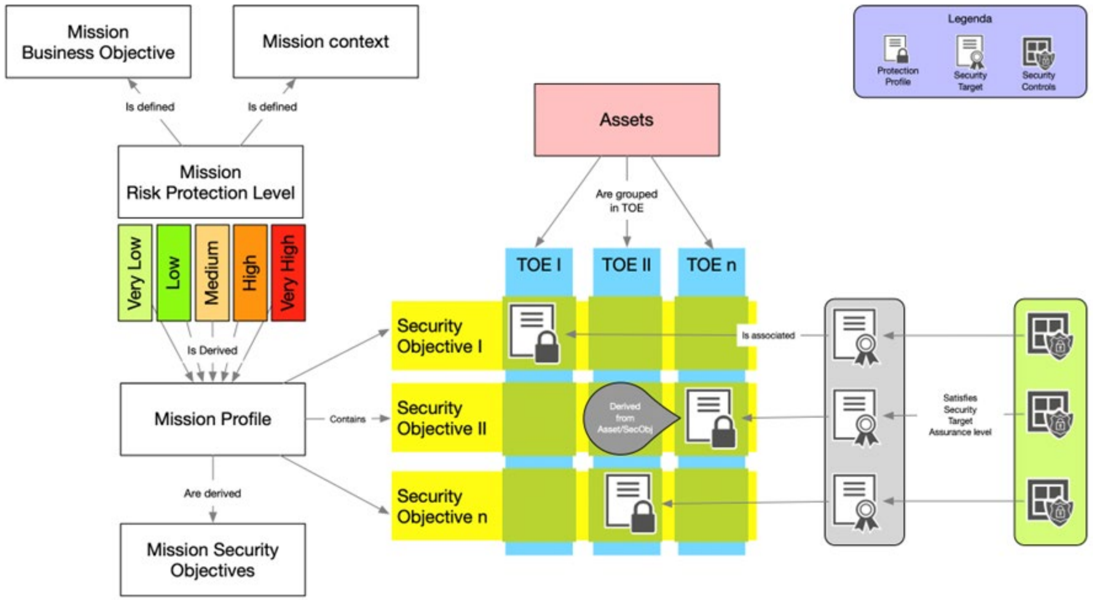
Integrate with the SDLC - From the initial phase to decommissioning

System (de)composition

Threat-Modelling

Risk Calculation based on OWASP - Risk Rating Methodology

Incorporates catalogues such as CWE, CVE, MITRE ATT&CK, SPACE-SHIELD, NIST-800-30



General process

Context Establishment

- Business Objectives and Security Objectives
- Mission Risk Protection Level

Mission Profiling

- Identify and decompose into ToE
- Vulnerability Assessment
- Protection profiles

Threat Modelling

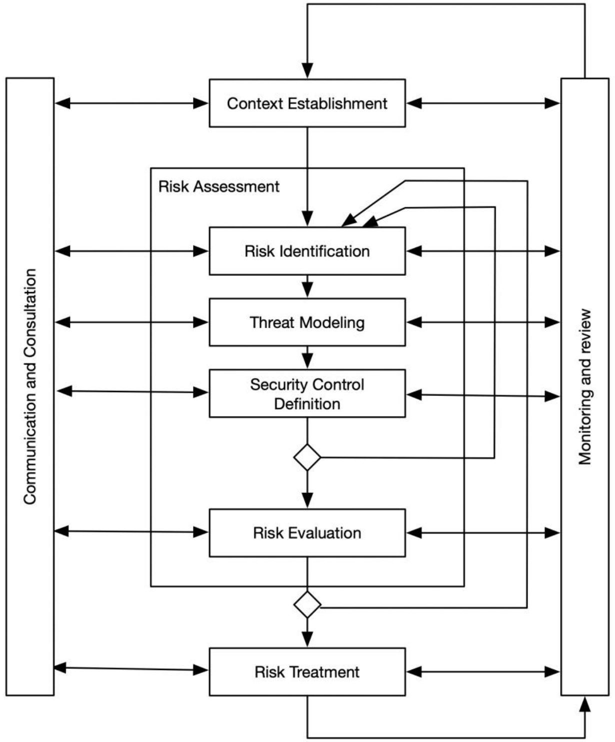
- Identify actors, scenarios and attack paths

Security Target

- Identification of Requirements and Controls

Risk Evaluation

Certification And Accreditation



Context Establishment

Mission Context:

- Description and general characteristics of a mission
- Mission Phase
- Impact Scales
- Business Objectives

Mission Classification

- Security Objectives
- Mission Risk Protection Level

Mission Profiling

Identify ToE

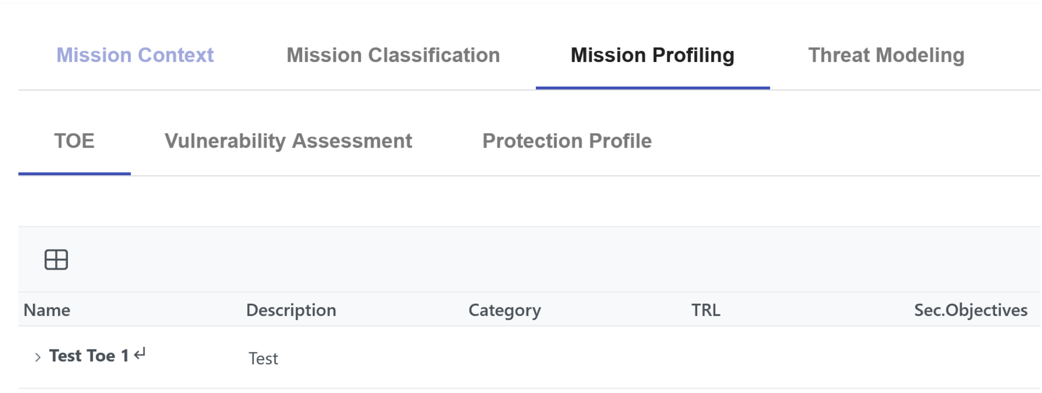
- Decompose System into separate Target of Evaluation
- Relations between assets and the entire system composition

Vulnerability Assessment

- Identify vulnerabilities within ToEs (for instance from CWE catalogue)

Protection Profile

- Express the security problem
- Link ToE with Security Objectives
- Define Protection Level
- Analyze threats, attack vectors, TTPs and mitigation domains



Name	Description	Category	TRL	Sec.Objectives
› Test Toe 1 ↵	Test			

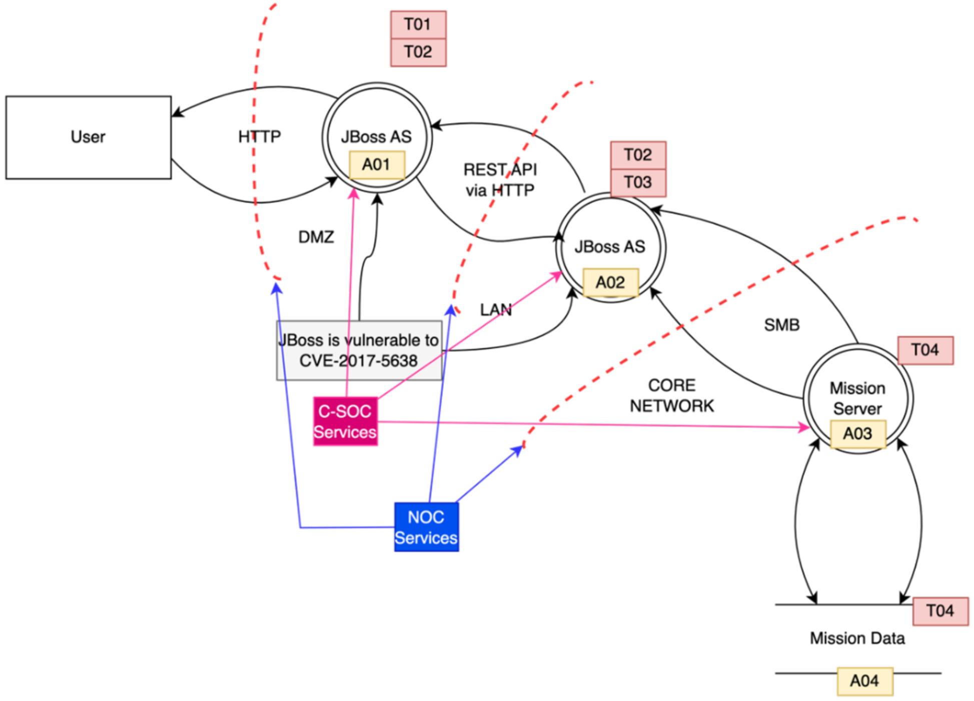
Threat Modelling

Adopt attacker point of view per ToE

- Structured approach to identify threats
- Understand how an attacker can compromise our system

Threat Scenarios

- Threat vectors, either new or from Protection Profile
- Specify attack steps
- Propose mitigations
- Risk determination using OWASP-risk rating



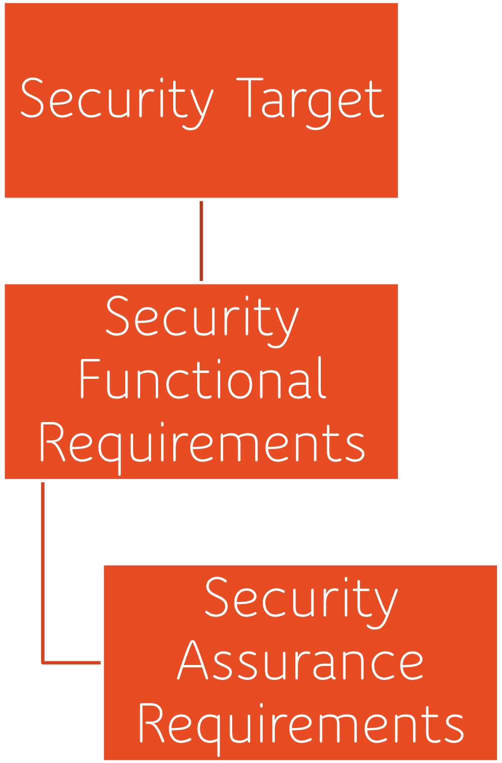
Security Target

Identification of requirements in response to threat scenarios

- Security Functional Requirements (SFR)
- Assurance Requirements (SAR)

Import of SecOps from SCCoE SVF

Assessment of the Residual Risk



Security Target

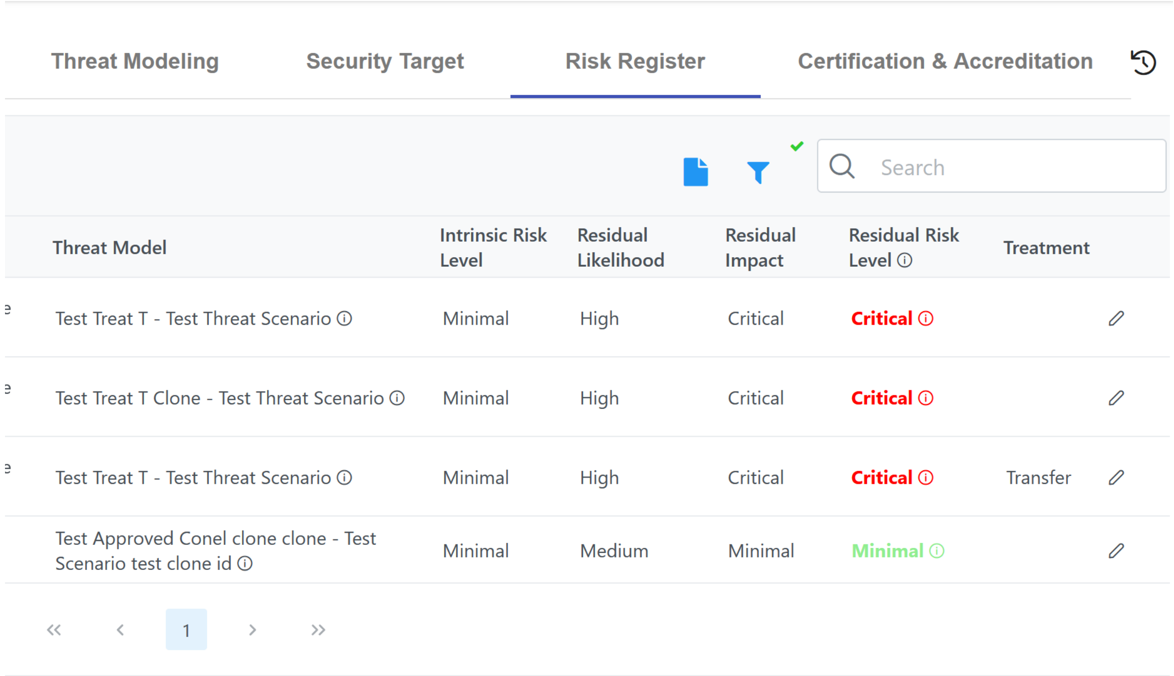
Security Functional Requirements

Security Assurance Requirements

Risk Evaluation

Overview of all threat scenarios

- Intrinsic and Residual Risks Levels
- Treatment plan



Threat Model	Intrinsic Risk Level	Residual Likelihood	Residual Impact	Residual Risk Level ⓘ	Treatment
Test Treat T - Test Threat Scenario ⓘ	Minimal	High	Critical	Critical ⓘ	
Test Treat T Clone - Test Threat Scenario ⓘ	Minimal	High	Critical	Critical ⓘ	
Test Treat T - Test Threat Scenario ⓘ	Minimal	High	Critical	Critical ⓘ	Transfer
Test Approved Conel clone clone - Test Scenario test clone id ⓘ	Minimal	Medium	Minimal	Minimal ⓘ	

Certification and Accreditation

Assurance Level

- Correct protection levels?
- Mitigations are sufficiently addressing risks?
- Ensure adequacy of profiling and threat models

Verification

- Requirements are correct and sufficient?
- Are they implemented and evidence provided?

ESA UNCLASSIFIED – RELEASABLE TO THE PUBLIC

Data model

PETER HAGSTROM

Essentials of a Robust SSE Data model

SSE4SPACE
Secure Systems Engineering for Space Missions

Facilitating System Exchange and Integration

Enabling Reuse and Scalability for Future Extensions

Standardizing Terms for Clarity and Consistency

Mapping of external catalogues

RHEA GROUP WMG THE UNIVERSITY OF WARWICK GREY CONSULTANTS OHB «DigitalEngineering» DEKonsult

Core components of the SSE4space Data Model?

SSE4SPACE
Secure Systems Engineering for Space Missions

Glossary of Terms

- Central repository for clear definitions and standardized terminology
- Comprehensive collection with over 1300 specific terms.

Reusable Data Constructs

- Structured using the UML2 framework for consistency and integration
- Facilitates interoperability and modular design

Taxonomy/Ontology

- Defines a clear hierarchy of types, inheritance and interrelations
- Supports logical data structuring and complex system modelling

RHEA GROUP WMG THE UNIVERSITY OF WARWICK GREY CONSULTANTS OHB «DigitalEngineering» DEKonsult

Leveraging the SSE4Space Data Model for Software Impact?

Semantic Integration:

- *Central to enabling consistent interpretation and use across software systems*
- *Ensure components speak the same language*

Model Transformations:

- *Facilitates efficient transitions from model to implementation, reducing development time*

Interoperability:

- *Support integration with MBSE tools like Capella, enhancing collaborative design and engineering.*
- *Ensures alignment with industry standards, promoting software compatibility and compliance*

Scalability and Maintenance:

- *The data model is designed for long-term maintainability, allowing software to evolve with minimal refactoring*
- *Support the growth of software architecture without compromising existing functionalities*

Key Concepts of the SSE4Space Data Model

Things

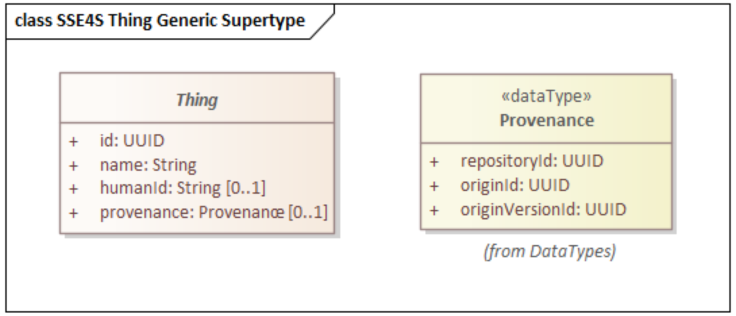
- Represents tangible and intangible entities within the system, serving as the core object of interaction and data collection

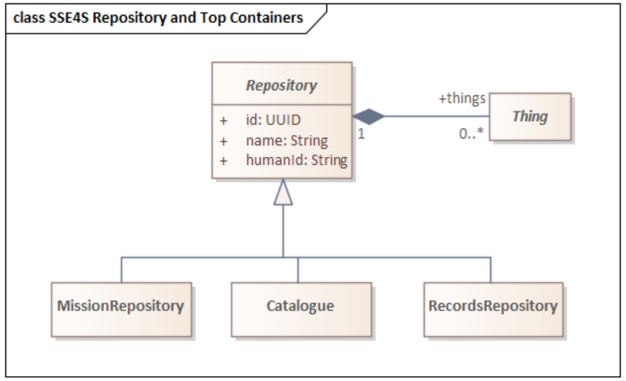
Provenance

- Tracks the origin and lifecycle of data within the system, ensuring traceability and accountability

Repositories

- Centralized storage locations for model elements, facilitating controlled access and version management





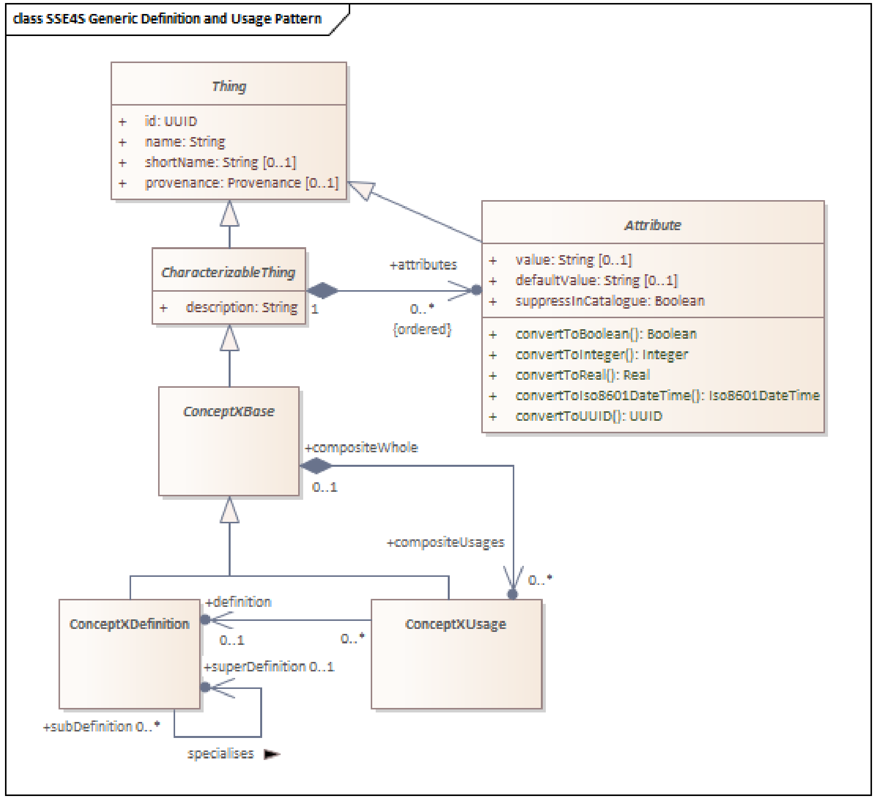
Key Concepts of the SSE4Space Data Model

Definition and Usage Patterns

- Defines how concepts are applied within the system, allowing for dynamic adaptation to new scenarios without system refactoring

User-Defined Attributes

- Allows customization of data points for specific needs, enhancing the model's flexibility and applicability.



class SSE4S Generic Definition and Usage Pattern

Thing
+ id: UUID
+ name: String
+ shortName: String [0..1]
+ provenance: Provenance [0..1]

CharacterizableThing
+ description: String

Attribute
+ value: String [0..1]
+ defaultValue: String [0..1]
+ suppressInCatalogue: Boolean
+ convertToBoolean(): Boolean
+ convertToInteger(): Integer
+ convertToReal(): Real
+ convertToIso8601DateTime(): Iso8601DateTime
+ convertToUUID(): UUID

ConceptXBase

ConceptXDefinition

ConceptXUsage

+attributes 1 0..* {ordered}

+compositeWhole 0..1

+compositeUsages 0..*

+definition 0..1 0..*

+superDefinition 0..1

+subDefinition 0..*

specialises ►

Conclusion: The Value of SSE4Space Data Model

Comprehensive understanding:

- Consolidated over 1300 terms for unambiguous communication within SSE.

Enhanced Interoperability

- Facilitates future integration with MBSE tools and standardization across systems.

Scalable and Flexible

- Designed to evolve with the framework, accommodating future extensions

Practical Application

Software architecture

Web based application (Java Spring/Angular/MongoDB)

Microservices based architecture

Nginx reverse proxy and load balancer

Keycloak SSO integrated

Docker deployment

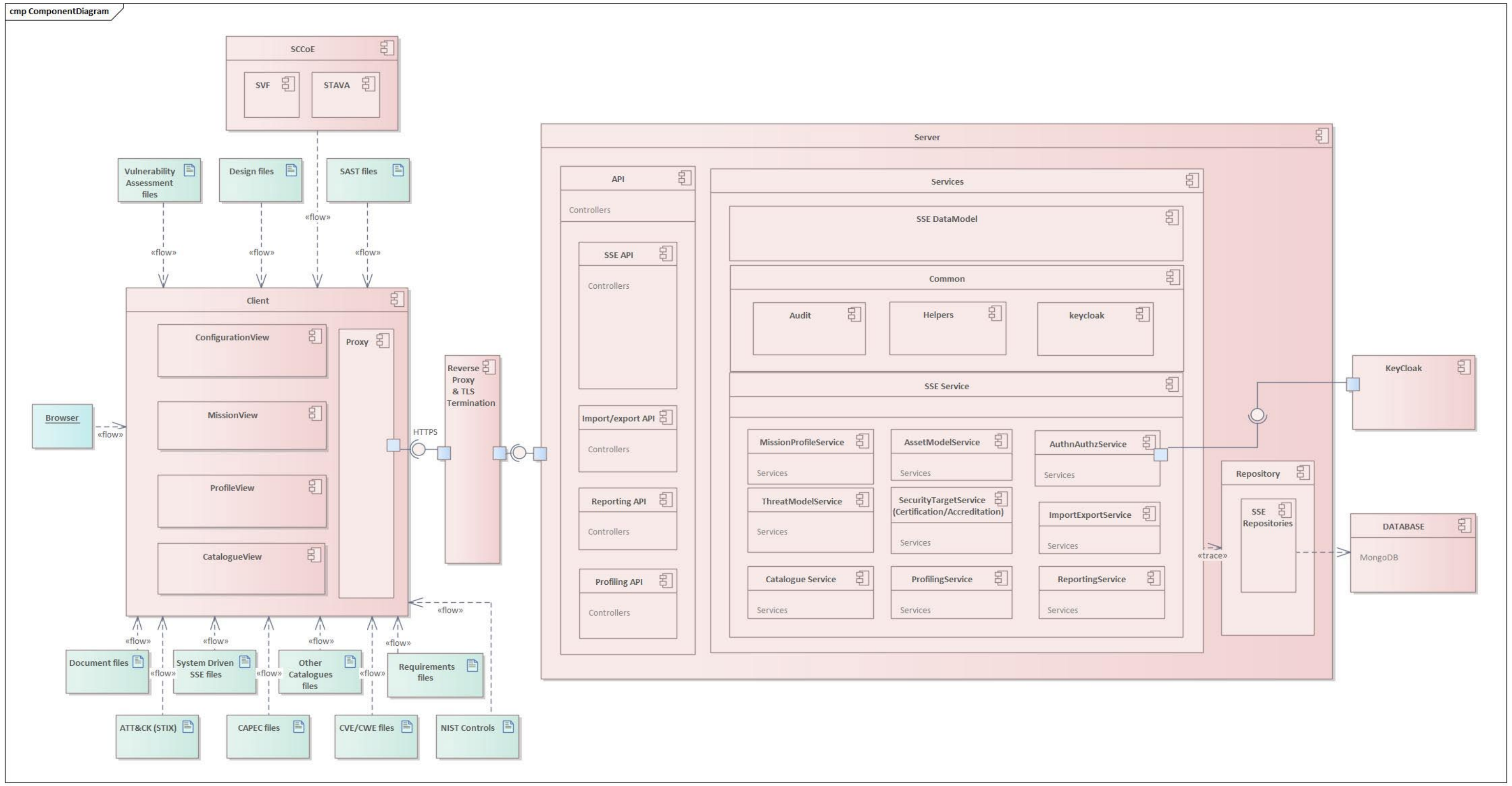
Compatible with the following sources:

- MITRE CVE/CWE, SAST (SonarQube)
- MITRE CAPEC, ATT&CK (STIX)
- GASF, NIST SP 800-53 Controls
- AEGIS

Integrated with SCCoE (STAVA/SVF)

Import/export in CSV/JSON formats

Javers versioning



HSICD

SCCoE integration is based on HSICD specification

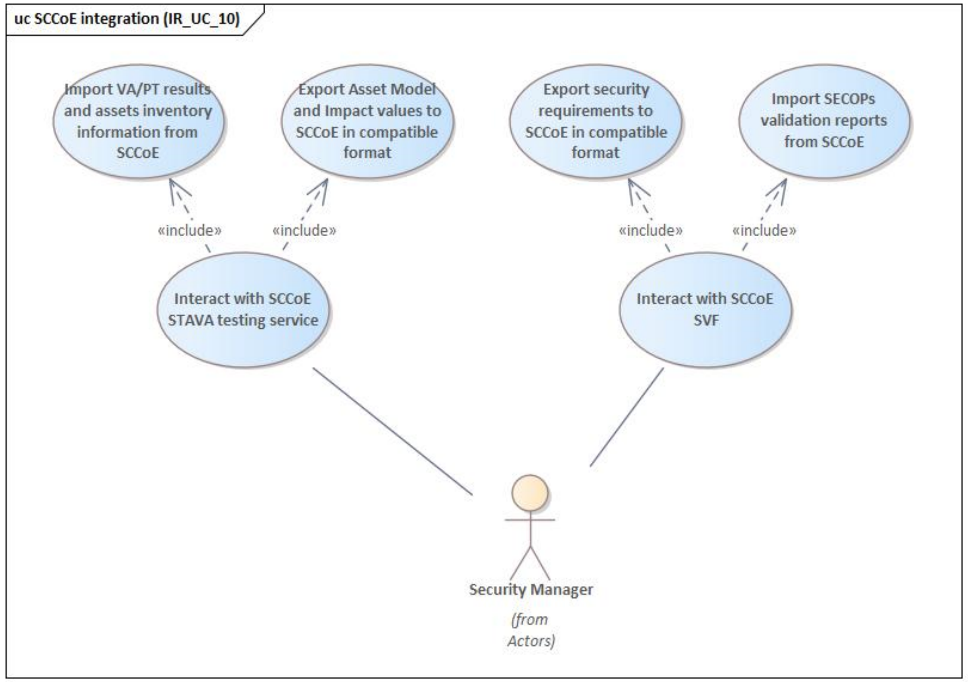
Information are exchanged between systems through JSON files import/export

SVF integration:

- Export Security Functional Requirements (available in Security Target)
- Import SecOps, including the verification evidences (visible under SSE4Space Certification & Accreditation)

STAVA integration:

- Export ToEs assets
- Import vulnerabilities and update asset attributes



uc SCCoE integration (IR_UC_10)
Import VA/PT results and assets inventory information from SCCoE
Export Asset Model and Impact values to SCCoE in compatible format
Export security requirements to SCCoE in compatible format
Import SECOPs validation reports from SCCoE
«include»
«include»
«include»
«include»
Interact with SCCoE STAVA testing service
Interact with SCCoE SVF
Security Manager
(from Actors)

Validation feedback

- The methodology and also the software tool allow for a variety of user types to perform and also evaluate the SSE process, throughout the life of a project from start to finish.

- The main advantage of the tool is to be the single repository of the overall amount of the mission security information relevant from a systems engineering and project management perspectives along the project phases.

- In the current stage of development, the tool is useful in the organization and manipulation of the information, while the methodology (and therefore the tool) is missing a reference model *(e.g. risk reduction points)* assisting in the risk calculation steps and therefore enabling the harmonization of the residual risk (manual) calculations carried out by the different actors involved in the risk assessment when analyzing complex systems.

SSE4SPACE
Secure Systems Engineering for Space Missions

Validation feedback

- During validation, the tool was continuously improved, either by eliminating software errors or adding minor functionalities

- Various suggestions were made for improving the methodology/tools, for example:
  - In the Methodology, the three profiles (Protection Profile, Security Target Profile and the Security Controls Profile) are separated from each other; in the tool, the Security Target Profile and Security Controls Profile are combined. This should be adapted to the methodology
  - Automatic suggestion of risk reduction points associated to each protective measure applied
  - Automatic combination of the overall risk residual risk based on the combination of each risk associated to each different asset involved in the same TOE

SSE4SPACE

Secure Systems Engineering for Space Missions

Lessons Learned and Future Roadmap

PETER HAGSTROM

RHEA GROUP

WMG THE UNIVERSITY OF WARWICK

GREY CONSULTANTS

OHB

«DigitalEngineering»

DEKonsult

Achievements

Methodology Development

A robust secure system engineering methodology

Embedded in SDLC

Integrating threat modelling, vulnerability analysis, risk assessment

Incorporating ECSS standards, space-specific taxonomies and best-practices and catalogues.

Data model

Powerful and flexible

Facilitates the future integration with MBSE tools

Software tool

Addressing a gap in existing industry tools

Implementing methodology and solid foundation for future

Validated on relevant mission

Lessons Learned

Complexity of Development

- Methodology requires thorough testing and a comprehensive worked examples
- Software development of novel approach to security engineering requires multifaceted knowledge and tight collaboration with end-users and stakeholders.

Glossaries and Taxonomies

- The utility of well-organized glossaries and taxonomies in providing common understanding of terms and facilitating communication.

Challenges

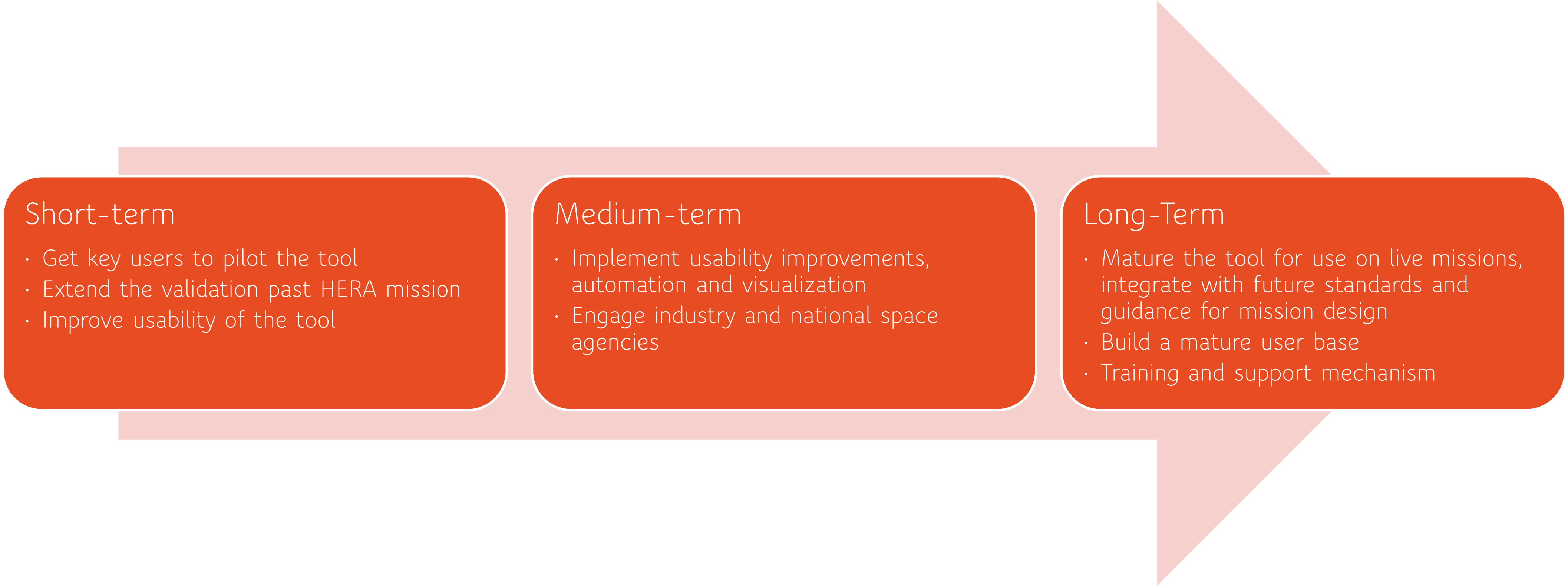
Complexity of the methodology

Usability, UI refinement and automation

Integration with existing tools

Training and Embedding

Future Roadmap



Short-term

- Get key users to pilot the tool
- Extend the validation past HERA mission
- Improve usability of the tool

Medium-term

- Implement usability improvements, automation and visualization
- Engage industry and national space agencies

Long-Term

- Mature the tool for use on live missions, integrate with future standards and guidance for mission design
- Build a mature user base
- Training and support mechanism