17th International Conference on Space Operations, Dubai, United Arab Emirates, 6 - 10 March 2023.

SpaceOps-2023, ID # 112

THE DESIGN OF THE SAFETY OPERATING CENTER TO MANAGE CYBERSECURITY OF THE SPACE MISSIONS

Jamel Metmati

[a] *Department of Cyber,* djamel.metmati@thalesgroup.com

Abstract

The cybersecurity in Space introduces methodology for the design and the accreditation of Space networks. Indeed, the process management on the ground uses the satellites support for the business purposes and the economic development. The operational procedure management requires the science of Computer in Space in which the Space networks shall integrate cybersecurity management. The monitoring of data from Space can adopt security operating center. Nevertheless, to complete the features of Space networks, the approach of Safety Operating Center appears suitable to cover the requirements of cybersecurity in Space. The reliability, availability, maintainability, safety methodology describes the information cycle in the engineering process in Space missions. Based on this methodology and completed by new entries, the safety operating center should be built to cover the requirements to manage the Space networks. The security information event management applicable for this center takes into account the features of the safety in Space. It concerns the satellites as KhalifaSat, as DubaiSat-1, DubaiSat-2 and the Mars Mission Hope. The effects of these operations procedures management is also applicable for the data dissemination for the customer and the business development. As the integrated system marks the trends of information and communication networks, the design of safety operating center shall be considered in the cybersecurity management.

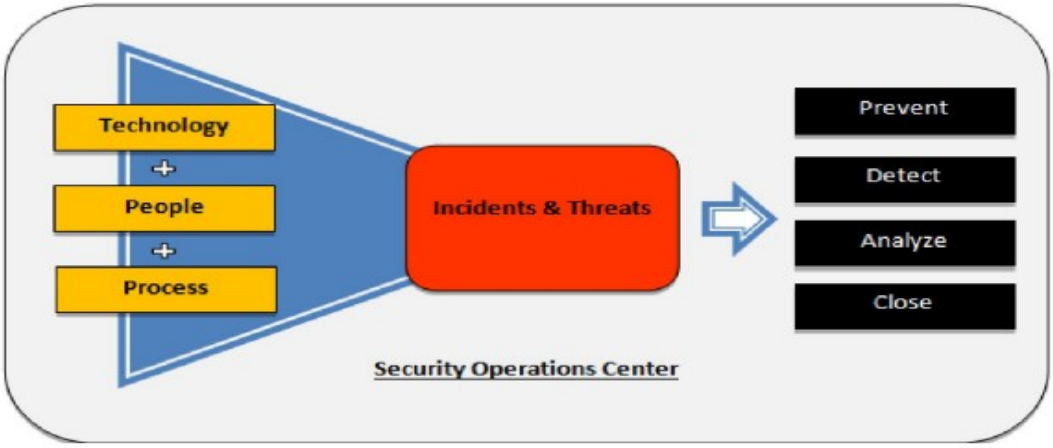
Keywords : safety, space missions, cybersecurity, networks

1-Introduction

The objectives of this work is the get the overview of the design a center to manage data flow in Space in the context of more dynamic flow due to the connectivity increasing on Earth orbit.

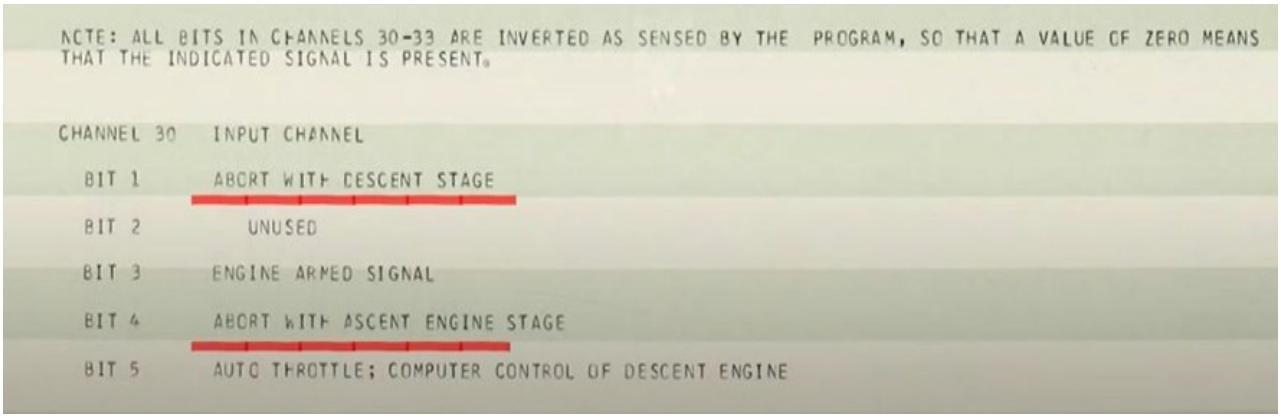
2-Methods

The key benefit of having a security operations center is the improvement of security incident detection through continuous monitoring and analysis of data activity. By analyzing this activity across an organization's networks, endpoints, servers, databases and critical infra around the clock. The 24/7 monitoring provided by a CSOC gives organizations an advantage to defend against incidents and intrusions, regardless of source, time of day, or attack type. The method is to add the safety approach at the security operations center described on the figure on below.



3-Results

The Test scenario is to perform and secure guidance computer in Space [1]. This scenario development applies to the sofware management of the computer errors guidance computer for command and lunar module Apollo 11 [4].Thanks to the Raspberry Pi running Virtual AGC with Nextion 4.3 LCD, the software is able to be replay and re-tested bit by bit for the command and control. For example,on the figure on below, show the bits allocation for the computer : bit 1 for the abort for descent stage and bit 4 for the abort for ascent engine stage.



The point is, at the final approach on the Lunar surface, was the flight software generated alarms.This status pushs Neil Amstrong to take back the commands manually without the automatic computer instructions.

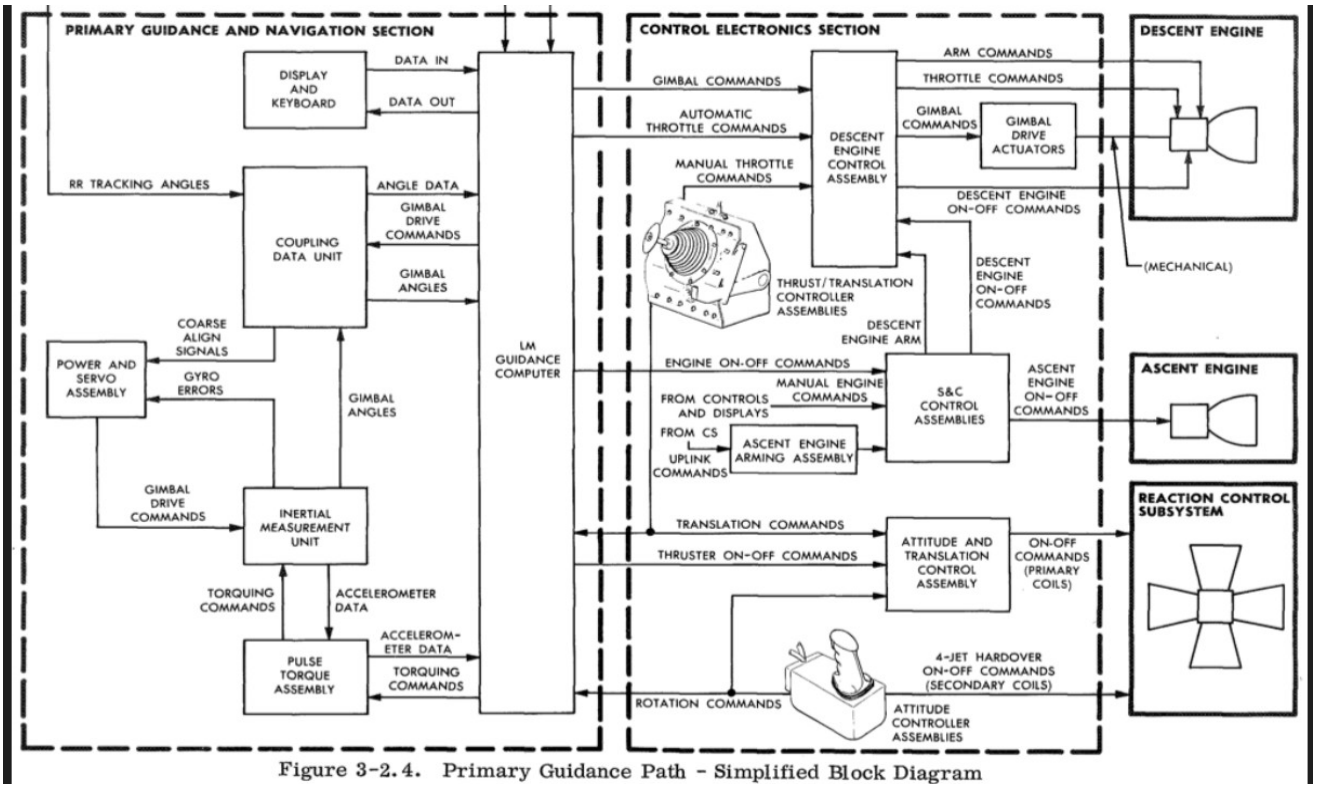


Figure 3-2.4. Primary Guidance Path - Simplified Block Diagram

The design of software included some weakness to be hack by the own system itself because we can not manage all instructions. The software worked from hardware support following : 6 tasks on parallel, 16 bits memory including 72Ko ROM memory with programs for navigation, guidance and control, 4Ko memory for the process, 12 micros clock speed, 70 Watts battery. The programs shared CPU cycles, then an executive program manage all of them. The point is the process used in software development in the rush on the moon : specification, formulation, design, coding, testing, documentation. The steps were not sequential because of the changes requirement and the ability to do the job in a harsh context. The software needed 750 program requests and the coding result in 2000 lines. Despite of design providing flexibility in the program execution the software behaviour was overwhelmed. And the computer was out of core sets provoking the 1201 and 1202 program alarms with manually approach.

The test scenario is to perform and secure flight sofware on Mars. This scenario development applies to the flight software for a chopper drone in the Mars condition. It integrates the parameters unknown on Earth from the open source framework F Prime tested in CubeSat in Space : Asteria, Lunar flashlight, NEAScout.

Stage 1: Concept Software components
The purpose is to give a rapid solution to develop the software functionalities thanks to the specific module. Each component (1,2,3) gets a behaviour as the telemetry, the interfaces, the command and control whereas the port 1 and the port, 2 allow the data interconnection. The UART interface offers a communication path between the component instances.

Stage 2: Re-use Architecture components
The purpose is to maintain the software life as longer as possible where each module can survive in the case of failure from another module. The set of Space processor families come from the X86, PPC, ARM, MSP430, Leon3. The fiability is the main criteria to implement it on the Spacecraft. And the language is multiple as C++, python or others. The library and the functionalities determine the language choice.

Stage 3: Coding
The purpose is to code the components with secure implementation without call of functions from another module. The coding is based on two deployment, one for the Qualcomm processor running on Linux and the others using ground support equipment like XTCE dictionaries and others framework (OpenMCT, ZMQ Radio) directly to the micro-controller exposed to the hack of Mars environnment (radiation, bit flip effect on the binary packets).

Stage 4: Test components
The purpose is to test, one by one, the components of the architecture with the same number of components. The Coverity scan analyzes the code in each components. The signal life expectancy from a module must be transmitted as longer as possible for the ground station to collect data. And the autonomy of chopper must be guaranteed by on board sequences through the list of scripts for the decision making : set of commands, set of conditions, set of events impacts like a restart or new command. The Space sofware development is now going in process for the micro and nano-satellite for mass market applications to the ground. It follows the exploitation of computer in Space through the private compagnies to agile development : small team, short schedule, reduced budget, piggylaunch, best effort and simplified verification and validation cycle. Instead of beginning from scratch, the use of proven framework to serve as design is a way to the New Space software development.
There needs to be a collection of recommendations [3] related to:
(1) Risk-based, cybersecurity-informed engineering, including continuous monitoring and resiliency.
(2) Planning for retention or recovery of positive control of commercial satellite systems in the event of a cybersecurity incident.
(3) Protection against unauthorized access to vital commercial satellite system functions.
(4) Physical protection measures designed to reduce the vulnerabilities of a commercial satellite system's command, control, and telemetry receiver systems.
(5) Protection against jamming and spoofing.
(6) Security against threats throughout a commercial satellite system's mission lifetime.
(7) Management of supply chain risks that affect the cybersecurity of commercial satellite systems.

(8) Protection against vulnerabilities posed by ownership of commercial satellite systems or commercial satellite system companies by foreign entities.
(9) Protection against vulnerabilities posed by locating physical infrastructure, such as satellite ground control systems, in foreign countries.
(10) Any other recommendations to ensure the confidentiality, availability, and integrity of data residing on or in transit through commercial satellite systems. In concert with the recommendations above, these recommendations should help refine existing cybersecurity frameworks that can be adopted by industry and implemented into regulations.

4-Discussion

4.1- Computer In Space

The computers have become part of the fabric of Space agencies and aerospace contractors which use the computerised machine tools [2]. Computing power to perform the tasks that define a spacecraft - getting out of the atmosphere, and staying on orbit, moving in Space, moving on the ground on Mars and on the Moon. The maneuvers are realised through automatic maneuver or by the radio from Earth. To understand the Computer In Space, it shall considered the evolution of the systems in Space sector. NASA's Mercury capsules of the early 1960s had no computers at all. For re-entry, retro-rocket timing and attitude information was radioed to the spacecraft from a tapes-and-teletypes computer centre on the ground. Then, Gemini capsules had their own computer capable of seven thousand instructions per second, to support the rendez-vous operations. And the Apollo system computer prototypes consumed two-thirds of the world's total supply of integrated circuits. The ISS is packed with processors. The core of its operational hardware are the Command and Control Computers. It marked by the core 80386SX-20s, and 80387 co-processors. The Space Shuttles were originally equipped with five parallel redundant IBM AP-101 general-purpose computers.
Each of those was equipped with a mighty 1,310,720 bits of ferrite core memory (more had to be tacked on to accommodate the elephantine 700-kilobyte size of the Shuttle's control software...), and was good for a neck-snapping 0.48 MIPS and 0.325 MFLOPS. Magnetic core memory is still used in mission-critical space computing applications, because it's radiation-proof and non-volatile. a major upgrade in 1991.
Since it running the AP-101S three times as fast as the AP-101. The hardware shall be able to survive the vibration and G-forces of launching, but a laptop can do that with a bit of padding. On the contrary, the vacuum gets some consequences on the work flow of the computer. An PC or laptop won't work at all in vacuum for the hard drive heads need an air cushion to float on. Hard drives have a maximum operating altitude rating of about 2500 metres, meaning they don't like pressure much below 11 pounds per square inch (psi). Normal sea level atmospheric pressure is 14.7psi, but many manned spacecraft use lower air pressure. Many normal computer components will overheat without air flow to cool them; purely radiative cooling is a lot less effective than even passive convection.
The hardware must bear the "cosmic ray strike". Some high-energy particle from a supernova millions of years ago whizzes through the vacuum, whacks into a RAM chip, and either it or the spray of secondary radiation from its impact flips one or more bits in the memory. If error detection and/or correction doesn't repair the damage. Space computers also have to deal with the sun's "solar wind", which is composed of electrons, protons (hydrogen nuclei), and small doses of heavier nuclei. The solar wind sleets out from the star all the time, though it's stronger when there's lots of sunspot or solar flare activity. For more critical systems, spacecraft use special radiation-hardened versions of current CMOS chips. The hardening can be achieved by something as simple as reducing the transistor density, or they stick with good old bipolar transistor technology, which is inherently much less radiation-sensitive. A radiation-hardened 80C85 (the CMOS version of the Intel 8085) did the thinking for the Sojourner rover on Mars. The Pathfinder lander and the later Spirit and Opportunity rovers use the popular RAD6000, which is a hardened version of the 25-MIPS IBM POWER chip that came before the PowerPC.
The software used in the computer can be instructions, can be updated from the ground, offers complex tasks at the distance. The Space segment uses the ground technology for the embedded system on the probe, on the Station, and on the first robots on the Moon and Mars. Except the Space environment changes the way to design and manage the life cycle of the software through : Power involves the batteries from solar panel with the no linear energy, Radiations and the gravity involves to protect the componements of software support by rad hard structure against the memories effects breaking the telecommunication link. The Earth gravity equal to 9,81 m/s² and that of Mars is worth 3,71 m/s², The errors management involves to be able to correct the computing errors of software in the case of memory trouble.
The approach of Space software are divided into three contexts : the rad hard components uses the major Spacecraft like the guidance computer for command and lunar module, the far approach uses by the first drone outer the Earth

by the Inguinety Chopper on Mars with its flight software, the New Space approach uses for the low cost mission with new satellite generation as nano and micro satelllite.
The life cycle of Space software gets both the ground segment and the Space one. The case studied concerns the real time software embedded in Spacecraft systems and payloads. The software defines itself as sets of instructions that tell system what to do in given situation. And several methods exist to reach the purpose of the development to the prototype : Waterfall, iterative, Spiral, V-model, Big bang, RAD. Space requirements need to combine these methods due to the New Space context. It means the software is the intelligence of the Space system.
To protect it for any internal and external process, this intelligence is to be secured at each steps of its development, for the software must be autonomous and be able to be associated with others programs of the Spacecraft.
The internal process is linked with the capacity to the software to work despite of the errors recorded in the volume of instructions produced. And the external process translates all command and control instructions to the software despite of the effects of the Space meteorology in Space as the charged particles to the signal transmission inside the hardware system. Following the operational examples of Apollo 11, the chopper Inguinety on Mars and the computer in Space for low cost mission like Raspberry Pi in New Space, secure software in Space integrates test and validation procedure with strong datasets in back office in the ground segment. And from the Apollo 11 to new spacecraft on orbit or in deep Space, the software in Space must manage more complex datasets associated with multiple programs with the need to be on times and the budget requirements. The flight software are also deployed on the assets in Space. The F-Prime, a free, open-source flight software framework developed at JPL and tailored to small-scale systems such as CubeSats, SmallSats, and instruments. F Prime comprises an architecture that decomposes flight software into discrete components with well-defined interfaces; a C++ framework that provides core capabilities such as message queues and threads; tools for specifying components and connections and automatically generating code; a growing collection of ready-to-use components; and tools for testing flight software at the unit and integration levels.

The basic challenge of space is remoteness through the ground station and the signal management through different types of modulation. The use case of LunaNet is defined as a telecommunications network capable of supporting human exploration and scientific missions to the Moon. The first building blocks of the telecommunications system will be nodes for lunar deployment and the first permanent installations. The features of this network combine a set of interoperable systems with government and commercial partners. And the aim of the system is to support the Artemis III, Artemis IV, Artemis V and commercial missions involved in the IOC and EOC phase. The structure of the LunaNet network is a first in human space exploration as it lays the foundation for interplanetary communications for the presence of human civilisation outside Earth. The LunaNet design encompasses all systems providing time, navigation, and communications services to users around the Moon and to Earth. In other words, the network equipment will be located both in lunar orbit and on the surface of the Moon. For the lunar segment, a specific chain is envisaged for which an interface could be implemented to the ground segments of the Earth. A relay system between the two segments is being studied in which the exchange configuration would be based on a private link. To establish the link between the two segments, the LunaNet will be built through a combination of LunaNet access providers who will themselves be service providers.
The interfaces between the segments can be divided into several categories.The first includes the physical interfaces and protocols between a user and a provider. The second concerns the interfaces between different access providers. The declination of interfaces is then divided into a series of connections involving typologies of interfaces: linkage between the lunar and terrestrial system, linkage between lunar surface users, linkage between surface users and those in lunar and terrestrial orbit, linkage between service providers according to linkage use cases. Permanent data transmission is achieved through a communication in space and a link from the lunar ground. Users will be able to establish communications through these two channels according to known standards and protocols. Thus, the Internet protocol could join the Bundle protocol in the Consultative Committee on Space Data Standards, the Advanced Orbiting Systems, and the IETF.
This Space Internet is based on three space telecommunication characteristics: real time, time shifting, and service messages. The applications supporting this transmission chain are related to alerts, Position Navigation Times, and service acquisition. Thus, the LunaSAR service corresponds to the Search and Rescue signal of the navigation satellite constellations constellations in Earth orbit. This service offers the ability to monitor the distress signal from any equipment and infrastructure on the Moon. Other services include space weather monitoring and the use of optical and radio links for measurement missions from Earth. Together, this creates an inter-planetary architecture in which Earth-Moon telecommunications use X, Ka, or optical bands to connect to relay nodes in lunar orbit. These nodes, connected to each other with a complementary band[5] communicate with spacecraft in lunar orbit and entities

on the surface of the Moon. The existing ground stations will transmit and receive the lunar signal from the constellation of navigation satellites. This means that terrestrial infrastructures will have to be able to supervise and monitor the state of the network by taking into account new parameters. These include the ability to manage integrated architectures with different systems and protocols, to understand the effect of the space environment on signal processing, to ensure signal availability within acceptable performance times for crews in orbit and on the lunar surface. To this end, in these network monitoring missions, the characteristics of the ground segment include a novel and complex incident response. However, the main points can be seen from the point of view of the current operation of the control centres of navigation systems or ground observatories.The case of the Entoto observatory demonstrates how LunaNet could fit into this signal supervision posture. The optical telescope of this observatory is connected to a command and control unit based on a navigation system. This same unit is connected to several interfaces based on a client-server relationship to users, external entities and a data-center for the backup link. The dome, the telescope, and the weather station rely on this client-server relationship through a software interface. The network must ensure the continuity of the system to fulfil the functions of the following segments: user interface for monitoring and tracking, for the data management system, for the telescope, for the control and command module. While these separate services are interdependent, they share the same architecture for the optical sensors, the active network elements and the software process. In the event that this process is no longer available, the Kenyan space agency would lose the ability to connect to the LunaNet segment. The chain of transmissions to the Moon therefore requires a novel application of operational cyber security concepts. This is especially true given that security is linked to the widespread introduction of digital techniques in the operation of spacecraft and telecommunications.

4.2- SIEM for the safety information event management

The safety operating center means the capacity to operate data to ensure the operational capacity of Space activities. It includes the requirement of RAMs and Cyber framework. The organization model of SOC is based on the architecture already used for the rocket launch and the missions in Space. The specificity of the SOC is the capacity to ensure with the data transmission and the data dissemination on the ground segment for the external entities. A security operations center (CSOC) is a facility that houses an information security team responsible for monitoring and analyzing an organization's security posture on an ongoing basis.

The art of statement of frameworks of Cybersecurity shall provide the specificities of computer in Space connected with the use of the ground. As the connectivity is going to improve thanks to the number of assets on orbits, the requirements should be completed by the introduction of Safety Information Event Management for the software and networks components. In July 2022, NIST issued a white paper entitled "Cybersecurity Profile for the Hybrid Satellite Networks (HSN) Cybersecurity: Draft Annotated Outline" ("HSN White Paper").

The HSN White Paper focused on hybrid satellite network systems that provide services such as satellite-based communications systems; position, navigation, and timing (PNT); remote sensing; weather monitoring; and, imaging. In addition, NIST published the "Introduction to Cybersecurity for Commercial Satellite Operations" which provides guidance to space actors on implementation of a cybersecurity framework in space operations. NIST also has held symposiums on space cybersecurity.

Legislation In the United States Congress, increased awareness of cyber vulnerabilities in the space sector prompted hearings and legislation. In 2022, legislation has been introduced in both the House of Representatives and Senate that would create a Commercial Satellite System Cybersecurity Clearinghouse tasked with providing cybersecurity resources online and the collection of recommendations. Additional legislation has been introduced in the United States Senate seeking voluntary recommendations from the Cybersecurity and Information Security Agency (CISA) within the Department of Homeland Security on the "development, maintenance, and operation of commercial satellite systems.

While best practices from NIST and other governmental agencies provide guidance, they do not secure compliance. Consequently, there needs to be the regulatory implementation of recommended cybersecurity frameworks. Should the FCC continue to believe it may not be the best agency to develop cybersecurity regulations, it certainly would be the best agency to require space station operators implement cybersecurity practices. As to the development, it can merely require that space station operators implement the then-current cybersecurity framework issued by NIST. Similarly, within the United States, the Federal Aviation Administration (FAA) can compel launch license applicants to demonstrate compliance with the applicable cybersecurity framework. And so, this same requirement can be implemented throughout domestic agencies in all space-faring nations. In the absence of immediate regulatory obligations, all entities engaged in space operations should adopt practices that implement a cybersecurity framework. At a minimum, these practices should include: Reviewing and Adopting Practices

Conclusion :

Companies in the space sector must embrace implementation of cybersecurity technology in the design phase of their space missions. As Germany has recognized: Satellite systems must meet stringent security requirements throughout their entire lifecycle. Aspects relevant to cyber security should be explicitly addressed early on in the design and development phases of control centres, receivers, connections and satellites [because of the] unusually long useful lives or satellites and the extreme operating conditions in space [that] require highly specialized IT security architecture[and only] limited adjustments and adaptations [can be made] to the IT security architecture once [orbital].

References

Reference to a journal publication:

[1] M. Manulis et al. "Cyber Security in New Space". In: *International Journal of Information Security* (May 12, 2020).

Reference to a conference/congress paper:

[2] Svetlana Hansonb, Charles Lee Mudd Jr.a, Cybersecurity in Space: Ensuring A Secure Space at the Operational System Level, 73rd International Astronautical Congress (IAC), Paris, France, 18-22 September 2022. Page 1 of 7.

Reference to a book:

[3] International Cyber Incidents: Legal Considerations. Tikk, E., Kaska, K., & Vihul, L. In: CCD COE Publications, 2010. Services, I. L., *KA-SAT Mission Overview*, 2010.

[4] Christopher Riley et Philip Dolling, NASA Mission AS-506 Apollo 11 Owner's Workshop Manual: 1969 (including Saturn V, CM-107, SM-107, LM-5). 21 mai 2019.

Reference to a website:

https://www.ftc.gov/business-guidance/smallbusinesses/cybersecurity/basics
https://www.orbitaltransports.com
https://github.com/nasa/fprime
https://www.nist.gov/cyberframework