USRF

Final Presentation

Agenda & Introduction

TELESPAZIO a LEONARDO and THALES company

VISIONSPACE

RHEA GROUP

Timeline

- ITT – Mid 2020
- KO – Mid 2021
- Final Architectural Design – Mid 2022
- First successful communication – Late 2022
- Successful Automated Testing – Mid 2023
- Security Assessment – Mid 2024
- Final presentation – Late 2024

Agenda

- Introduction to USRF
- Presentations by the consortium
  - Automated E2E test procedures– By VisionSpace
    - Test environment and tools
      - ESTEC
        - ATB
        - EagleEye
      - ESOC
        - EGS-CC
        - TEMPPO
        - EUDART
      - EKSE based automated scripts
      - Scenario validation framework
      - EagleEye Configuration and On-board software upgrade
    - FBO test procedures
  - OBSW – By Telespazio
  - Security Tests – By RHEA
- Demos
  - EGS-CC FBO Demo
  - Scenario Validation Demo 1
  - Scenario Validation Demo 2
- Q&A

Introduction to USRF

- Who has been involved in USRF?
- What is USRF?
- Key features and functionalities of USRF.

Who has been involved in USRF?

Who has been involved in USRF?

- Jean-Christophe Berton, Technical Officer (TO) - ESA/ESOC
- Quirien Wijnands, ESA/ESTEC
- Alexia Mallet, ESA/ESTEC
- Quinten Van Woerkom, ESA/ESTEC
- Miguel Rey, VisionSpace Technologies GmbH
- Temesgen Gebremedhin, VisionSpace Technologies GmbH
- Stephan Kranz, Telespazio Germany
- Johan Marx, Telespazio Germany
- Danilo Ingami, RHEA Group
- Matteo Merialdo, RHEA Group
- Panagiotis Bellonias, RHEA Group

TELESPAZIO a LEONARDO and THALES company

VISIONSPACE

RHEA GROUP

What is USRF?

- Unique (“Unified”) Space Mission Simulation Reference Facility (USRF)
- Demonstrates a prototype to perform End-to-End (E2E) mission-level simulations, testing (including security), verification, validation, and mission operations preparation.
- Integrates space and ground assets from various ESA sites (ESOC & ESTEC) and facilities to create representative mission-level E2E scenarios.
- Establishes connectivity between Ground systems (EGS-CC) at ESOC and the Avionics Test Bench (ATB) at ESTEC.
- Reference mission: **EagleEye**

Key features and functionalities of USRF

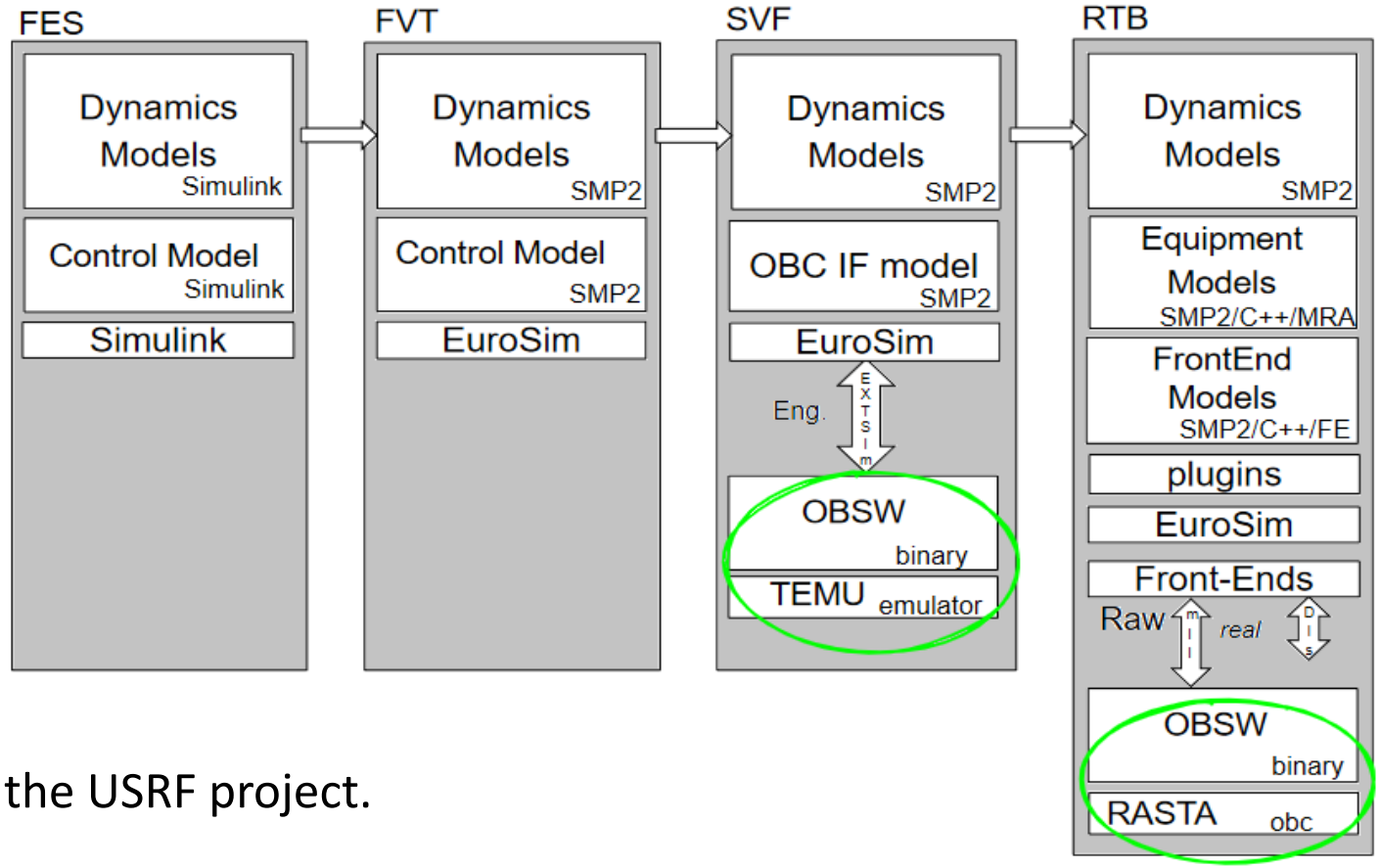
- Utilizes a common set of tools for designing, configuring, conducting and reporting tests.
- Enables the integration of resources across various ESA facilities to establish Test Assemblies.
- The capability to enable, monitor and control the secured connections between the different facilities and other relevant aspects of the USRF.

Automated E2E test procedures

- Test environment and tools
  - ESTEC
    - ATB
  - ESOC
    - MCS-CC
    - TEMPPO
    - EUDART
- EKSE based automated scripts
- EGS-CC WebUI tests
- EagleEye Configuration and On-board software upgrade
- Scenario Validation testing framework

EagleEye ATB

- **ESTEC ATB** is an ESA test bench that facilitates the evaluation, validation, and demonstration of spacecraft technology standards.
  - FES (a Functional Engineering Simulator)
  - FVT (a Functional Validation Testbench)
  - SVF (a Software Validation Facility)
  - RTB (Real-Time Bench)



- THE **SVF** configuration has been used for the USRF project.

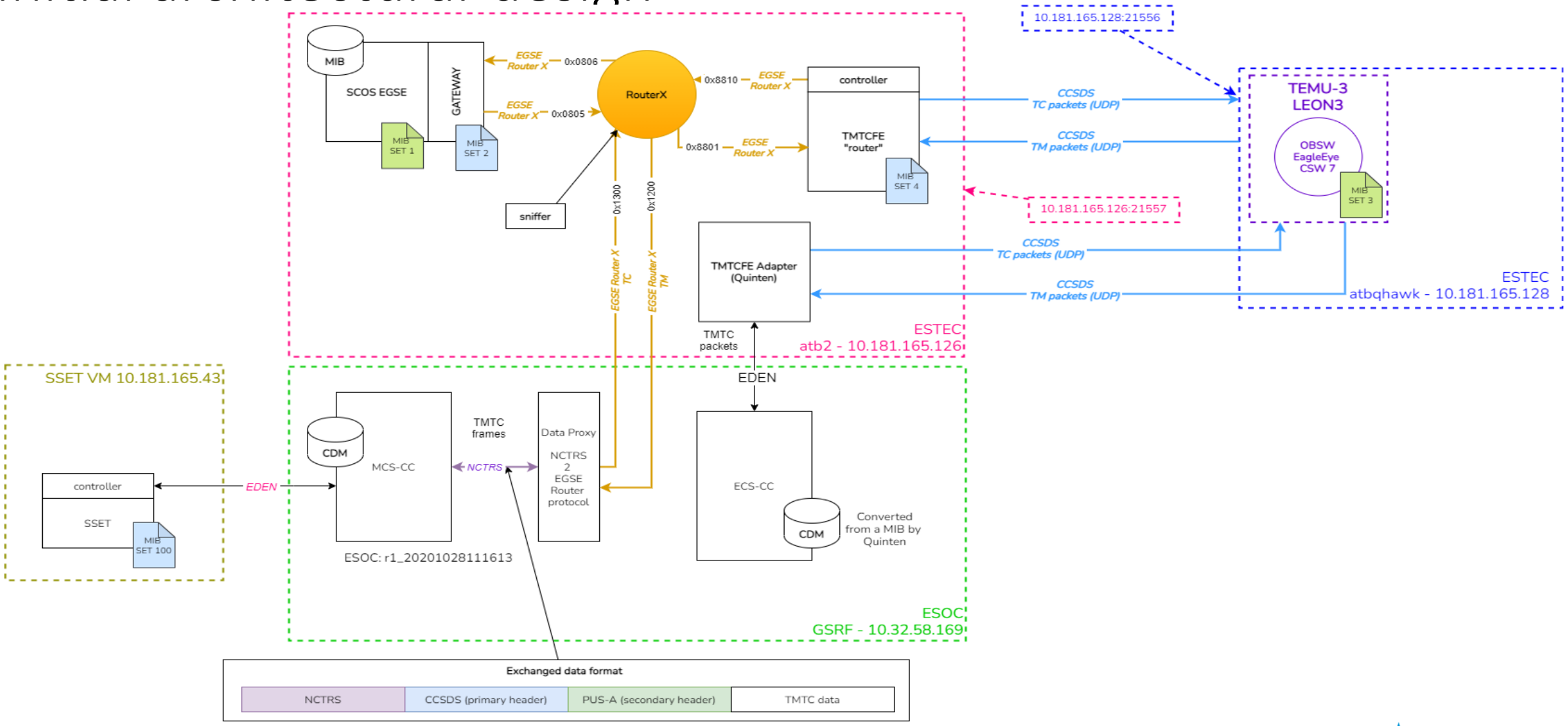
EagleEye

- A reference mission configuration which is used in the ATB development.
- Simulates an Earth Observation satellite composed by a set of AOCS sensor/actuators, thermal/power subsystems, and a simple optical payload (GoldenEye).
- The EagleEye On-board software runs in the TEMU(Terma Emulator).
- The simulation models cover the following parts:
  - Environment
  - AOCS (Sensors & Actuators)
  - Power Subsystem
  - Thermal Subsystem
  - Payload

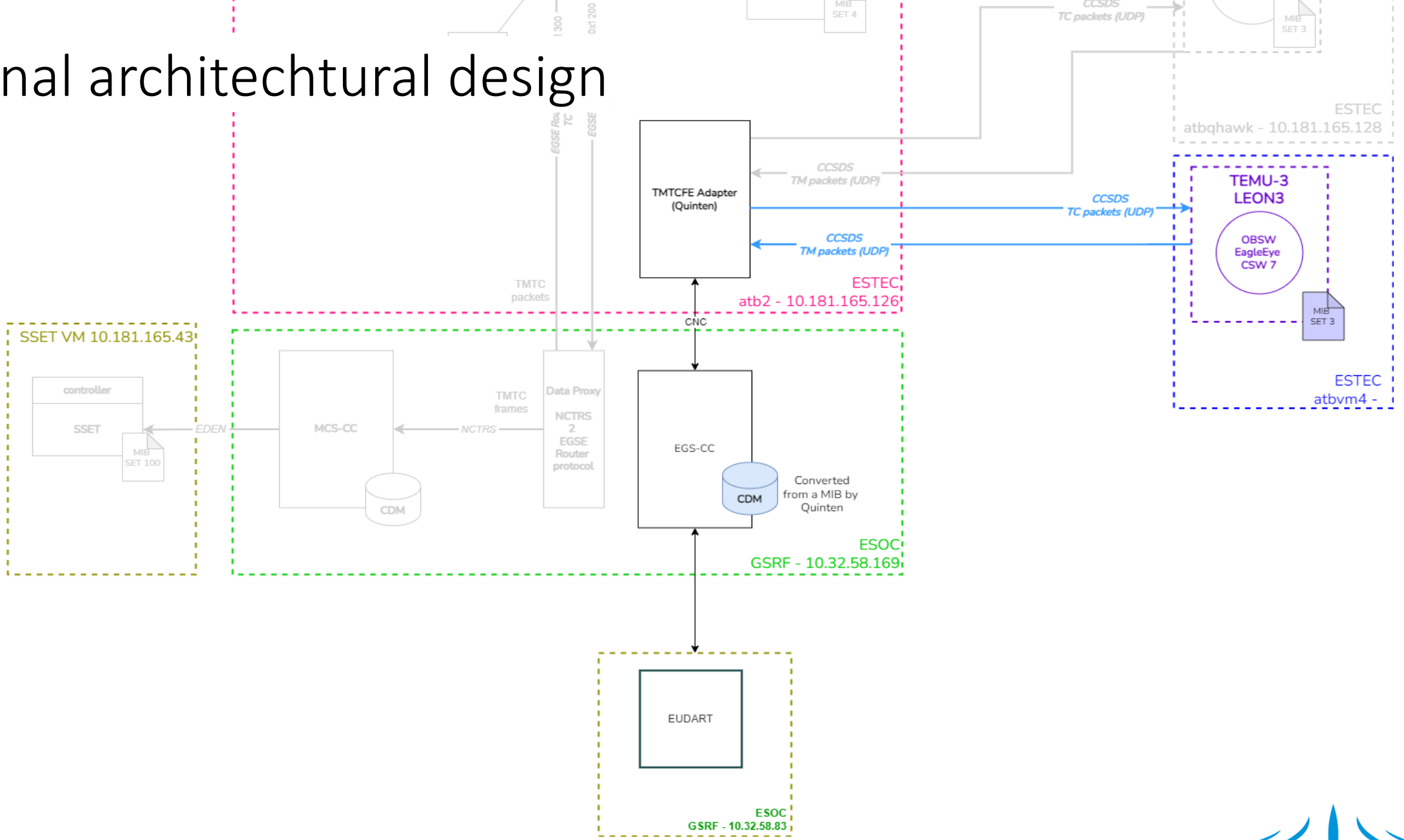
Mission Control System

- At the start of the project, we deployed MCS-CC, which includes the EGOS-CC components (with one C2LOCO component). However, since the TM packet format provided by ESTEC does not match the format expected by MCS-CC, we opted to use a pure EGS-CC deployment instead.
- During the project duration, releases R1, R1.6, and R1.8 of EGS-CC were utilized.
- At the start of the project, the OPS-SAT DataProxy tool was used to enable communication between the Mission Control System (MCS) and the ground station, which connected to the RouterX at the ESTEC Avionics Test Bed (ATB).
- The final design approach demonstrates that communication between the EGS-CC (ESOC GSRF) and the TMTCFE adapter (ESTEC ATB) is enabled through the use of CNC. The following features have been achieved:
  - Receive TM flow from OBSW emulator.
  - Send TC, perform file-based operations
  - Access EGS-CC using the latest Web-UI

Initial architectural design

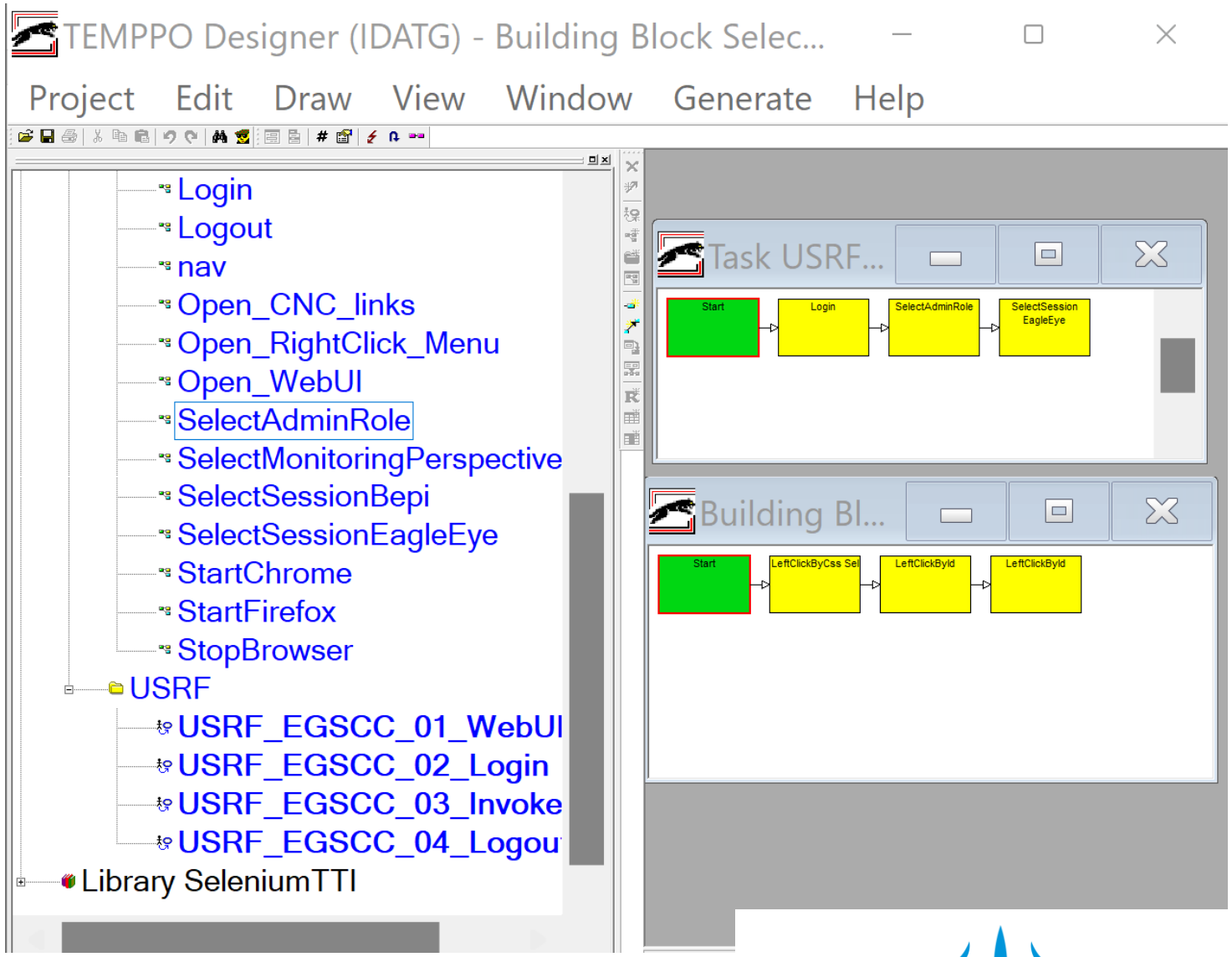


Final architechtural design



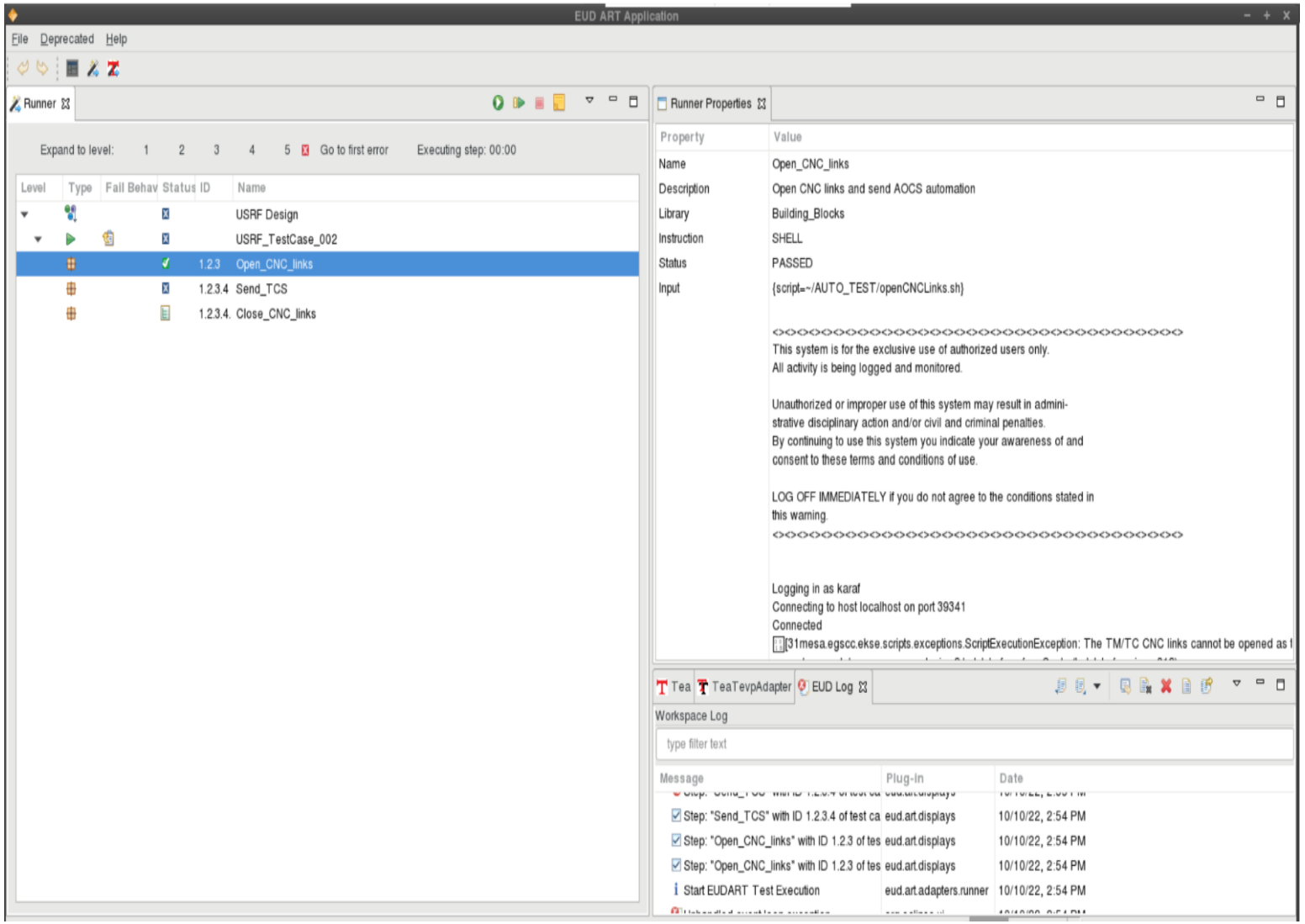
Test Execution Managing, Planning, and Reporting Organizer (TEMPPO)

- Used for specification of hierarchical sequence diagrams and automated generation of test cases.
- In USRF, TEMPPO designer is utilized to define test specifications and generate a test script, which will be executed using EUDART.



EGOS User Desktop Automated Regression Testing (EUDART)

- An ART tool based on EUD framework.
- Execute automated tests designed for EGS-CC.



EGOS User Desktop Automated Regression Testing (EUDART)

```
<?xml version="1.0" encoding="UTF-8" ?>
<TESTITEM name="USRF_test2" description="EagleEye test automation " version="1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" >
<TESTDESIGN name="USRF Design" test_level="" test_type="test" description="EagleEye test design">
        <TESTCASE name="USRF_TestCase_002" type="Graph Coverage" category="" title="test" description="EUDART -> EGS-CC -> EagleEye testcase" configuration="
" required_tool="" criticality="MAJOR" test_case_type="START" >

<STEP name="Open_CNC_links" is_executable="1" step_id="1_2_3" depth="3" library="Building_Blocks" description="Open CNC links and send AOCS automation" expec
ted_result_text="EKSE started" expected_result_value="0" test_oracle="COMPARE_INTEGER" instruction="SHELL" criticality="MAJOR" timeout="0" internal_id="5wvEy
MWZc@Cb">
        <PARAMETER name="script" value="~/AUTO_TEST/openCNCLinks.sh"/>

</STEP>
<STEP name="Send_TCS" is_executable="1" step_id="1_2_3_4" depth="3" library="Building_Blocks" description="Invoke AOCS_TS110" expected_result_text="EKSE star
ted" expected_result_value="0" test_oracle="COMPARE_INTEGER" instruction="SHELL" criticality="MAJOR" timeout="0" internal_id="5wvEyMWZc@Cb">
        <PARAMETER name="script" value="~/AUTO_TEST/automationAOCS.sh"/>

</STEP>

<STEP name="Close_CNC_links" is_executable="1" step_id="1_2_3_4_5" depth="3" library="Building_Blocks" description="Close CNC Links " expected_result_text="E
KSE started" expected_result_value="0" test_oracle="COMPARE_INTEGER" instruction="SHELL" criticality="MAJOR" timeout="0" internal_id="5wvEyMWZc@Cb">
        <PARAMETER name="script" value="~/AUTO_TEST/closeCNCLinks.sh"/>

</STEP>

</TESTCASE>
</TESTDESIGN>
</TESTITEM>
```

Scenario Validation Testing framework

Is used to define and execute tests by interacting with the EGS-CC Web UI. It includes a set of tools such as Selenium, pytest, and the Page Object Pattern.

- **Selenium**: An open-source framework used to create regression automation tests.
- **Page Object Pattern**: A design pattern that wraps all elements, actions, and validations happening on a page into a single object.

Selenium Grid: A component of Selenium that allows you to run tests on different machines against different browsers in parallel. It consists of a central hub and multiple nodes.

- **Selenium Hub**: The central point that controls the test execution. It routes the tests to the appropriate nodes based on the configuration and available resources.
- **Selenium Nodes**: Machines that execute the tests. They can run different browsers and environments, allowing for a diverse and robust testing setup.

FBO test procedures

- CreateFile
- CopyFile to Ground (Download)

Telespazio Contribution in USRF

Final Presentation

TELESPAZIO a LEONARDO and THALES company

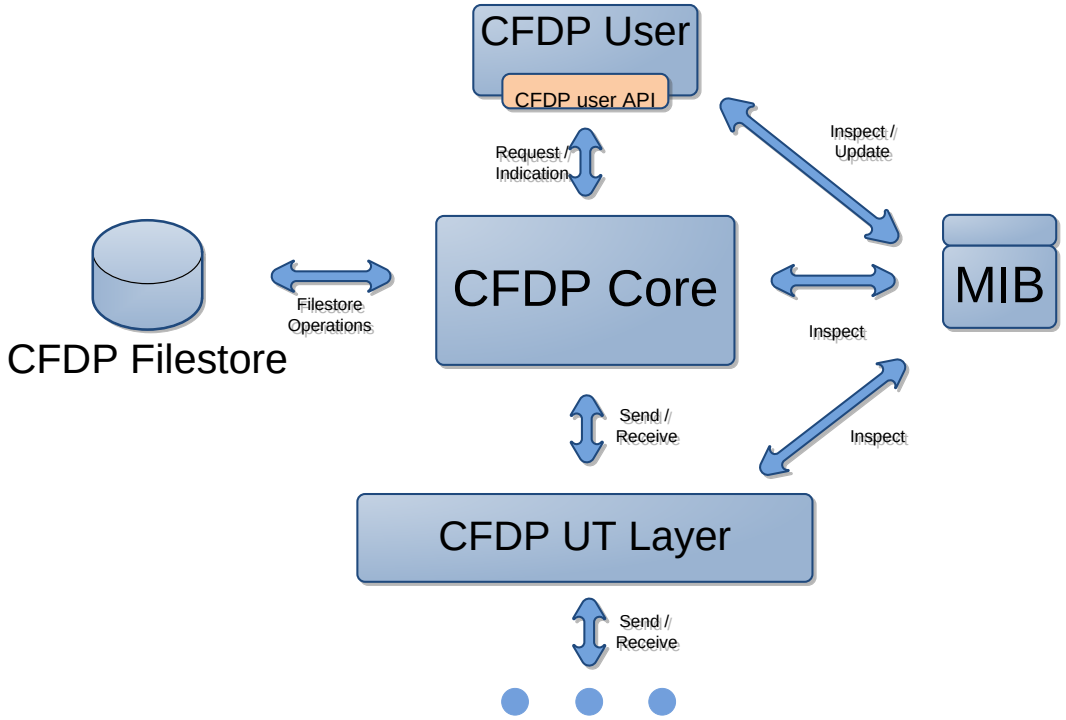
VISIONSPACE

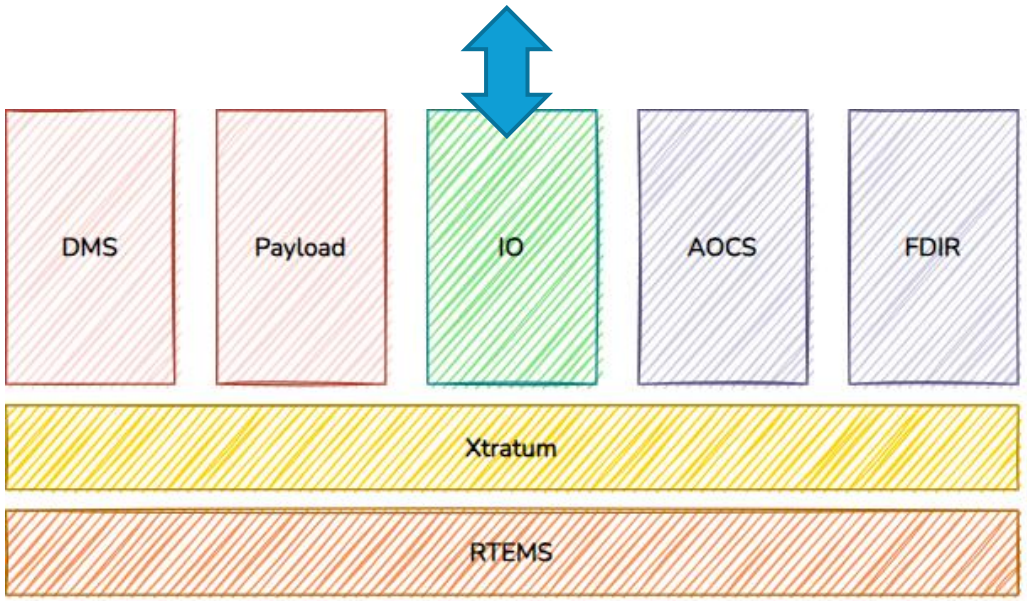
RHEA GROUP

USRF File Based Operations (FBO)

- CCSDS File Delivery Protocol (CFDP)
- Euclid Space to Ground Interface, i.e. TM/TC Service 140
- Telespazio responsible for Space Segment
  - Avionics Test Bench in Software Validation Facility (SVF) Configuration
  - Eagle Eye Reference Mission (Simulation and On-board software)
  - ENEA CFDP Library (Reused 3rd party software)

ENEA CFDP Library vs Eagle Eye OBSW



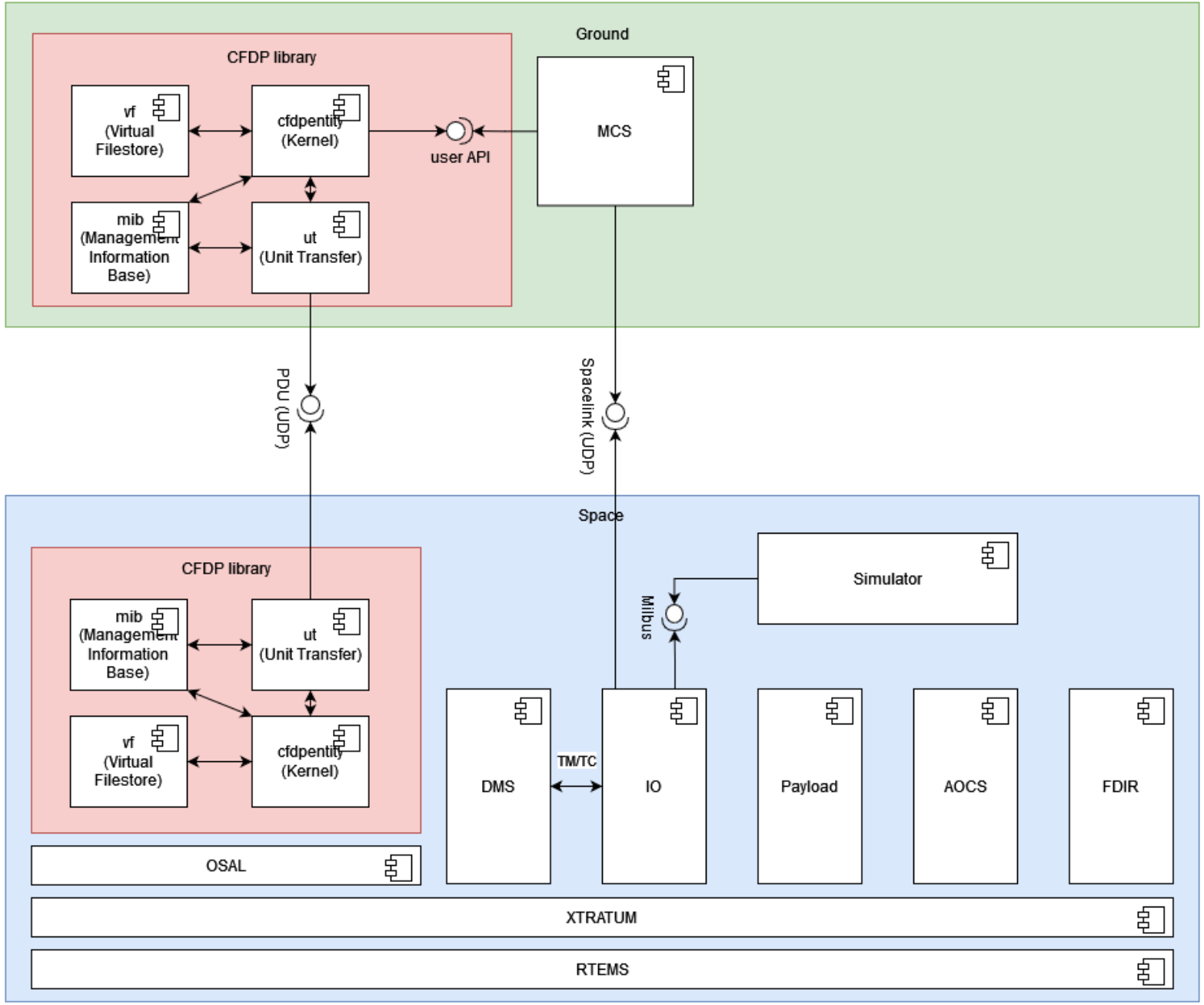


Integration I

Separate UDP Channel

does not follow

Euclid Space to Ground ICD

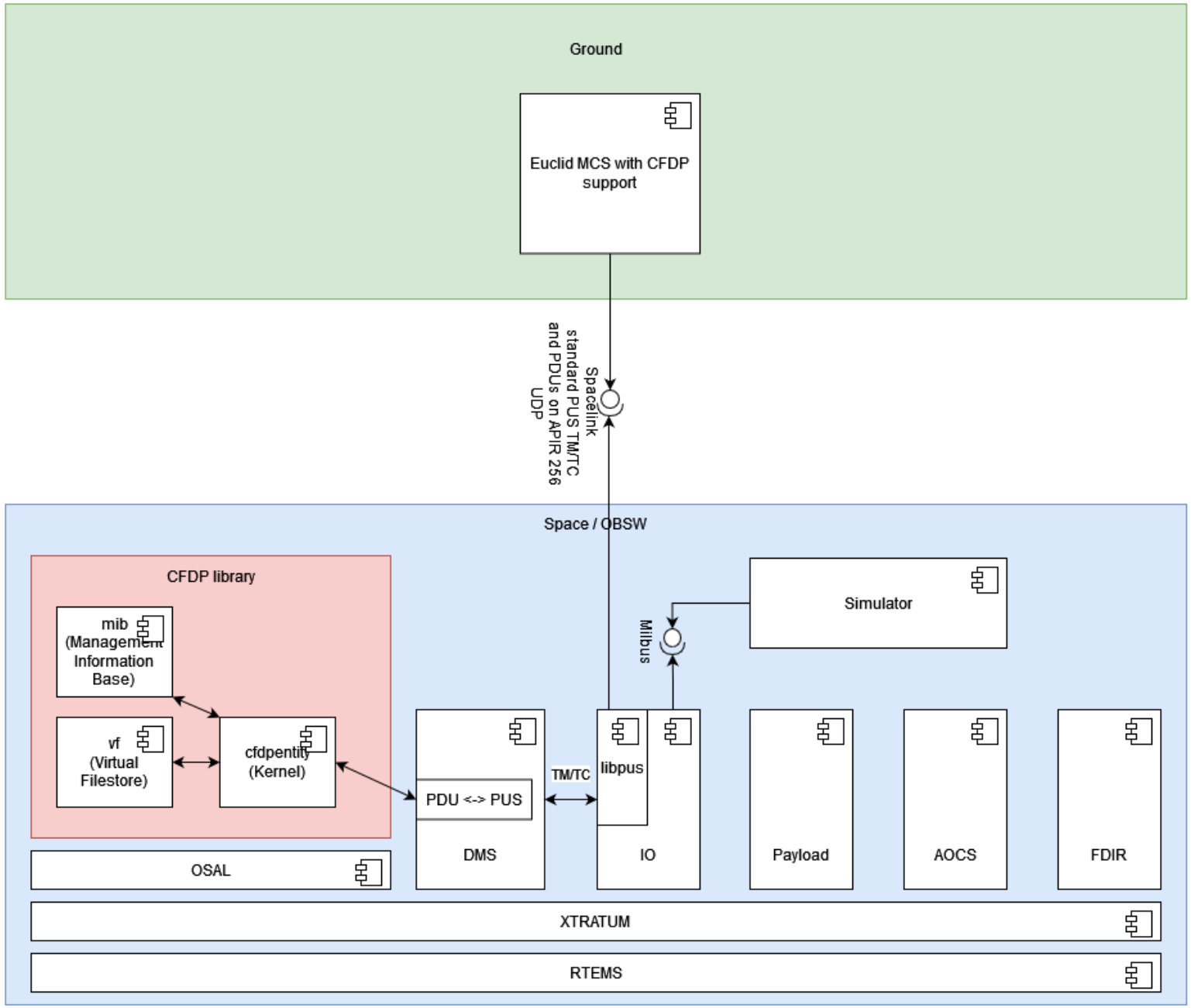


Integration II

Use standard Spacelink

and

replace CFDP UT component by PDU <-> PUS adapter



Implementation

- SVF Configuration using TEMU 3.0
- Eagle Eye OBSW available in GIT under ctusrf branch
- Using existing Sparc partition memory specification
- Local (atbqhawk) test setup using Test Sequence Controller to send TC 140, X and PDUs

PDU – PUS Adapter Features

- Ground to Space
  - PUS Service TCs 140 with APID 892 are converted into CFDP Filestore Requests
    - TC 140, 1 Create Directory
    - TC 140, 2 Remove Directory
    - TC 140, 20 Create File
    - TC 140, 21 Remove File
    - TC 140, 50 Copy File
  - CFDP PDUs with APID 256 within TC packets are simply forwarded
    - Extended libpus to handle TC packets without secondary header (special routing)
- Space To Ground
  - CFDP PDUs are encapsulated into TC packets with APID 256
    - Message PDU
    - File Data PDU
    - EOF PDU

Conclusions and Next steps

- Conclusions
  - Integration of CFDP support into EagleEye OBSW has been performed successfully within certain limitations:
    - Euclid ICD
    - Available on-board memory
- Next steps
  - Extend MCS to support native CFDP packets ground to space
  - Assess required on board VFS size and configure OBSW partition memory layout accordingly.
  - Extend Test Sequence Controller to support CFDP packets for open loop testing.

USRF

Final Presentation – Security Aspects – RHEA Contribution

TELESPAZIO a LEONARDO and THALES company

VISIONSPACE

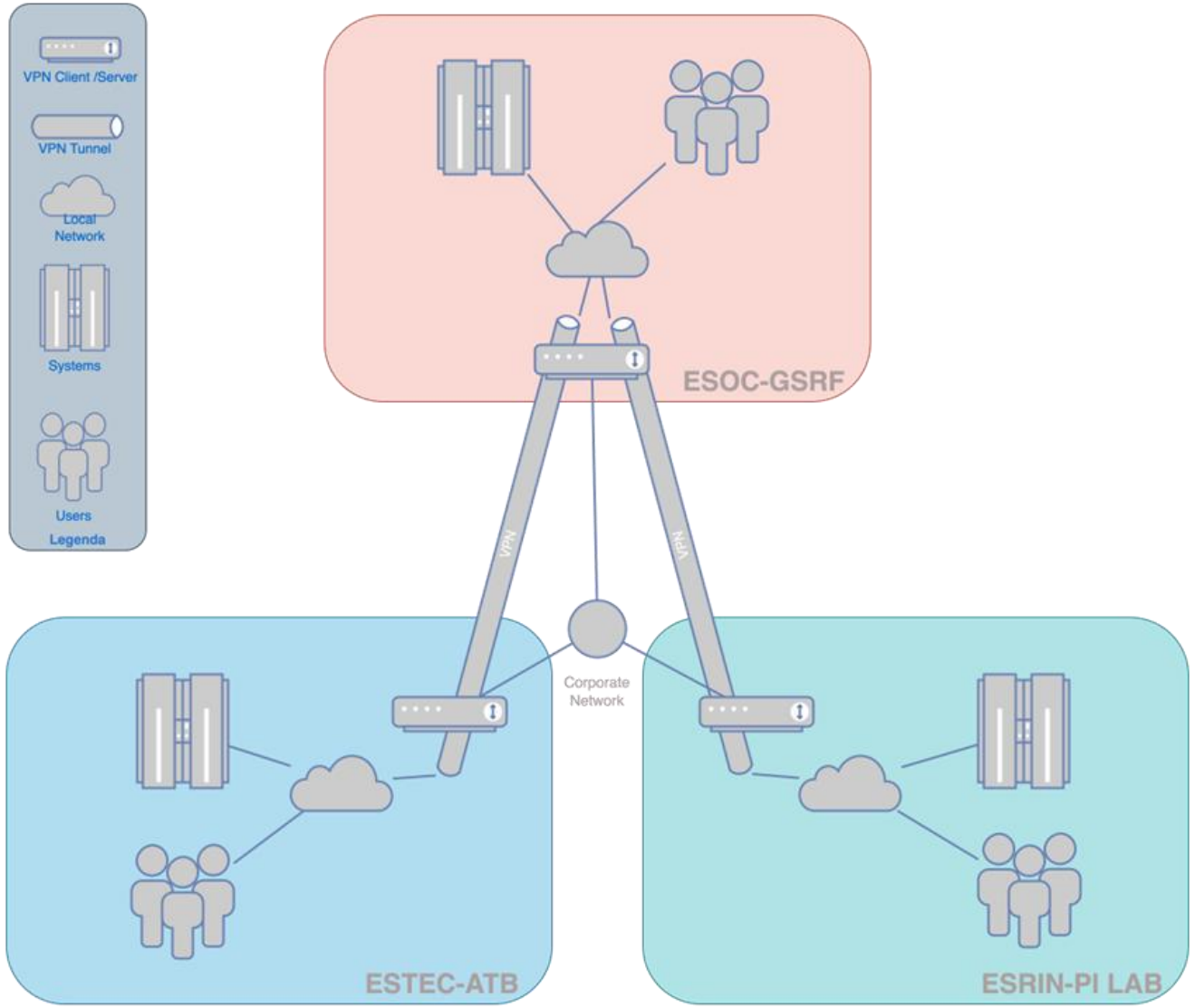
RHEA GROUP

RHEA Contribution in USRF - Requirements

- Contribution to *Requirements Baseline* document (VST-ESA-USRF-RS-001)
  - Supported Visionspace on the requirements elicitation and provided Security Requirements to be added to the Baseline

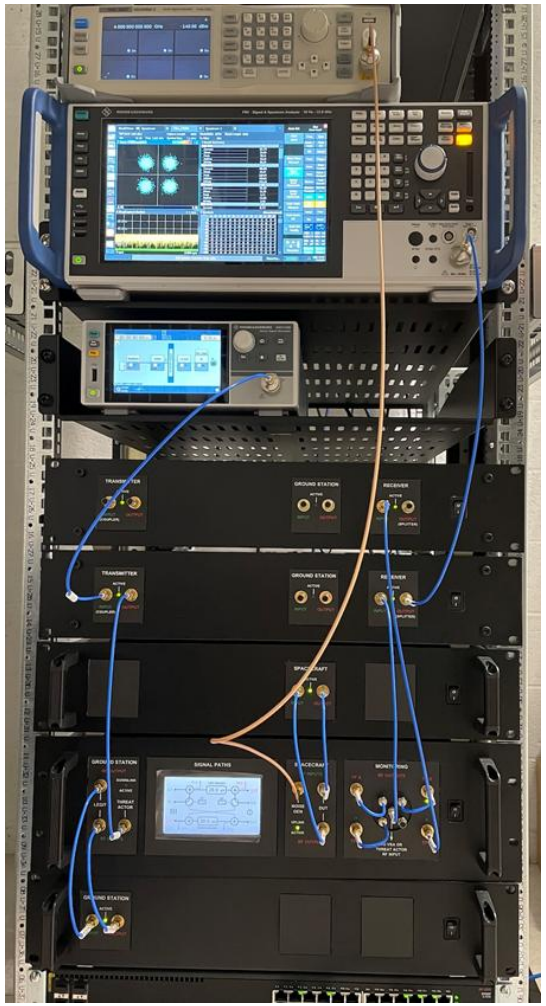
RHEA Contribution to USRF - Design

- Contribution to *USRF System Design Document* (VST-ESA-USRF-DD-001)
  - RHEA analysis focused on the USRF Interconnection between ESOC-GSRF and ESTEC-ATB and ESRIN-FLAB and the related Functional, System (SYS), Management, Security and Performance Requirements for the VPN Virtual Machine to be used to establish the interconnection



RHEA Contribution to USRF – AIV Tests

- Contribution to *USRF Technical Note for space mission AIV tests* document (VST-ESA-USRF-TN-011)
  - Leveraging on the SPARTA framework, we defined a set of generic attack scenarios (mainly focused on LEOP Phase) for space systems
  - **Approach**:
    - Development of **generic attack scenarios** based on the SPARTA framework, integrated with outputs from RHEA's project Cyber Defense 4 Space (ESA/EDA)
    - The attack scenarios are traced to Tactics and their related Techniques from SPARTA
    - Practical method to define possible scenarios useful to guide penetration testing or risk analysis activities.
  - **Application**:
    - Elicited scenarios are mainly focus on the LEOP Phase but can be extended to other phases.
    - Includes R/F-based attacks, excludes physical, APT, and supply chain scenarios.
  - **Testing Considerations**:
    - Scenarios impacting in-orbit satellites should be pen tested using an IP-R/F testbed (e.g., ESA Traleo 2 project).
    - The list elicited during the project is non-exhaustive and can be expanded using SPARTA and related matrices.
  - **Perspective**:
    - Attack scenarios are described from an attacker's point of view.



RHEA Contribution to USRF – AIV Tests

Example of elicited generic attack scenario

Attack Scenario	Tactic	Tactic Description in the context of the attack scenario	Technique(s) – Attack Vector(s)
Exploiting Software Vulnerabilities	Initial Access	Identify and exploit a software vulnerability (on the ground or space segments), such as an unpatched bug or a security misconfiguration.	1. Compromise Supply Chain 2. Compromise Ground Segment 3. Compromise Hosted Payload 4. Auxiliary Device Compromise
Exploiting Software Vulnerabilities	Execution	Use the exploited vulnerability to inject and execute malicious code on the device.	1. Malicious Code
Exploiting Software Vulnerabilities	Persistence	Install a rootkit or other type of persistent malware to maintain access over time.	1. Backdoor 2. Ground System Presence
Exploiting Software Vulnerabilities	Defense Evasion	The attacker tries to use software exploits to conceal its own identity.	1. Overflow Audit Log 2. Modify Whitelist
Exploiting Software Vulnerabilities	Impact	Disrupt the device's operations, alter its data, or cause physical damage.	2. Deception 3. Disruption 4. Denial 5. Degradation 6. Destruction

RHEA Contribution to USRF – Penetration tests

Date of Execution: May 22-24, 2024

Focus:

- Identifying vulnerabilities in network services.
- Examining security of communication between GSRF and ATB networks.

Approach:

- Blackbox assessment simulating external attacker perspective.
- Inspired to the 'Exploiting Software Vulnerabilities' attack scenario.

Conclusion:

- Tests concluded ahead of time, after ESA alert due to malicious software detection.

Scope and Setup of the Penetration Test

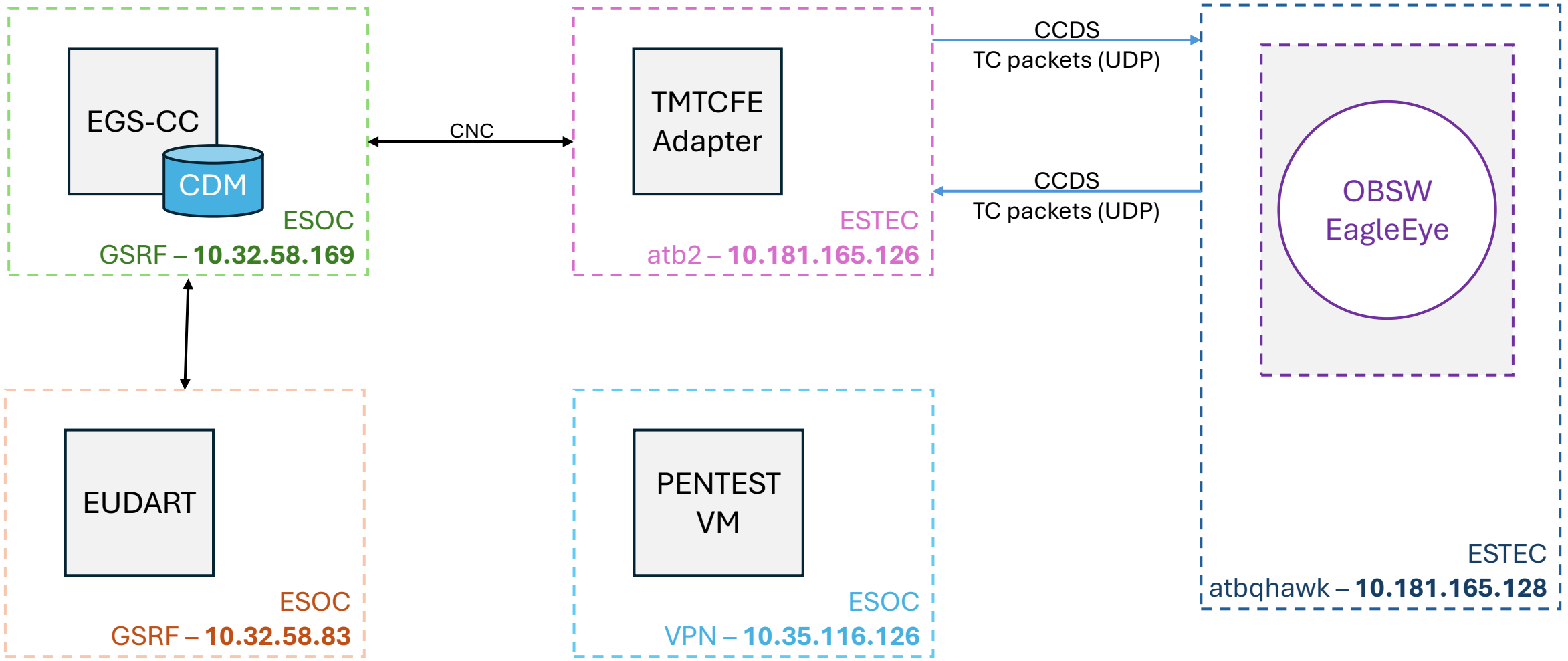
Scope:

- Targets: ESOC GSRF (IP: 10.32.58.169, 10.32.58.83) and ESTEC ATB (IP: 10.181.165.126, 10.181.165.128).
- Hosts included EGS-CC installation, automated test tooling, and EagleEye OBSW.

Setup:

- - VPN connection provided to access the environment.
- - Pentest VM with IP 10.35.116.126 was used for the assessment.

Network Diagram



Network Scan Findings

Tools Used:

- nmap for TCP and UDP scans.
- ssh-audit for SSH configuration.
- Wireshark for network analysis.

Key Findings:

- Open Ports: SSH (22), MySQL (3306), VNC (5901), XRDP (3389).
- Higher Ports: Used for information exchange; TCP connections established but no additional details revealed.

Identified Vulnerabilities and Recommendations

Identified Vulnerabilities:

- Weak SSH algorithms and deprecated encryption algorithms.
- Simple authentication methods (username/password).
- Easy-to-guess passwords.

Recommendations:

- Remove weak algorithms and enforce key-based authentication.
- Use unique passwords and password managers.

Conclusion and Key Findings

High-Risk Findings:
- Easy-to-guess passwords with high impact.

Medium-Risk Findings:
- Weak SSH algorithms.
- Simple authentication enabled.

Overall Recommendation:
- Improve security configurations to mitigate identified risks.
- Tighter coordination with ESACert and ESA CSOC.

Possible Next Steps

- Perform a security assessment of the network communication while a simulation is running.
- Conduct periodic threat modelling sessions to proactively identify and address potential attack paths as the environment evolves.

- These tasks could be performed by the CSOC T3 team and coordinated with ESA CSIRT and MOI NOC

Demos

- EGS-CC FBO Demo
- Scenario Validation Demo 1
- Scenario Validation Demo 2

Conclusions & Future Work

- The USRF project successfully demonstrated the feasibility of securely integrating different ESA facilities into a cohesive mission simulation environment.
  - Define test specifications to validate EGS-CC through EKSE using the TEMPPO designer and generate test scripts for execution in EUDART.
  - Create test cases aimed at validating and executing UI-based tests on the EGS-CC WebUI using the Scenario Validation framework (Selenium).
- The prototype has proven its ability to support End-to-End mission scenarios, contributing to thorough test and validation of future mission operations infrastructure systems in a more coordinated, representative and coherent environment.

Thanks!

Q&A