ENGINEERING THE WORLD WITH YOU

TRALEO Threat and Risk Assessment on LEO constellations

TRALEO EXECUTIVE SUMMARY

Reference: RHEA/WO300571-TRALEO/ESR
Issue: 1.0
Issue date: 07/12/2020
Prepared by: TRALEO team

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS

Table 1: Acronyms

Acronym	Meaning
CR	Cyber Range
CSP	CubeSat Space Protocol
MCOP	Mega-Constellation Operations Platform
PT	Penetration testing
RDP	Reliable Datagram Protocol
TRA	Threat and Risk Assessment
TTC	Telemetry, Tracking and Command
VA	Vulnerability assessment
VGS	Virtual Ground Station
VM	Virtual Machine
VS	Virtual Satellite

1. BACKGROUND AND OBJECTIVES

In recent years there has been a proliferation of ideas about using larger satellites constellations based on smaller and cheaper satellites in Low Earth Orbit (LEO) to provide innovative services for communication, e.g. IoT, Earth Observation, AIS and ADS-B data collection respectively from Maritime users and Airplanes. For instance, LEO Nanosatellites are smaller in size (<30 kg) and operate in orbits closer to earth which makes them an order of magnitude cheaper to buy and manage than conventional Geostationary satellites.

In addition, the demand for providing high throughput broadband secure communication and 5G space enabling services through cost-efficient and robust constellation of LEO satellites has significantly increased due to the fact that a LEO satellite approach to broadband communication will reduce the network latency due to signal time of travel in space with ~85% resulting in a much better user response to demand e.g. for browsing, compared to GEO and MEO constellations.

In the recent decades, satellite service providers have been put on a high alert of a possible cyberattack by a variety of threat actors, from individual hackers to powerful nation states.

The satellite communications that ships, planes, drones etc. use and which are operated by civil and military institutions to connect to the internet are vulnerable to hackers who, in the worst-case scenario, could carry out “cyber-physical attacks”, turning satellite antennas into weapons. In addition, different failures can result from jamming satellite communication.

In particular, since satellite networks are becoming an integral part of larger terrestrial networks in 5G networks, hackers are now using space infrastructures as soft targets. Furthermore, as satellites play a unique role in the Internet of Things, hijacking them or controlling them can yield a bouquet of benefits to hackers.

As the demand for using satellite constellation networks increases, the users expect to connect to a highly available communication network delivering secure and reliable/integer data which are resilient against attacks.

These platforms require “**security by design**” and comprehensive cyber security protection to tackle any cyberattacks threats.

In this context, the operation of future LEO constellations still needs to be addressed from the cyber resilience point of view. Unfortunately, nowadays there is no particular benchmark or tool that exists to access LEO satellite constellation cyber security and/or to validate their level of resilience against cyber-attacks.

The technical objective of the TRALEO activity was to gain a first insight in the overall cyber resilience of a Small/NanoSat space mission in order to mitigate for cyber threats in existing missions and to enhance resilience in upcoming new Small/NanoSat constellation missions.

This has been achieved by RHEA, an established space systems and security solutions company taking advantage of an unprecedented and very recent flight heritage by GOMSpace on a twin GOMX-4 A/B platform still flying in formation.

The activity was based on the analysis, carried out by several means (penetration testing, risk analysis, vulnerability assessment) of the GOMX-4B satellite and its emulation implemented over the RHEA Cyber Range, a cloud based virtualization environment located at ESEC in Redu, able to perform integration, testing and evaluation of a space system.

2. ACTIVITIES PERFORMED

The activity was carried out in three main steps:

- definition of the satellite and ground architecture and Cyber Range emulation implementation
- development and implementation of the Cyber-attacks tool
- Vulnerability, threats and risk assessment

GomSpace has provided a software emulation corresponding to a part of the components of the GOMX4-B and of the Mission Control Centre, that were relevant for this study.

As shown in Figure 1, the virtual satellite is a series of virtualized Linux environments, running the exact same libraries as those running on the actual satellites. For this activity, the communication between the virtual satellite and the virtual ground station is emulated through a ZMQ bridge, that connects both environments, thus extending the CSP network from the satellite to the ground systems. This bridge is used for both the up and downlink chains of the feeder link and TT&C link.

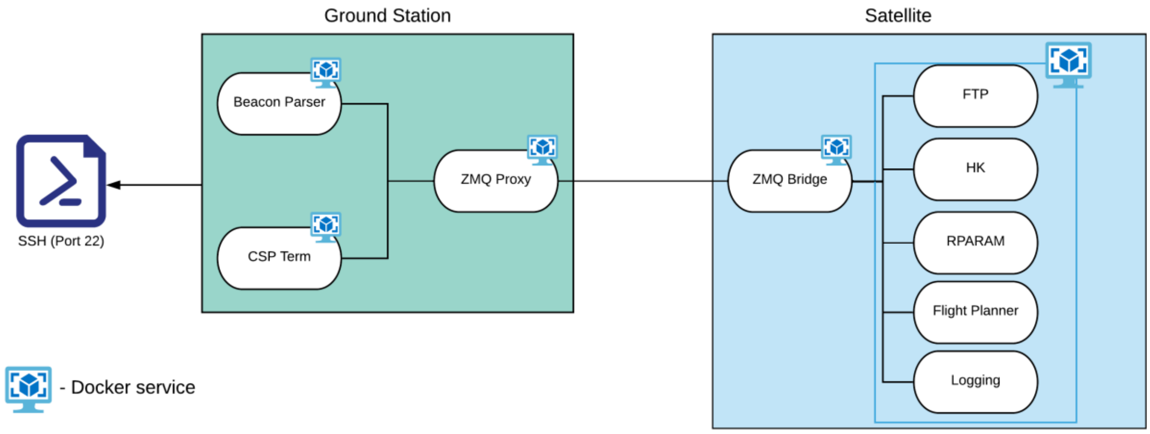

Figure 1 - GOMX-4 representation on virtual systems

The RHEA Cyber Range platform (also referred to in the following as RHEA-CR, shown in Figure 2) enables design and instantiation of complex virtual environments where it will be possible to engage multiple capabilities consistent with advanced cyber range services.

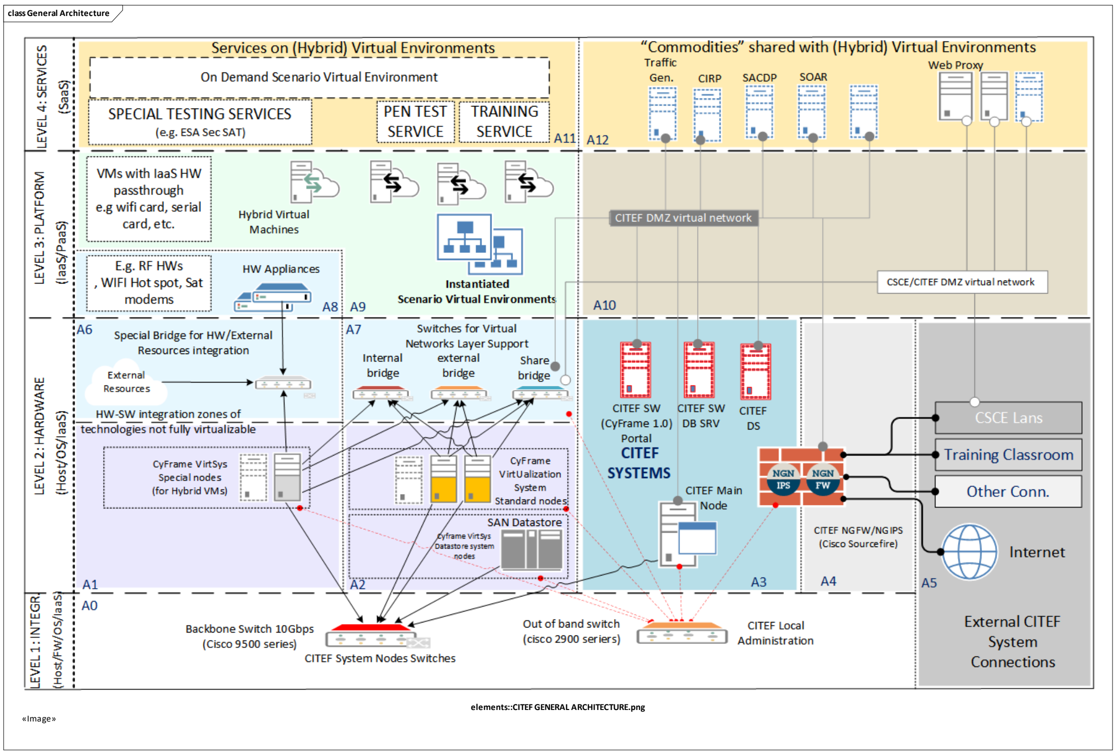
class General Architecture
LEVEL 4: SERVICES (SaaS)
LEVEL 3: PLATFORM (IaaS/PaaS)
LEVEL 2: HARDWARE (Host/OS/IaaS)
LEVEL 1: INTEGR (Host/FW/OS/IaaS)
Services on (Hybrid) Virtual Environments
On Demand Scenario Virtual Environment
SPECIAL TESTING SERVICES
(e.g. ESA Sec SAT)
PEN TEST SERVICE
TRAINING SERVICE
A11
A12
"Commodities" shared with (Hybrid) Virtual Environments
Traffic Gen.
CIRP
SACDP
SOAR
Web Proxy
VMs with IaaS HW passthrough e.g wifi card, serial card, etc.
Hybrid Virtual Machines
E.g. RF HWs , WIFI Hot spot, Sat modems
HW Appliances
A8
A9
Instantiated Scenario Virtual Environments
CITEF DMZ virtual network
CSCE/CITEF DMZ virtual network
A10
A6
Special Bridge for HW/External Resources integration
External Resources
HW-SW integration zones of technologies not fully virtualizable
A7
Switches for Virtual Networks Layer Support
Internal bridge
external bridge
Share bridge
CyFrame VirtSys Special nodes (for Hybrid VMs)
CyFrame VirtUalization System Standard nodes
SAN Datastore
Cyframe VirtSys Datastore system nodes
A1
A2
CITEF SW (CyFrame 1.0) Portal
CITEF SW DB SRV
CITEF DS
CITEF SYSTEMS
CITEF Main Node
A3
NGN IPS
NGN FW
CITEF NGFW/NGIPS (Cisco Sourcefire)
A4
CSCE Lans
Training Classroom
Other Conn.
Internet
A5
External CITEF System Connections
A0
Backbone Switch 10Gbps (Cisco 9500 series)
CITEF System Nodes Switches
Out of band switch (cisco 2900 seriers)
CITEF Local Administration
elements::CITEF GENERAL ARCHITECTURE.png
«Image»

Figure 2- RHEA-CR general architecture

The actual implementation of the emulated GOMX-4B is shown in Figure 3.

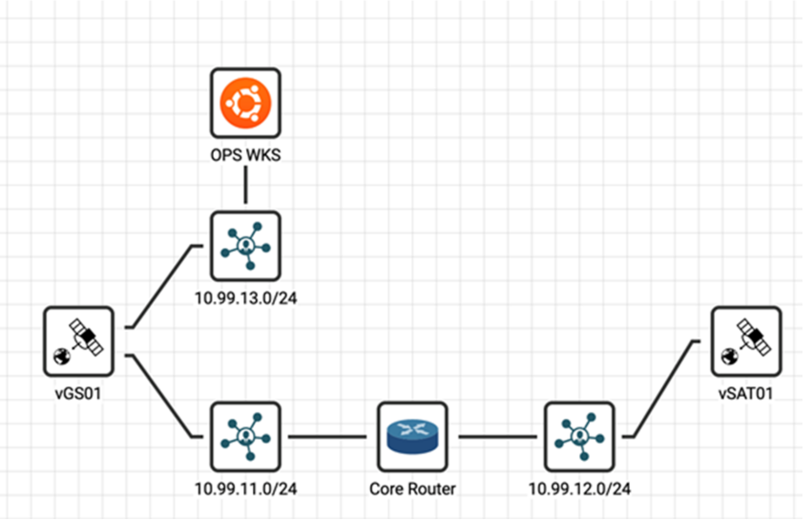

Figure 3 - TRALEO scenario in RHEA Cyber-Range

The emulation consisted in the deployment of the emulated Virtual Satellites (VS) and Virtual Ground Stations (VGS). The VS and VGS run the software from GomSpace, while the communication channels are emulated via Ethernet virtual network confined in the cyber-range infrastructure up to an appropriate level of affinity driven by the associated cyber-attacks simulated.

Figure 3 shows a graphical view of the instantiated scenario, where:

1. The virtual Satellite (vSAT01) and virtual Ground Station (vGS01) are the virtual representation of the GOMX-4B nodes
2. The satellite operator workstation is represented by the node Ops WKS
3. The Networking elements identified by the core router and the IP addresses (10.99.x.y) represents the following links:
    a. the communication link between the Satellite Operator WKS and the satellite vGS01 is implemented by the network element 10.99.13.0/24;
    b. the link between the satellite vSAT01 and the ground station vGS01 is implemented by the items Network 10.99.12.0/24 (interconnecting vSAT to Core Router), Linux host CoreRouter and the Network 10.99.11.0/24 (vGS to Core Router). This link:
        i. implements both TTC link and Feeder link

ii. encapsulates the CSP (Cubesat Space Protocol) used by GOMX4 to implement all communications (between space and ground but also for the intersatellite link).

The preliminary activity was to demonstrate that the emulation of GOMX4-B satellite in the RHEA Cyber Range is representative with respect to the actual orbiting satellite and provides the minimum set of functions necessary to pursue the objectives of the project. A set of acceptance tests were executed on the GOMX4-B satellite emulated to achieve this objective.

The second steps consisted in the development of a series of attacks (including the necessary tools to perform them) against the emulated scenario to investigate on the cyber resilience of small/nanosat space missions.

A set of potential security attacks were identified for satellite systems analysing existing literature and in particular the report “Security threats against space missions” issued by CCSDS (the Consultative Committee for Space Data systems), where a graphical representation of potential attacks to the different part of a satellite is shown in Figure 4

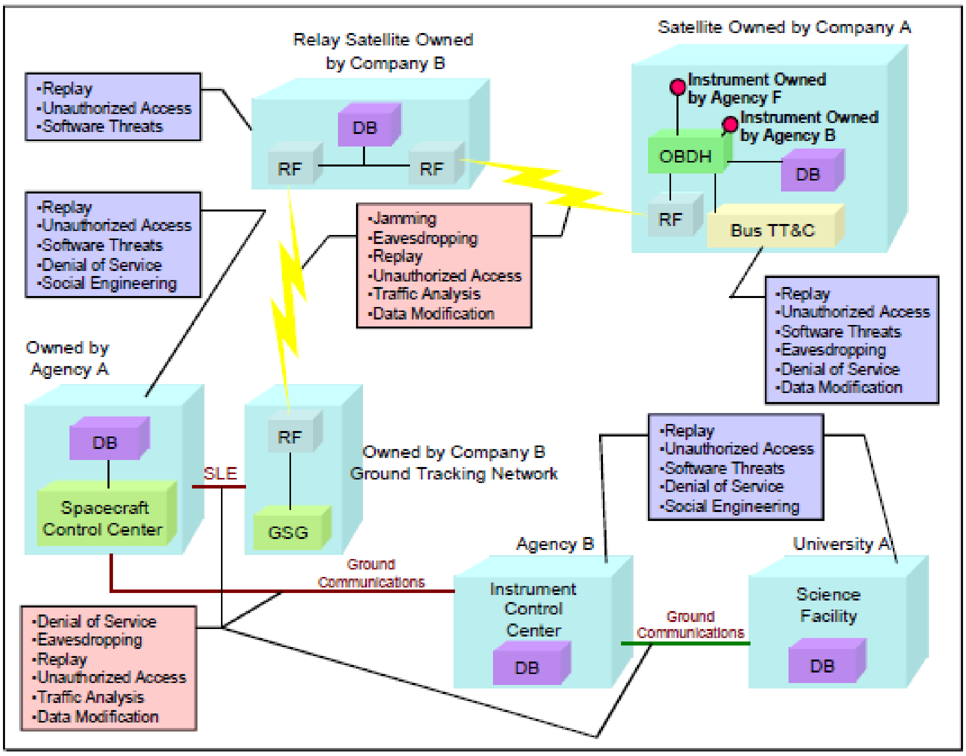

Figure 4 - Security threats against space missions (source: CCSDS 350.1-G2)

For each potential attack, a security test case was defined, with an associated test procedure and success/failure criteria. It must be noted that the test cases are representative of the possible attacks with some limitations due to the test environment and current representations. The attacks for example are carried out at digital level, e.g. analyzing directly the baseband signal and protocol content, not the RF signal. The test results have shown that indeed the current emulation is susceptible to the attacks carried out in the project.

The last step was to complement the analysis on the emulated system with a theorical threats-, vulnerability- and risks assessment of the real system. In this case the analysis was conducted at two levels:

- “as-designed”
- “as-built”.

In the “as-designed” analysis a risk assessment was conducted to identify potential threats that could exploit exposed vulnerabilities affecting the system with negative consequences. In the “as-designed” analysis the real GOMX-4B system is analysed and modelled in terms of assets and associated threats and vulnerabilities. This analysis was carried out leveraging the MEHARI methodology (a European open-source widely known risk assessment methodology, fully compatible with ISO 27001), supported by use of SEST (Secure Engineering Software Tool), a prototype software developed by RHEA for ESA to support risk analysis in ESA programs. The methodology is applicable to satellites of any size. In the case of nanosatellites, the same threats still apply but vulnerabilities related to COTS have to be also considered.

The “as-designed” risk assessment has identified a set of threats that can potentially exploit the satellite system with a high probability to create a serious impact on the system.

In the “as-built” analysis the system was assessed from the technological perspective, analysing the actual hardware and software components used to build the satellite and searching for known technological vulnerabilities. The “as-built” risk assessment has shown that vulnerabilities have already been identified on the hardware and software components used to implement the on-board units and that is actually possible to exploit such vulnerabilities. The details on threats, vulnerabilities and risks are not detailed in this report as they are sensitive information that could be used to provide a detrimental impact to GOMX-4B and GOMSpace.

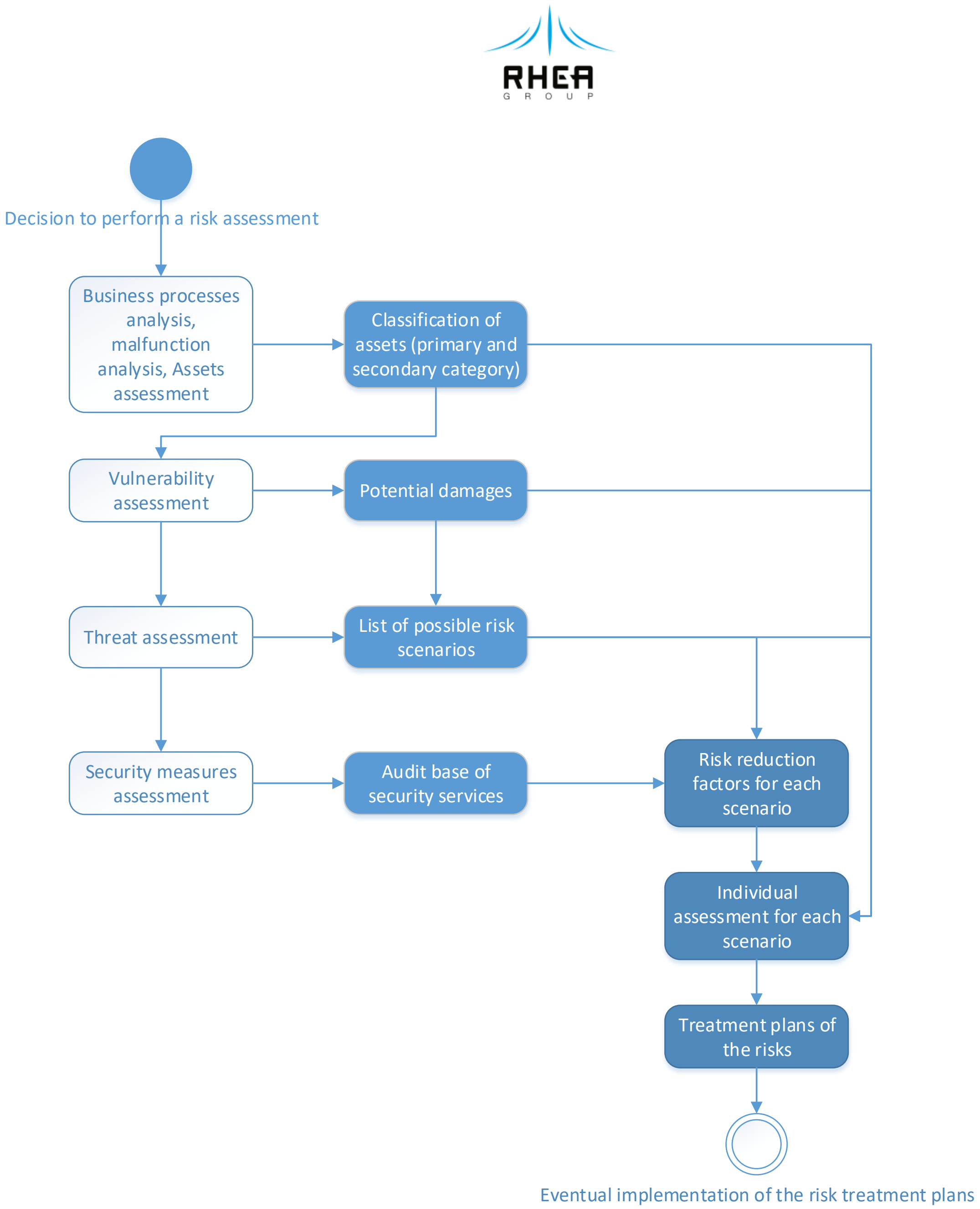
Decision to perform a risk assessment
Business processes analysis, malfunction analysis, Assets assessment
Classification of assets (primary and secondary category)
Vulnerability assessment
Potential damages
Threat assessment
List of possible risk scenarios
Security measures assessment
Audit base of security services
Risk reduction factors for each scenario
Individual assessment for each scenario
Treatment plans of the risks
Eventual implementation of the risk treatment plans

Figure 5 - MEHARI risk assessment procedure

Following the identified risks, a set of potential mitigation measures were identified to counteract the identified issues and mitigate risks. Such measures should be considered from the early stage of the mission requirements definition and completed along the different phases system development and operation lifecycle. The identified measures are described in the next section.

3. RESULTS ACHIEVED

The main result of the activity was to outline a set of recommendations on how to enhance cyber resilience against attacks and threats identified in the course of the work, providing initial treatment against the identified vulnerabilities and security-by-design recommendation for the future satellite constellation robustness. The main ones are reported hereafter.

The first recommendation is to design the system to limit and encrypt the traffic, in particular on the TTC link, but also on the user link. The attack modelling defined by Lockeed-Martin as "Cyber kill chain" (Figure 6) shows that each attack starts with the information gathering phase (also called "reconnaissance"), therefore the first recommendation is avoid spreading information unless it is really needed.

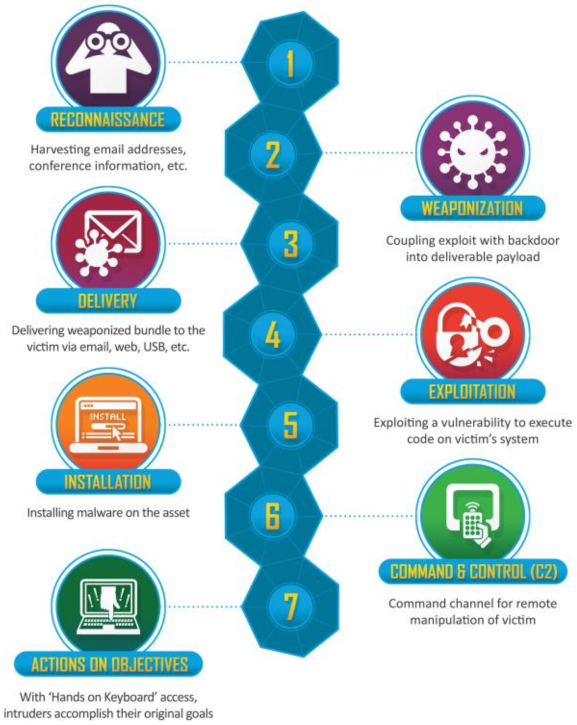
1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Figure 6 – "Cyber kill chain" model (developed by Lockheed Martin)

Encryption can be implemented in several ways: full packet encryption, partial information encryption, electronic signature to authenticate the sender or the receiver or the content.

The second recommendation is to improve the protocol robustness leveraging some mechanism that are already used in the TCP-IP networks like: encrypted checksum, asymmetric bandwidth, windows sizing, session control, etc. it is strongly recommended to review the design of the CSP protocol, like the header length that can be easily saturated, but also the type of commands that are exchanged and introduce additional security controls on critical commands.

The third recommendation is to ensure software maintainability and security patching of the on-board system: COTS used on board of small/nanosat are susceptible of common vulnerabilities, therefore a security maintenance must be granted through proper technical and organization (contractual) measures.

The fourth recommendation is to implement authentication and authorization for privileged users (like satellite operators and system administrators): uncontrolled access to operation systems may allow unintended use or abuse of the satellite system. Every system is now connected to Internet and operational systems are therefore vulnerable as any other system connected to the Internet.

The fifth recommendation is to deploy an online security detection system able to detect potential security events and prevent or contain security incidents. Security measures can be bypassed, sometimes it is only a matter of time (depending on the strength of the implementation of the measure, but the cost and effort are also proportionated to the strength), without being aware of the breach, therefore it is of utmost importance to have in place a detection measure able to identify such breaches. Solution like SIEM (Security Information Event Management System) can also be deployed as a service offered by specialised third parties.

4. CONCLUSIONS

The best application of the results of this work would be to implement a **security-by-design** approach in satellite system development, starting from the mitigation measures identified in this study, in order to increase the cyber resilience.

The key principle in the security-by-design approach is that security is properly:

- Defined
- Implemented
- Operated.

This can be assured using an iterative risk assessment approach along the system design and operation lifecycle that states the need of a control, its correct implementation and its actual effectiveness in counterfeiting security threats. A high level view of the approach is sketched in Figure 7

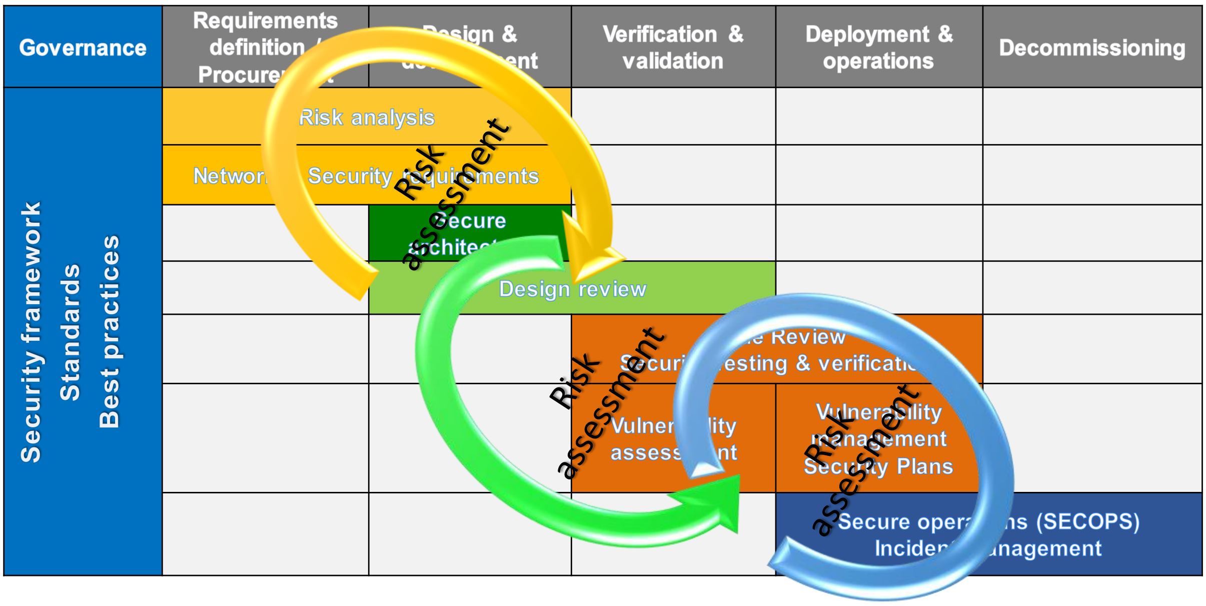

Figure 7 - Security-by-design approach to Space Mission

This approach can be fruitfully implemented to increase the cyber resilience of new nanosat constellations. In particular the use of the risk assessment to drive security measures selection, design, implementation and operations allow to implement the security in a viable manner and suitable to the purpose and objectives of the missions.