OPS-SAT – opening a satellite to the internet

Dominik Marszk[1], José Luís Feiteirinha[2], Benjamin Fischer[3], Daniela Taubert[4], Thorsten Graber[5], André Lofaldli[3], Mehran Sarkarati[3], David Evans[3], Mario Merri[3]

[1] IMS Space Consultancy GmbH
Robert-Bosch-Str. 5, 64293 Darmstadt, Germany
Mail: dominik.marszk@esa.int

[2] Serco GmbH
Robert-Bosch-Str. 5, 64293 Darmstadt, Germany
Mail: jose.luis.feiteirinha@esa.int

[3] European Space Operations Centre
Robert-Bosch-Str. 5, 64293 Darmstadt, Germany
Mail: name.lastname@esa.int

[4] LSE Space GmbH
Robert-Bosch-Str. 5, 64293 Darmstadt, Germany
Mail: daniela.taubert@esa.int

[5] Solenix Deutschland GmbH
Robert-Bosch-Str. 5, 64293 Darmstadt, Germany
Mail: thorsten.graber@esa.int

Abstract: OPS-SAT is a flying hardware and software laboratory in a form of a triple unit CubeSat currently being built by the European Space Agency and scheduled to launch in Q4 2019.
To this date, over 100 entities from 18 countries have registered proposals to fly an experiment on OPS-SAT. To accommodate the needs of all these entities, ESOC offers the experimenters a multitude of access mechanisms to both the ground and space systems of the mission.
In this paper we discuss the safety and security challenges, trade-offs, and lessons learned involved in exposing the ESA ground and space systems over internet to a wider community in an unprecedented scope for the space agency. Finally, we present the OPS-SAT's space and ground segment, focusing on the uniqueness required to reach the presented challenges.

1. INTRODUCTION

1.1. Mission goal

OPS-SAT is a flying hardware and software laboratory in a form of a triple unit CubeSat currently being built by the European Space Agency and scheduled to launch in Q4 2019. The mission's primary goal is to break the "has never flown, therefore it will never fly" cycle. This prevents many ideas from ever reaching the real world environment, as they are deemed too risky, or too expensive to implement and test. In order to achieve this it was necessary to design secure space and ground segments immune to both purposeful and accidental damage. To minimize such risk, we have enclosed all mission subsystems in robust safety mechanisms, allowing the users from around the world to use the satellite for an in-orbit experimentation without risk for the satellite. [1]

1.2. Main mission features

To increase the spectrum of possible applications, the mission includes multiple subsystems representative of a typical spacecraft, plus some novel ones. These subsystems consist of a programmable Satellite Experimental Processing Platform (SEPP – based on a dual core ARM CPU + FPGA), Attitude Determination and Control System (ADCS), GNSS receiver, HD camera, UHF software-defined radio receiver, optical receiver, S-band radio transceiver, X-band transmitter. [1] [2]

To date, over 100 entities from 18 countries have registered experiment proposals to fly on OPS-SAT. These include space agencies, multi-national corporations, universities, and one-man shows. To accommodate such a group of people with very diverse backgrounds, resources, and domains of interest, ESOC offers the experimenters multiple access mechanisms, from remote experiment execution with basic real-time telemetry and telecommanding link forwarding, to higher-level application interfaces such as file uplink and downlink, space-to-ground data mirroring, lightweight web-based monitoring and control system and a user-friendly on-board API wrapping the lower level interfaces.

Furthermore, to ease the process of testing and validation required to qualify the experiment for uplink, we provide scheduled access slots to the satellite's engineering model. Experimenters can also use those access slots to test software, simulate their operations and get acquainted with the operational setting.

2. MISSION DATA SYSTEM INTERFACES

OPS-SAT's requirement from the mission data system is to facilitate a large variety of experiments, wanting to utilize and access the satellite through different links and different layers of the communication stack. In order to meet that requirement, we have developed a set of solutions meant to readily fit the majority of our users.

2.1. Space segment data system

Developing, testing, deploying, and operating the spacecraft On-Board Software (OBSW) is a difficult task due to the extra requirements derived from the uniqueness of the environment and the hardware design, as well as desired reliability. We aim to minimize any extra, repeatable effort spent by the OPS-SAT users in that area. We are going to achieve that through providing the experimenter community with a comprehensive, fully functional reference firmware and software stack running on the SEPP, consisting of:

- reference Altera Cyclone V SoC design,
- baseline configuration and FPGA IP cores handling all of the SEPP interfaces like CAN, I2C, SPI, SpaceWire, radio transceivers bypass,
- embedded Linux system image,
- protocol bridge applications allowing access the CCSDS-compliant data streams on CAN and SpaceWire buses through a TCP socket,
- set of userspace libraries, implementing drivers for all of the payloads connected to the SEPP,
- Nanosat MO Framework (NMF) – a set of Java libraries implementing CCSDS MO Services standards in a form of abstract software components, enabling the users to quickly build experiments as portable applications, already including a simple, service-oriented Monitoring & Control interface; the apps are also executable in a desktop simulation environment. [3][4]

2.2. Ground segment data system

The OPS-SAT ground segment was developed with two major drivers in mind. One was to reuse and innovate as much as possible of the ESA Mission Control System (MICO-

NYS [5]) baseline – a software suite shared not only by ESA missions but also by other major European space industry actors – making it not only the first real-life use of this software for a CubeSat mission, but also the first use of this software together with a space system using CCSDS MO Services instead of ECSS Packet Utilization Standard, also making OPS-SAT mission an early adopter of the latest MICONYS features like CCSDS File Delivery Protocol (CFDP) implementation. Another driver was to meet the already discussed unique requirements of the mission. Keeping that in mind allowed us to create a hybrid ground data system consisting of:

- a fully representative operational network, with the same MCS core (SCOS-2000) as every other ESA mission uses to the day, including bleeding edge features, like CCSDS File Delivery Protocol (CFDP) or support for CCSDS MO Services.
- a set of applications first time demonstrated in OPS-SAT, like Data Proxy, allowing to dynamically switch between different Ground-Space interfaces, NMF Ground MO Proxy, serving as a protocol-bridge and a ground data archive for NMF experiments, or Lightweight MCS, serving as a GUI for the experiment applications developed on top of the NMF.

A high level diagram of the ground and space systems with focus on the experimenter interfaces was demonstrated on the Figure 1. A diagram going into more details of the system was demonstrated on the Figure 2.

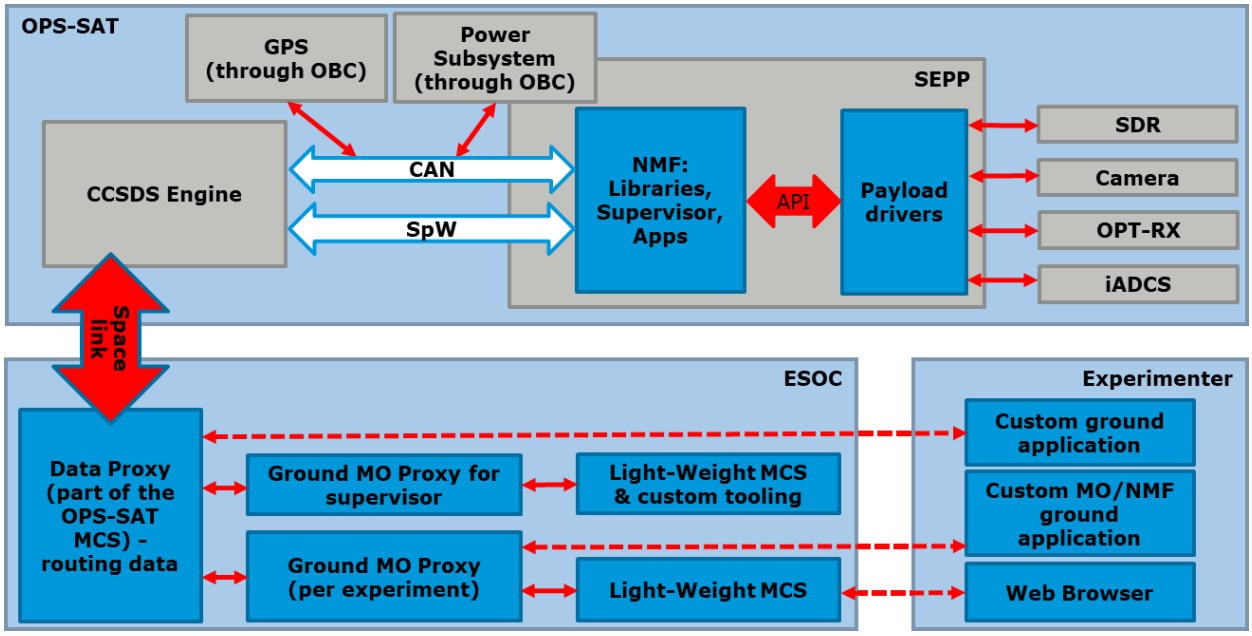

Figure 1 – High level OPS-SAT system diagram from the experimenter perspective

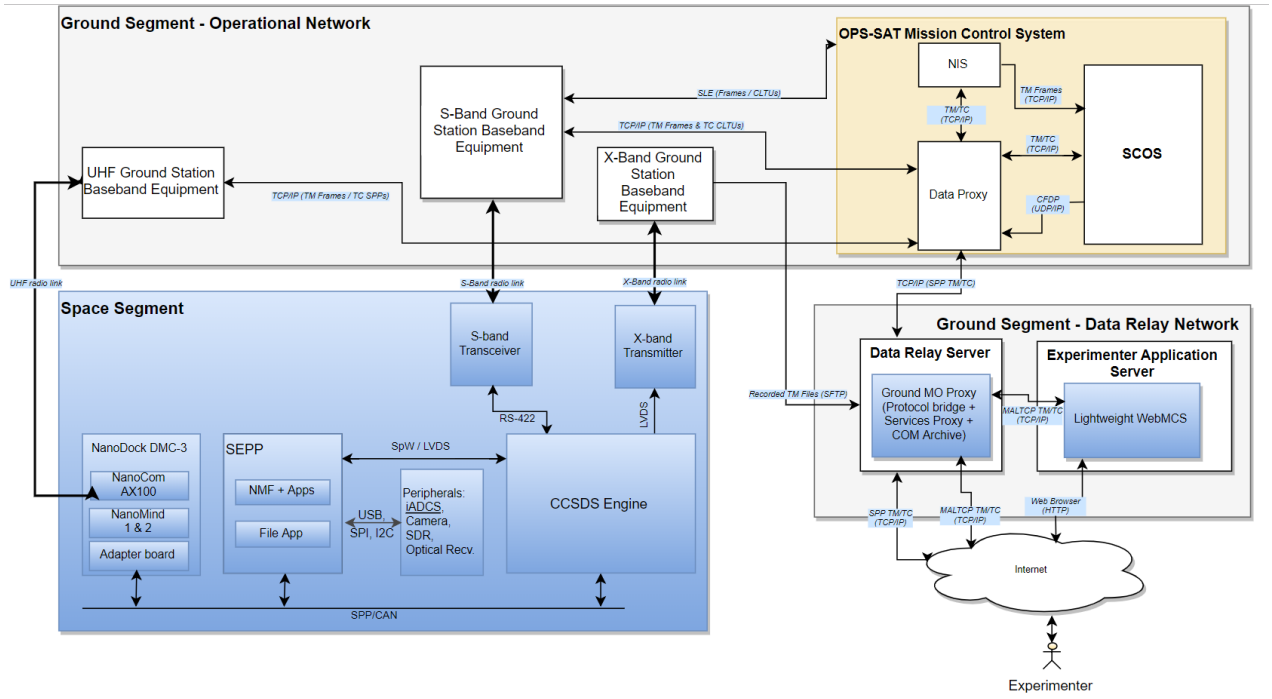

Figure 2 – OPS-SAT data system diagram with focus on the interfaces

3. SECURITY AND SAFETY ASPECTS OF THE MISSION DATA SYSTEMS

3.1. Domain separation and risk assessment

In order to compartmentalise the risk assessment and allow it to be addressed at different levels, the mission subsystems were grouped into a few domains: Data Relay network, Development and Validation Chain network, Operations network, Spacecraft Experimental Payload Platform, and Spacecraft bus, as displayed on the Figure 3.

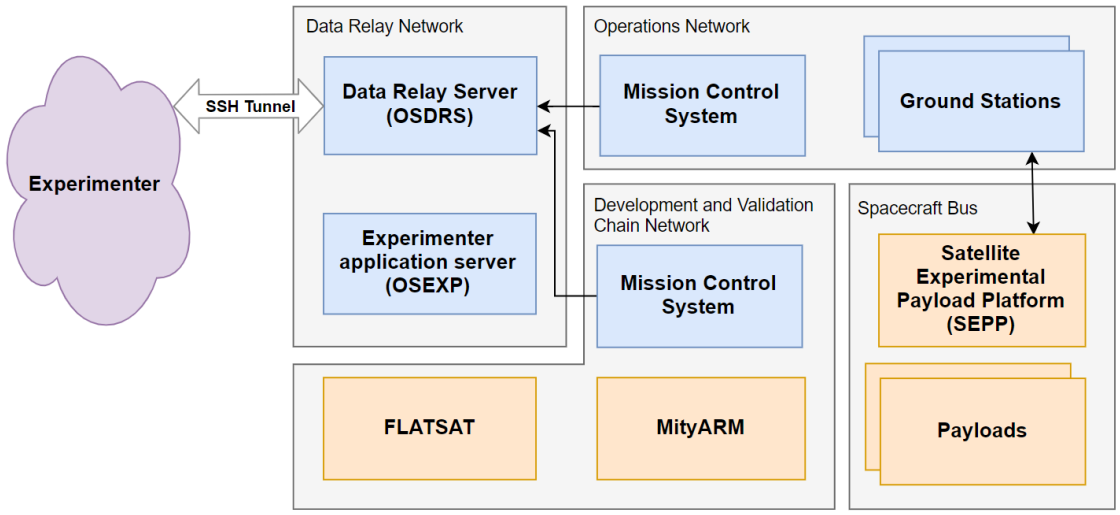

Figure 3 – OPS-SAT security domains separation

Threat and impact in each domain were rudimentarily assessed and given a numeric level, on a scale from 0 to 5 as two main risk factors. The definitions are assumed to be the following:

- **Threat level** is a potential estimated number of events involving external actors trying to access and use the system in a manner they should not. Whether it may be because of a malicious intent, or a lack of proper knowledge.
- **Impact level** is a potential level of damage that can be done from within a particular domain.
- **Risk level** is a measure of the extent to which an entity is threatened by a potential circumstance or an event, calculated as a sum of threat and impact level, resulting with a number on a scale from 0 to 10. [6]

Domain	Threat (T)	Impact (I)	Risk (T+I)
Data Relay network	5	2	7
Development & Validation Chain network	3	3	6
Operational network	0	5	5
SEPP	2	2	4
Spacecraft hardware bus	1	4	5

Table 1 – Risk assessment for different mission domains

3.2. Security and safety measures implemented in the given domains

This subsection outlines the general system design measures taken in order to minimize the security and safety risks for the mission.

All systems have detailed access logging enabled by default, both for user and administrator accounts. Furthermore, a daily backup is performed to data centres distributed over different parts of the agency. This is critical for live monitoring of the system and any eventual post-failure analysis and recovery.

3.2.1. Data Relay network

The data relay network has been assessed to be at the highest risk, as it is the part of the system accessible from the internet. Potential impact on the whole system is rather low, as the Data Relay Server (DRS) is still well separated from the rest of the mission network. Risk mitigation measures include:

- Firewalled access to the DRS with a whitelist of the IP addresses which can access the server.
- Externally audited network configuration.
- Regular reviews of the active accounts on the server.
- Enforcing strong passwords or public-key authentication accessing the server.
- chroot isolation of the users.
- Restriction of binaries executable by the experimenters.

3.2.2. Development and Validation Chain network

The network containing the OPS-SAT Development and Validation chain has been determined to be at a moderately high risk, as the current design will allow automatically scheduled and executed remote access time slots for the registered experimenters. Po-

tential impact is average, as the satellite's engineering model could be damaged by an improperly designed or malicious experiment. Risk mitigation measures include:

- Manual pre-screening of the experimenters and the experiment designs before granting them an access and execution rights on the validation chain.
- Distinguishing between different types of experiments, requiring different access levels to the system.
- Monitoring of the validation chain by an external hardware. The monitoring hardware could shut down the experiment in case of an abnormal behaviour, possibly restricting the execution rights to the user until a manual review by a mission engineer.

3.2.3. Operational network

The risk to the operational network is moderate. Although the threat has been determined to be very low (as the network is well isolated and invisible to the external actors), the potential impact to the mission could be very high as any external actor accessing the Mission Control System could control and damage the spacecraft using easily understandable interfaces. Risk mitigation measures include:

- Complete separation of the mission operational LAN from any other networks and missions operated by ESA.
- Password protected access to all operational machines and to the Mission Control System software.
- Disallowing any incoming connection to the operational network by design. Any kind of data transfer, including relaying of the experimenter data, has to be initiated from the inside.

3.2.4. Satellite Experimental Payload Platform (SEPP)

The risk to the SEPP is rather low, as the typical experiment will have restricted execution rights within the system. Safety measures include:

- Mandatory successful execution of the experiment in the development and validation chain prior to granting an authorization for executing the experiment in space.
- Isolation of the experiments through restricting access to the hardware interfaces of the SEPP by using mechanisms provided by the Linux Kernel and additional modules like *SELinux* or *iptables owner*. [7]
- Requirement to package the experiments on ESA side (by an automated system).
- Wrapping the payload devices drivers into an API enabling remote calls, allowing a complete separation of many experiments from the hardware interfaces.

3.2.5. Spacecraft hardware bus

The risk in the domain of the spacecraft bus is moderate. The potential threat has been determined to be low. The potential impact is high, as having a sufficient level of knowledge, a malicious user could control or damage the spacecraft hardware. Additionally, an improper software implementation could also cause a loss of the control over the satellite and a damage to the hardware. Risk mitigation measures include:

- Providing a well-tested set of drivers implementing the satellite payload interfaces.

- Granting a privileged user access to the SEPP (and therefore the satellite bus) on a basis of an exception requiring a proper justification.
- Reviewing the privileged experiments with an extra scrutiny.
- Requirement to perform project build and packaging on ESA side.
- Automatic cyclic resets of the satellite hardware.

4. CONCLUSION

The OPS-SAT project is a mission posing a multitude of unique challenges not yet tackled in such depth by any previous ESA project. One of the principles guiding the design decisions of various safety and security mechanisms of the innermost systems of the mission is Hanlon's Razor – a user having an access to a particular mission subsystem is much more likely to cause a damage without intending it, than to have evil intentions. The concrete experience derived from the ground and space system design, implementation, and operations is going to provide a foundations for any future project posed with a similar set of challenges. Such projects are expected to become more common now, as the space industry is experiencing the next stage of commercialization and integration with other industries, technologies, and on-line services.

5. REFERENCES

[1] D. Evans and A. Lange, OPS-SAT: Operational Concept for ESA'S First Mission Dedicated to Operational Technology, SpaceOps 2016 conference

[2] OPS-SAT – eoPortal Satellite Missions Directory: https://directory.eoportal.org/web/eoportal/satellite-missions/o/ops-sat (accessed January 2019)

[3] C. Coelho, O. Koudelka, M. Merri, NanoSat MO framework: When OBSW turns into apps, 2017 IEEE Aerospace Conference (2017)

[4] C. Coelho, A Software Framework for Nanosatellites based on CCSDS Mission Operations Services with Reference Implementation for ESA's OPS-SAT Mission (2017)

[5] ESA, MICONYS software suite: https://www.esa.int/Our_Activities/Operations/gse/MICONYS (accessed April 2019)

[6] National Institute of Standards and Technology, Guide for Conducting Risk Assessments, NIST Special Publication 800-30 Revision 1, 15-16 (2012)

[7] Stephen Smalley, Configuring the SELinux Policy, National Security Agency (2005)