2025-10-23

WHITEPAPER

Knockin’ on Space’s Door

PRESENTED BY:

Alberto Volpatto - Anvil Secure

Davide Avanzi - D-Orbit

Anvil Secure

2125 Western Ave Suite 208

Seattle, WA 98121

United States of America

+1 206.753.7649

info@anvilsecure.com

Table of Contents

Introduction

Anvil Secure and D-Orbit security started a collaboration aimed at the application of cyber security principles to the space ecosystem, with particular focus on the satellites and their systems, and to understand the status and identify research opportunities introduced by the new space landscape.

The purpose of this white paper is to provide an overview of the main potential cyber security threats that might impact products of private satellite manufacturers, focusing exclusively on the areas directly related to the space vehicle and its operations. Systems and flows that are part of the ecosystem, such as ground stations, Cloud and IT infrastructure, and third-party services are excluded from the review as they might not be actionable by manufacturers like D-Orbit.

This work targeted D-Orbit's ION SCV spacecraft and its mission lifecycle which could differ from products and solutions offered by other companies. Therefore, while the general concepts and the approach could be applied to multiple contexts, some information may not be an exact match and could require ad-hoc review and analysis.

Any confidential and / or proprietary information has been omitted from this work.

The Context

The Space System

To set the foundation and provide information for understanding the topic, we must first provide a general overview of what a space system is and how it works. The most basic example consists of a device on the ground that transmits to and / or receives from a device in space that is transmitting and / or receiving. We will refer to the device on the ground as *ground station* and the one in space as *space vehicle*, regardless of its size, purpose and capabilities.

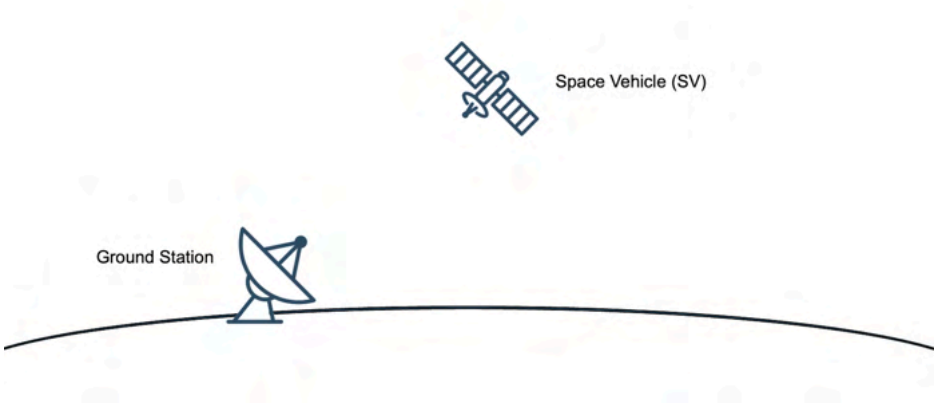

Figure 1: The Space System

Data transmission is generally performed through *radio* signals. Both space vehicles and ground stations are equipped with antennas and *Software Defined Radio* (SDR) devices that perform encoding and digital-to-analog conversion (and vice versa). Modern SDR are capable of encrypting and decrypting data on the fly with standard cypher suites like AES-256-GCM for improved security. Some examples are:

- Satlab SRS-4
- EnduroSat S-Band Transceiver
- SkyLabs NANOlink

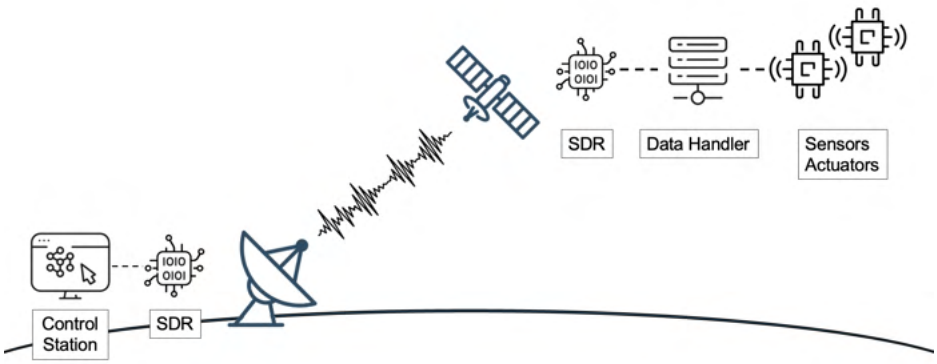

Figure 2: The Space System (2)

While almost all commercial ground-to-space communications are made via radio signals, there exist *optical ground stations* that use lasers for high-speed bi-directional data communications. However, this technology is still relatively new and it is not yet widely available even though some companies and providers are actively working on it (KSAT - Optical Communications, SSC - Optical technology revolutionizing space communications, Cailabs - Optical Ground Stations).

To communicate with a space vehicle, a ground station must know its orbital elements and the uplink / downlink frequencies to properly point the *directional antenna* - if equipped - to the *space vehicle*, and establish the communication during the *passing time* of the space vehicle, which varies depending on its *orbit*.

> *An orbit is the curved path that an object in space (like a star, planet, moon, asteroid or spacecraft) follows around another object due to gravity.*

In some instances, the communication windows where a space vehicle is in view of a ground station can be very short. Tasking the space vehicle and its payloads may require multiple connections, and the waiting times between passages could not be acceptable as per the *mission* requirements. In addition, weather conditions may affect the link between ground and space, introducing further delays. To overcome such challenges, *multiple ground stations* are distributed on the planet and interconnected via terrestrial networks such as the Internet.

Networks of ground stations are owned and operated by providers who offer their use on a pay-per-use basis as a *Ground Station as a Service* (GSaaS) model, allowing satellites operators to reduce their cost and access a broad network of stations. Some examples of GSaaS providers are:

- AWS Ground Station
- Leaf Space
- KSAT
- SSC

As previously mentioned, the orbit followed by a space vehicle directly affects the communication time window with ground stations, but also the latency of communication, Earth surface coverage and the potential use cases.

The *type of orbit* is determined by three (3) factors:

- Altitude
- Eccentricity
- Inclination

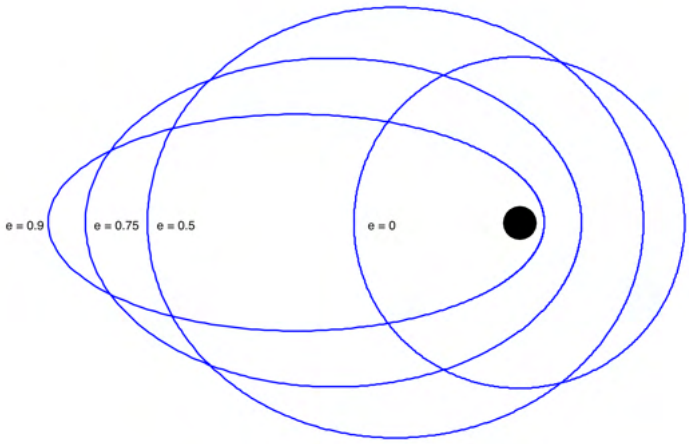

Figure 3: Examples of orbits with different eccentricity

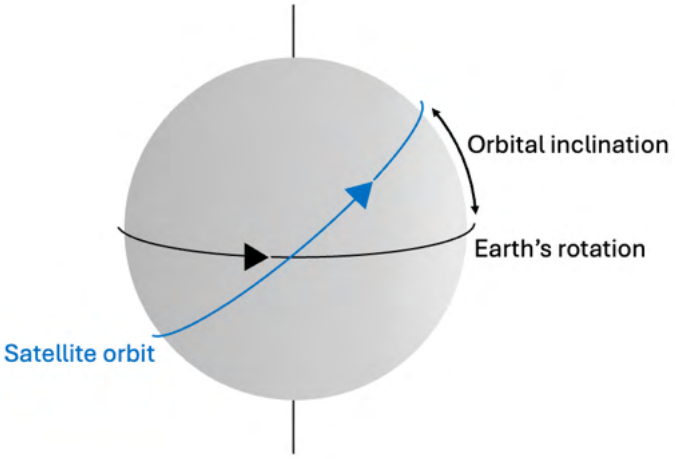

Figure 4: Example of orbital inclination

Without diving into the specific physics and mathematics, we can say that a higher altitude corresponds with a slower orbital speed, broader Earth surface coverage, and higher latency. On the other hand, satellites at lower altitudes orbit around the planet at much faster speed, have lower latency but also smaller coverage.

The three (3) main types of orbits defined by altitude are:

- Low Earth Orbit (LEO)
- Medium Earth Orbit (MEO)
- Geostationary Orbit (GEO)

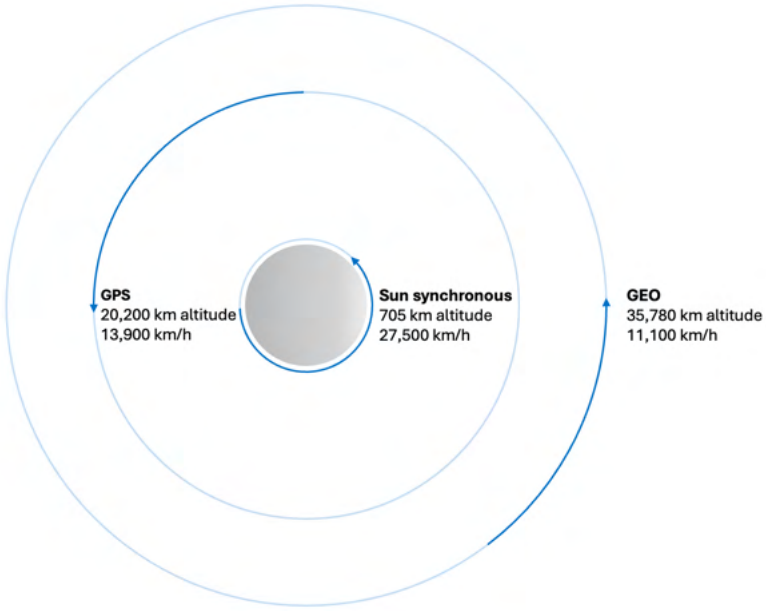

Figure 5: Examples of three orbits defined by altitude

This work focused only on space vehicles, use-cases and scenarios for the LEO orbits for multiple reasons, which are described in the next chapter.

Threat Modeling

Threat modeling is the process by which potential threats against the target system are identified and assessed, and proper mitigations are defined and prioritized based on the estimated risk. The purpose of threat modeling is to provide a systematic analysis of what countermeasures must be included to safeguard the assets against the attack vectors that could be perpetrated by the identified threat actors.

Multiple threat modeling frameworks are available, with STRIDE being the one commonly used in *Software Development Life Cycle (SDLC)*, which groups threats into six categories:

- **S**poofing identity
- **T**ampering with data
- **R**epudiation
- **I**nformation disclosure
- **D**enial of service
- **E**levation of privilege

As can be observed, the STRIDE threats map directly to the absence of some of the security properties that a

system must have (authentication, integrity, non-repudiation, confidentiality, availability, authorization). This helps identify the type of controls and countermeasures to include - or improve - in the system, which depend on the operational context and the specific design of the system under analysis.

While STRIDE provides a way for identifying vulnerabilities that could be exploited by threat actors, the MITRE ATT&CK knowledge base documents the attack *Tactics, Techniques and Procedures (TTP)* based on real-world observations, providing information on known threats and mitigations against them.

On October 2022, the Aerospace Corporation released the first version of Space Attack Research and Tactic Analysis (SPARTA), a knowledge base similar to MITRE ATT&CK but focused on providing information about how space vehicles may be compromised via cyber means.

For our work, we combined the information gathered from threat modeling with those provided by SPARTA to identify what could be applied to the D-Orbit satellite, and what countermeasures should be implemented by any similar organization.

Motivations

A Growing Space Economy

Since the first artificial satellite, Sputnik 1, was launched in 1957, the space economy evolved at rapid pace developing technologies and infrastructures for a variety of services such as Earth Observation (EO), communications and navigation. Less than forty years later, in 1994, the Global Positioning System (GPS) became fully operative for civil use with its constellation of 24 satellites, revolutionizing transport and creating opportunities for a variety of new services.

The evolution of the *space economy*, which is defined as *"all activities and resources that contribute to human progress through the exploration, research, understanding, management, and utilization of space"* by the Organisation for Economic Co-operation and Development (OECD), has been defined by three phases with different involvement of the public and private sector. The first phase (1950-1969) was mainly characterized by governmental space programs, while the second one (1970-2000) was marked by the gradual entry of private actors. The third phase (from 2000 to date) saw a progressively higher participation of private companies in different areas, from components and satellites manufacturing to space launch and logistics.

Small satellites have been introduced (e.g., CubeSat), reducing the cost of production and service operation. The cost of launch and access to space has been significantly reduced since SpaceX successfully developed the Falcon 9 program, providing access to space for many small and medium-sized companies, as well as educational and research institutions.

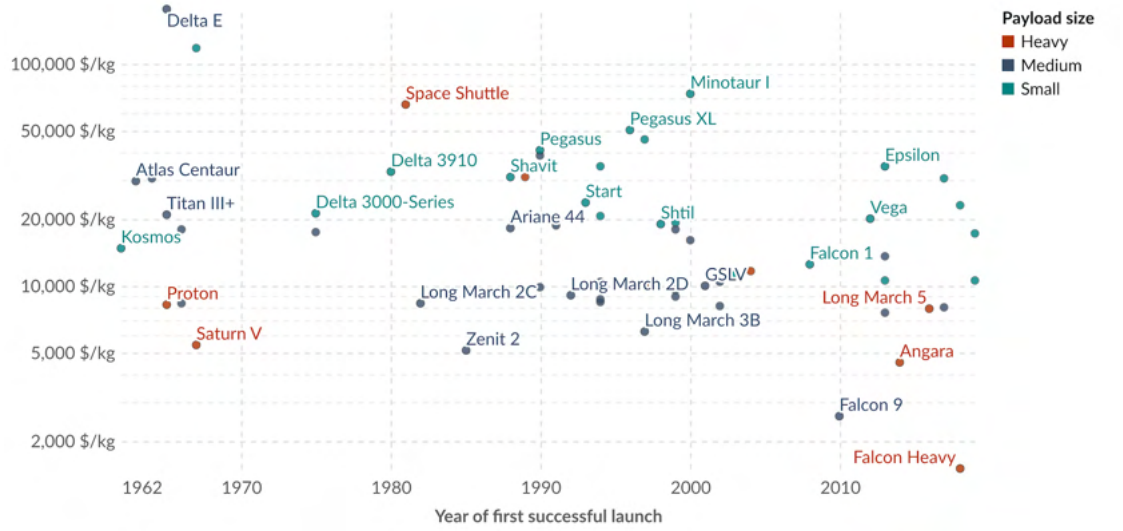

Figure 6: Cost of space launches to Low Earth Orbit (source: ourworldindata.org)

According to the McKinsey's report published in April 2024 for the World Economic Forum, the global space economy is estimated to grow from $630 billion in 2023 to $1.8 trillion in 2035, including growth of both the backbone segment and special services, which are estimated to represent the bigger part of the economy.

These include connectivity services we are already familiar with, like satellite-based Internet providers via LEO constellations (e.g., Starlink) and Earth Observation (EO) services, but also innovative ones such as:

- Space 5G cellular broadband (e.g., AST SpaceMobile)

- IoT satellite connectivity (e.g., Apogeo Space)
- Edge Computing in Space (e.g., SkyServe)

Space logistics services are also estimated to grow significantly as part of the new space economy to support the increasing demand for transporting and deploying space components, including *last-mile space logistics* services for small satellite delivery and dispatch, repositioning and in-space transportation.

Security Implications and Challenges

From a security point of view, the new space economy will likely introduce new private companies in the market with different services, solutions, applications and devices that will be part of a broader ecosystem.

Traditionally, the development of space systems focused on safety and reliability rather than security, similar to what characterized the *Industrial Control Systems (ICS)* in the past decades. Those systems were designed to be isolated and not exposed to external threats thanks to *airgapped* networks and physical boundaries. Relatively few actors had the opportunity to interact with such systems, whose main requirement was their *availability* rather than *confidentiality* and *integrity*. Common digital security pillars like authentication, authorization and encryption were simply absent. When industrial networks were connected to IT networks - often in a non-secure way - however, the attack surface changed dramatically, introducing attack scenarios not contemplated before. Space systems are undergoing the same transition and will likely face similar challenges.

Space systems often relied on *security through obscurity* as they mostly used proprietary technology whose access was restricted to governments and their contractors. However, the context is changing as private companies - especially small ones - are increasingly relying on common *Commercial Off The Shelves* (COTS) components and tools, as well as open-source ones (e.g., Cubesat Space Protocol), which can be assessed by security researchers and threat actors more easily.

However, accessibility to space components is still a significant challenge. From a security researcher's point of view, accessing a complete and functional space system like a satellite in its entirety cannot be done without the collaboration of the manufacturer. While, for example, in the automotive sector one can, in the worst case, purchase a car or ECUs for research purposes, this cannot be done for satellites as they are not for retail sales, and the list of components is not public.

From the manufacturer's point of view, physical access to space systems once they are deployed in orbit is extremely challenging and costly, making that hardware upgrades or recovery procedures in case of failures very difficult. Systems are designed focusing mainly on reliability to be fault tolerant through the use of redundant systems and components; however, in case of security compromise that would block remote control such as hijacking, the system could be rendered inoperable.

General Awareness

The increasing awareness of the Space economy and its risks played a significant role in motivating us into taking the first step into exploring this industry. While other exciting technologies exist and are worth being explored with dedicated work (e.g., Quantum computing architectures), they still represent a *market niche* with very few players and consumers, as well as threat actors.

Service providers based on LEO constellations are now available for general audience at affordable costs, meaning that both customers and threat actors could easily get access to them with different goals, of course. As

an example, in Dishing Out DoS: How to Disable and Secure the Starlink User Terminal researchers demonstrated feasible attack scenarios against Starlink user terminals.

As previously mentioned, to communicate with an in-orbit satellite we must know its orbital elements and frequencies. These are partially known and can be acquired - in whole or in part - publicly. Like the well-known services for tracking flights across the globe, there exist multiple public online platforms for tracking satellites and their radio frequencies. Some examples are:

- SatNOGS DB
- OrbTrack
- N2YO
- Satellite Tracker 3d

Notable security incidents involving space infrastructures and services resonated through the news, bringing the topic to a much broader - and general - audience. For example, in 2022 the cyberattack against Viasat right before the Ukraine invasion had a significant *hybrid* impact across Europe.

On October 13, 2025, security researchers from the University of California, San Diego and the University of Maryland, College Park published the research paper Don't Look Up: There Are Sensitive Internal Links in the Clear on GEO Satellites where they examine the security of transmitted data, demonstrating how often sensitive information is not encrypted and susceptible to being intercepted.

D-Orbit ION Satellite Carrier

The ION Satellite Carrier, with "ION" standing for "InOrbit NOW", is D-Orbit's flagship product, designed with modularity and flexibility to deliver a broad spectrum of services. The proprietary orbital transfer vehicle was designed as *last-mile* carrier to transport CubeSat-sized payloads and microsatellites in space across orbits and deploy them in their final operational slots.

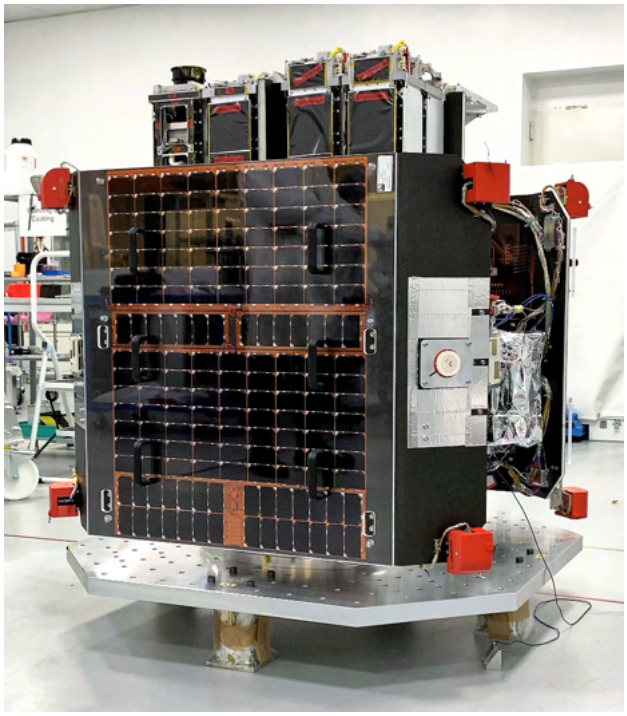

Figure 7: "ION SCV Laurentius" satellite

The satellite is composed of three (3) main modules:

- The Payload Bay, which hosts the payloads and the related mechanical electrical interface ends
- The Platform, which includes all the spacecraft subsystems and avionics
- The ION Propulsion Module, which hosts all the propulsion actuation functionalities

The first module is customizable based on the type, size and number of payloads that are part of the mission, consisting of a reconfigurable cargo bay that features a customizable 64U satellite dispenser capable of hosting a combination of CubeSats and Payloads that fits that volume, while the others are common across the different missions.

However, precision payload deployment is not the only service provided by D-Orbit thanks to the ION. With the ION Hosted Payload Service, space hardware companies can get their payloads to orbit for testing or operations thanks to a plug-and-play mechanical, electrical and data interface, using the ION satellite as a platform without needing a dedicated satellite.

Furthermore, new upcoming services for moving computation in space will allow customers to deploy their containerized software on ION's computation platform for processing data acquired by sensors in space *locally*,

without the need of transmitting down to Earth massive amount of data. Only the final output will be transmitted, with significant efficiency improvements.

This work focused on one of the latest ION satellites, whose maiden flight happened on June 23, 2025 aboard the Transporter 14 flight. The satellite *ION SCV Passionate Paula* is flying Skytrail, the 19th commercial mission of ION.

Mission Life Cycle

An ION mission – using D-Orbit's ION Satellite Carrier – is a multi-stage journey that takes a batch of small satellites from concept to orbit. It is a self-contained space mission that carries multiple satellites to space, deploys them into their target orbits, and even hosts in-orbit experiments. The entire lifecycle of an ION mission can be understood in distinct phases, each with specific goals and activities, from the initial planning to the mission's conclusion. Below is an overview of these key phases in an ION mission's life, explained in accessible terms for a general audience.

Phase 1: Mission Planning & Preparation

Every ION mission starts long before reaching the launch pad. In this planning phase, engineers and mission managers work together to define the mission's goals and constraints. They decide which satellites will be on board, what orbits those satellites need, and any additional experiments the ION carrier will perform. Detailed mission analyses are carried out to ensure everything is feasible – from orbital trajectories to fuel requirements – and to identify any risks early.

This is also when success criteria are set. The team coordinates with launch providers and regulatory bodies, schedules the launch, and prepares contingency plans for potential challenges like launch delays or satellite issues. By the end of the planning and preparation phase, the mission has a clear schedule, and the ION spacecraft is built and rigorously tested on the ground to ensure it's ready for the harsh environment of space. From hardware stress tests to software simulations, every system is checked and double-checked, giving the team confidence as they approach launch day.

Phase 2: Launch & Early Orbit Operations

When launch day arrives, ION – loaded with its cohort of small satellites – blasts off atop a rocket. This marks the beginning of the execution phase. After the rocket reaches the right altitude, it deploys the ION spacecraft into orbit. Now the focus shifts to the critical first hours and days in space, often called *Launch and Early Orbit Phase* (LEOP). During this period, the ION vehicle "wakes up" and automatically performs initial tasks: it stabilizes its orientation (a process known as detumbling) and points its solar panels to the Sun to start powering up. Almost immediately, it aims to establish a communication channel with the ground. Shortly after separation from the launcher, the mission control team typically receives the first signals from ION, confirming it is operating.

Engineers at the Mission Control Center carefully check the spacecraft's health and status – they verify the power levels, thermal conditions, and that all core systems (like navigation and communications) are functioning correctly. This early orbit phase is intense: if any anomaly is detected, the ground team can send commands to troubleshoot. Fortunately, ION missions are designed to handle this phase robustly through extensive pre-flight testing. Once ION passes these checkouts after separation from the launcher, the mission is officially on a solid footing in orbit.

A short commissioning period follows, during which the spacecraft might run self-calibration routines and small test maneuvers to ensure it is fully ready for the main mission objectives. By the end of Phase 2, the ION carrier is stable, healthy, and primed to begin its work delivering satellites to their destinations.

Phase 3: Deployment & In-Orbit Mission Operations

This phase is the heart of the ION mission – the nominal operations phase, which can span several weeks or even months or years if needed. With the spacecraft functioning normally, mission control initiates the deployment plan. One by one, at pre-planned times and orbital positions, the ION carrier releases each satellite on board by adjusting its orbit between deployments, ensuring each satellite is dropped off in its correct orbital slot.

In addition to deploying customer satellites, the ION vehicle often has its own hosted payloads or experiments to run. The spacecraft's onboard computer and communication systems allow it to perform edge computing tasks and send valuable data back to Earth for analysis.

Throughout the operations, the ground team remains in continuous contact with ION via radio signals. They send up commands (like instructing a deployment or a burn to change orbit) and receive telemetry data in return. All this data is carefully analyzed in real-time to ensure the mission stays on track and to handle any unexpected events.

By the end of this phase, ION will have deployed all its passenger satellites to their new homes in orbit and completed any in-orbit demonstration activities. Each deployed satellite is now operating independently, while the hosted payloads are operated on behalf of the customers by D-Orbit through ION carrier.

Phase 4: Mission Conclusion & Post-Mission Wrap-Up

After completing its deliveries and on-orbit tasks, the ION spacecraft enters the conclusion phase of the mission. At this point, the focus is on safely ending the mission and ensuring the spacecraft does not become a hazard in orbit. Using any remaining fuel, it will perform a final burn (or a series of maneuvers) to lower its orbit. The goal is to bring the spacecraft back into Earth's atmosphere eventually, where it will burn up harmlessly. As ION executes this last step, it also goes through a shutdown sequence to passivate itself – leaving no energy sources that could cause an explosion – making the retired spacecraft as inert and safe as possible.

On the ground, the mission team closely monitors this decommissioning. Once it is confirmed that ION is on a safe trajectory and all final commands have been executed, the operational phase officially ends. But the mission lifecycle isn't truly complete until the post-mission analysis is done. The satellites ION deployed are operating independently in orbit, the ION carrier is safely out of the way, and the entire project's outcomes are recorded.

Threats and Mitigations

This section provides information on the threats identified by reviewing the ION life cycle and its documentation, with the collaboration of D-Orbit security team.

As previously mentioned, this work focused only on the space vehicle, leaving anything related to corporate infrastructure, cloud services, GSaaS, and anything on which satellite manufacturers do not have control, out of scope. The reason is that we aim to provide recommendations for securing space vehicles independently of the other components of the space system. While they could be improved or replaced throughout a mission, the satellites could not, making it extremely hard - if not even impossible - to apply changes once deployed.

The following diagram is a general high-level representation of the satellite architecture built on top of a

CAN-bus architecture, whose choice is based on reliability and fault-tolerance requirements. Systems and subsystems are redundant, as well as the CAN-bus, to remove single point of failure components. Each subsystem has its own redundant on-board computers which are not represented in the diagram for simplicity.

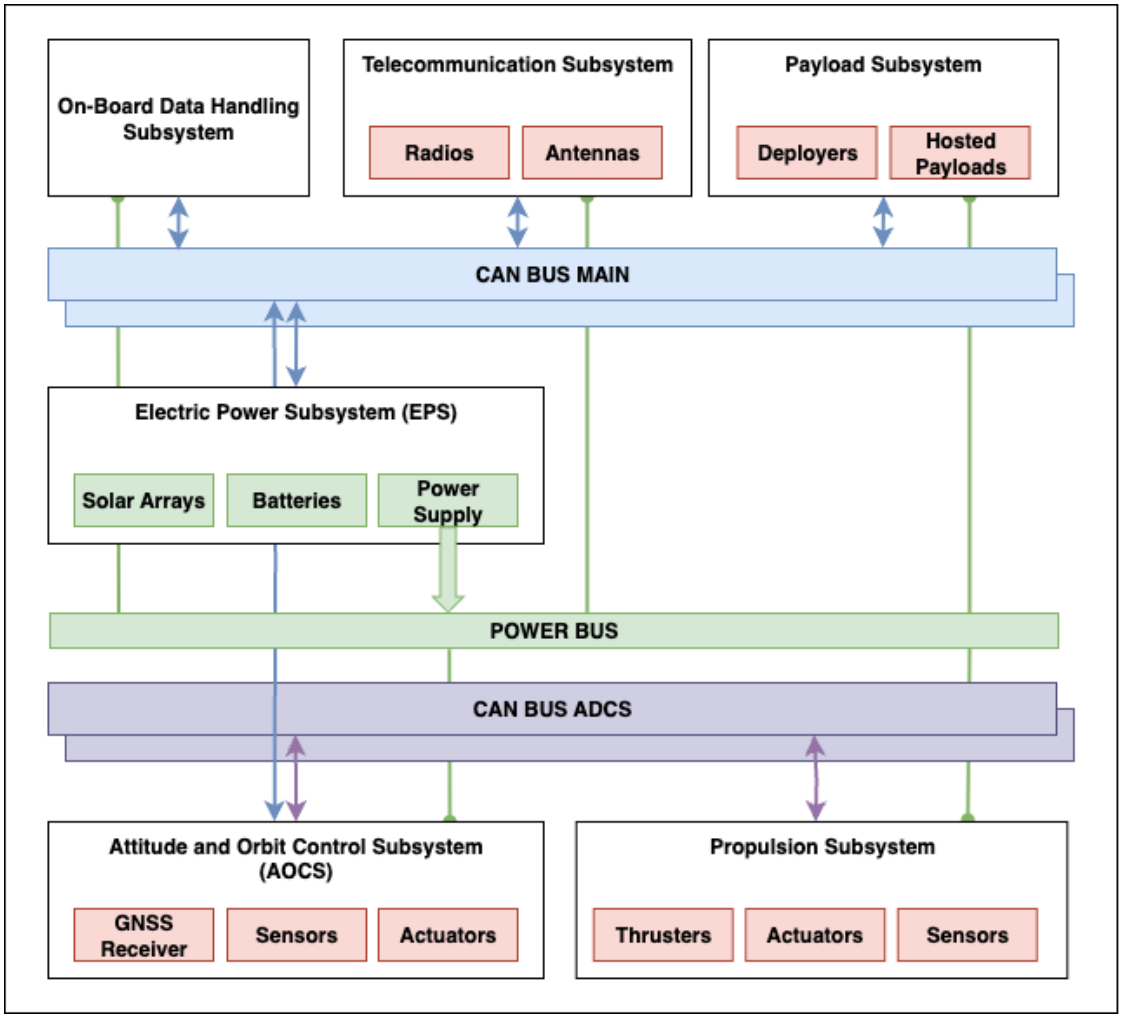

Figure 8: General high-level system architecture

We identified three (3) main threat areas that could expose the satellite to compromise by cyber attacks:

- Radio communication
- Hosted payloads
- Firmware compromise via physical access

Different threat actors could have different motivations for potentially targeting ION and its missions. They could be:

- **Nation State actors**
  - Threat actor with almost unlimited resources and advanced technical skills. They could be motivated by geopolitical reasons and conflicts.

- **Competitors**
  - Threat actor with potentially high financial and technical resources, who is motivated by economic interests and would benefit from D-Orbit's reputational damage.
- **Hacktivists**
  - Threat actor motivated by cultural and morale reasons with average technical skills and resources.
- **Criminals**
  - Threat actor with technical resources mainly motivated by economic interests, who would abuse compromised systems for stealing valuable data, deploying malware for creating or expanding botnets, perpetrating ransomware-like attacks against D-Orbit, or performing kinetic attacks against other space vehicles by hijacking ION.

Communication

STRIDE Threat Category	Vulnerability	Threat
Information Disclosure	Missing or weak encryption	Eavesdropping radio communications
Spoofing	Missing signal authentication	Transmission of unauthorized radio messages
Denial of Service	-	Jamming

When a satellite is deployed in space, the only feasible way for interacting with and controlling it is via wireless communication with either radio or optical signals (in this context, we will focus on radio signals). Due to the nature of wireless communication, the signals are intrinsically exposed to the risk of being *eavesdropped*.

Eavesdropping is the act of capturing network communications with specialized hardware (e.g., Software Defined Radio (SDR)) and packet capture software. The main purpose is to acquire exchanged data to access confidential information, which could require *reverse engineering* analysis if the communication protocol is unknown or proprietary.

Even though wireless communications are intrinsically exposed to the risk of being eavesdropped by threat actors located in the range of wireless coverage, threat actors would need to:

- Know the transmission frequencies
- Have the eavesdropping hardware located close to the radio signal (e.g., close to the ground station), or
- Know the orbital elements of the satellite and listen for downlink radio communications.

The transmission frequencies used by a satellite are partially known and could be publicly available via online services. Similarly, the real-time position of the satellite could be tracked and estimated, allowing threat actors to know when and where the satellite would fly above a specific location. By connecting the dots, threat actors could be able to capture data transmitted by the satellite, which would likely be telemetry.

What might not be known and hard to predict is *which* ground station will send data to the satellite and *when*. In fact, if the mission control team relies on GSaaS with ground stations distributed across the planet - like D-Orbit - capturing uplink communications containing control commands, or downlink ones with command results or processed payloads would be unlikely, but not impossible, to happen.

Organizations often rely on *security through obscurity* to protect their information, assuming that if no one can access the instrumentation to parse and extract meaningful information from the data, nor have knowledge of the protocol, the communication is *secure*.

If data is captured, threat actors could parse the proprietary protocol and data structure by means of reverse engineering, potentially allowing direct communication with the satellite.

To mitigate the risk, organizations should adopt in-transit end-to-end encryption and enforce message authentication which, however, is more challenging than in traditional IT infrastructures. Higher latency, short communication window, and the impossibility to physically access the satellite to restore the communication in case keys are corrupted are just the main challenges. Also, encrypted protocols may require transmitting more bytes, potentially affecting the actual throughput which could be bound by *Service Level Agreement (SLA)*.

Current S-Band transceivers for space like those mentioned in The Space System section implement AES-GCM which provides authenticated encryption and integrity verification, offering an easier option for enabling secure communication offloading the encryption and decryption operation to the transmission appliance. However, the following challenges should be considered:

- The system should provide a reliable process for updating keys while in orbit on a regular basis to mitigate the risks associated to a compromised key.
- The system should be able to switch to a *safe mode* in the event the key is lost due to an incident or disaster. For example, if no encrypted communications are established for a specific amount of time, the system should fall back to a state where only a pre-defined key is accepted and only for a subset of commands used for restoring the communication capabilities.

Some of the security solutions adopted by the new space industry include the use of radio encryption for higher performance and leveraging on *Over-the-air Rekeying (OTAR)* method to securely rotate keys used both for end-to-end encryption and message authentication. In fact, the ground station - or GSaaS provider - receives the messages already encrypted and signed by the sender, and forwards it to the receiver. Only the mission control systems and satellites can authenticate the message and decrypt it. Alternative strategies may include software solutions with ad-hoc encryption libraries (e.g., CryptoLib) which, however, could not be suitable for the on-board computers.

In contexts where multiple communication flows related to different and independent entities are transmitted through the encrypted channel, like in a multi-tenant environment, adding an additional authentication code such as a key-based *Hashed Message Authentication Code (HMAC)* to the payload would be helpful in mitigating the risk of spoofing attacks at application level. While this scenario is not applicable to the current D-Orbit platform, manufacturers offering multi-tenant services with direct access to the clients should implement authentication and integrity verification at every communication level.

Jamming is another type of attack which aims to interfere with communications by sending strong radio signals on the same frequencies used by the communication parties. In our context, jamming is an *accepted risk* for the following reasons:

- Defending effectively through the adoption of advanced solutions like frequency hopping requires using different type of radio devices, whose cost can be an significantly higher.
- The likelihood of attack for missions without geopolitical or military relevance is extremely low. Threat actors with economic motivations do not have sufficient reason to carry out such an attack against D-Orbit, nor do hacktivists.

- Jamming a LEO satellite requires the use of another nearby satellite or a global network of antennas. In the case of ground-based jamming, given the high orbital velocity, the satellite would be out of a static ground-based jammer's visibility in a few minutes, and communication would be restored as soon as the satellite is visible from any ground station placed elsewhere on the globe. Therefore, the costs to carry out a stable and long-lasting attack are very high, and consequently, the likelihood of occurrence is limited.

Mitigation against such attack could include threat intelligence to identify geographic areas where jamming is more likely to happen and therefore avoid using ground stations located there, deployment of multiple satellite in a constellation for redundancy, which could communicate to each other in-space, and others.

Finally, a contingency plan should be defined to handle the unlikely situation where a continuous jamming attack would make the satellite unable to communicate for longer periods. In our context, the satellite will automatically switch to a "safe mode" when contact from ground is lost for a given amount of time to prevent it performing actions that, without supervision from the mission control systems, could lead to unexpected behaviors. When the communication channel between ground and the satellite is restored, specific procedures are performed by the Flight Operations team to restore the nominal conditions.

Hosted Payload

STRIDE Threat Category	Vulnerability	Threat
Spoofing	Inherited trust of components	Transmission of unauthorized messages
Information Disclosure	Insecure intercomponent messaging infrastructure	Eavesdropping information
Elevation of privilege	Improper authorization controls	Acquiring access to systems and components outside the trust boundary of the hosted payload
Tampering and Elevation of privilege	Hosted payload firmware not validated	Use of firmware with malicious or vulnerable components
Denial of Service	Lack of quality of service. Insufficient input validation	Volumetric attack against the satellite interfaces. Fuzzing APIs.

ION missions could include payloads that are not intended to be deployed in orbit but instead be *hosted* by the D-Orbit platform for different reasons and goals, like testing, experimenting or scientific research. A hosted payload is a component designed and developed by a third party which is connected to the ION platform and can interact with the on-board system through specific interfaces and a restricted set of APIs. Hosted payloads can be monitored and controlled from the ground by the D-Orbit mission control team. Currently, customers do not have direct access to them, but only through D-Orbit.

A hosted payload could represent a significant threat to ION and D-Orbit if not securely managed. In fact, a *malicious device* connected to the platform deployed in orbit could be one of the best ways to attack the satellite and compromise it, as also documented by SPARTA in Compromise Hosted Payload.

D-Orbit was aware of the risks introduced by connecting a third-party component to their platform, and because of that they designed a thorough validation process to ensure the hosted payload could not affect ION and its nominal state. In addition, none of the critical functions, such as those related to the Attitude and Orbital Control Subsystem for maneuvering the spacecraft, are exposed to the hosted payload system.

The process includes:

- Connection of the hosted payload to the ION *physical twin* on the ground to validate that it does not interfere nor affect the platform during all its operational states.
- Monitoring of the data exchanged with the platform during all potential operational states and in various conditions.
- Review and validation on the ground of each command and script provided by the customer to be executed on the payload.

The process is focused on ensuring that the hosted payload does not introduce any issue in terms of safety and reliability. Anvil identified some potential attack scenarios and assessed them with the D-Orbit security team, resulting in strategic actions to further mitigate them.

Some of the potential risks are:

- A hosted payload could embed sensors used to determine when it is in orbit or not to change its behavior (i.e., space time bomb).
- A hosted payload could behave differently when connected to the ground test platform and when in orbit, potentially hiding malicious behaviors during the testing phases.
- Malicious commands, scripts or tasks could be enabled in orbit via specific tasks requested by the client, that a review might not detect.
- The firmware of the hosted payload could embed vulnerable dependencies that, if exploited, could allow bypassing the security boundaries.

They could be mitigated with the following actions:

- Perform a full code review of hosted payloads firmware and software to detect potential malicious functions, modules or vulnerabilities.
- Request customers to provide an additional payload to keep connected to the physical twin platform for testing and validation purposes throughout the life of the mission. This should be used to dynamically validate any requested tasks before executing them in-orbit.
- Connect hosted payloads to a security module which acts as a middleware / sandbox, and monitor the data sent by the payloads for anomaly detection, allowing ION to isolate them.
- Introduce fuzz testing for the interfaces and the APIs available to the hosted payloads to ensure they are robust against unexpected data.
- Perform regular comprehensive security assessments of the hosted payload controller system to which they are connected to.

It is worth mentioning that firmware assessments and reviews cannot always be performed because of Intellectual Property agreements. In such cases, customers could engage independent third-party vendors to assess their software and provide the results.

Physical Compromise

STRIDE Threat Category	Vulnerability	Threat
Tampering and Elevation of privilege	Lack of firmware integrity check	Replacing the firmware with malicious versions for sabotage or unauthorized access via backdoors
Tampering and Elevation of privilege	Lack of hardware integrity check	Tampering with the onboard hardware or adding malicious devices to the CAN bus

Anvil and D-Orbit security assessed the risk of threat actors compromising ION by tampering with its firmware and onboard software to bypass security measures and acquire persistent access, for example by introducing backdoors.

During the first phase of a mission, the spacecraft and all its components are in a clean room whose access is restricted to authorized personnel only (i.e., engineers), enforced and monitored 24/7. Unauthorized access to the room and malicious interactions with the embedded systems are extremely unlikely to happen during this phase.

Similarly, code repositories, artifacts and building pipelines are secured and compliant with security best practices to ensure changes are reviewed and validated, preventing modifications to the software before it is flashed to the embedded systems.

Firmware are signed at build time for integrity and authenticity checks and flashed also to read-only memories acting as *golden images* to be used for re-flashing in case any corruption is detected by the integrity check routines.

Organizations should also consider using consolidated and effective solutions like Secure Boot to prevent the hardware devices from executing firmware that are not signed by trusted sources. However, not all embedded controllers offer such features, and their adoption could introduce additional challenges in handling unexpected failures and certificate management.

Once the validation processes are completed and the first phase of the mission is approaching the final stages, the satellite is shipped to the SpaceX facility. This is the phase where ION leaves the clean room of the factory and could, potentially, be exposed to external threats.

However, several mitigations have been put in place along with DHL to make the attack scenario almost unfeasible:

- The satellite is enclosed in a container with unique tamper-evident and tilt-evident seals to detect any attempt to affect its integrity during the travel.
- The container is a clean room itself. Only authorized personnel can access it.
- Trucks are tracked via satellites and monitored, as well as the flights.
- Once arrived in the US, the container is transported to the local facility with a secure transport, tracked and escorted.

- The container is examined to ensure its integrity has not been compromised. If any suspicious event is detected, a confidential and undisclosable contingency plan is started. Otherwise, all tests and validation procedures are repeated and compared to those performed at the factory to ensure all systems are in their nominal states and their integrity is preserved. Final payloads are integrated, if needed.

At this stage, if any of the embedded systems and software components would have been tampered with, chances are that differences would have been observed. Nation-state actors could have the resources to perform sophisticated attacks to bypass the described countermeasures, but no sufficient motivations have been identified to consider the scenario likely to happen.

Conclusion and Future Work

The evolution of the new space economy is changing the landscape by introducing new private players, from startup companies to consolidated corporates, bringing new technologies and solutions to drive tomorrow's businesses. The significant reduction in launch costs to LEO has greatly broadened access to space, allowing small companies to develop and deploy in-orbit their own satellites which could be as small as a CubeSat. We are already seeing the deployment of LEO constellations for various purposes, ranging from Earth observation to Internet access and IoT infrastructures, to space edge computing solutions.

Soon, we could have access to a broader catalogue of services relying on LEO satellites that could help us overcome limitations such as poor cellular coverage in rural areas or the need for large ground infrastructures to interconnect wide IoT networks. However, this also means that more systems could be exposed to cyber threats and must therefore be properly designed and protected.

Thanks to D-Orbit's joint work, we have explored a fraction of the space ecosystem and observed how satellites are designed, manufactured, tested and deployed in space, ensuring reliability and safety. We have reviewed satellite architectures and subsystems, the mission lifecycle, and associated processes, with the goal of identifying potential cyber security threats and corresponding mitigations, drawing both on D-Orbit's expertise and established security best practices.

The work presented in this document represents our starting point in the cyber security for space domain, with future works will focusing on the security of applications and embedded systems that form part of a space vehicle.

About the Authors

Alberto Volpatto is Technical Director at Anvil Secure. Prior to joining Anvil, Alberto worked as CTO at Secure Network, and as COO at its holding company. Alberto got his start in information security as research fellow at the Polytechnic University of Milan and then developed strong technical skills in threat modeling, application and infrastructure security throughout his career. He has assisted some of the leading companies and security groups in improving their security posture.

Davide Avanzi is the Head of Space Product Security at D-Orbit, where he is responsible for ensuring the security of the company's space platforms and their operations, alongside security R&D activities. Before joining D-Orbit, he worked as an Information Security Engineer at Secure Network, conducting red teaming and penetration testing engagements for various clients. His background in information security began during his M.Sc. in Computer Science and Engineering at the Polytechnic University of Milan, where he specialized in cybersecurity.

About Anvil Secure

Anvil was founded in 2016 with a vision to make a change in the information security consulting services industry. Anvil has since grown to be an industry recognized information security partner to some of the largest tech and Fortune 500 companies across the globe.

Anvil was founded with the principles of creating an information consulting services company that is honest, transparent, professional, and that will consistently deliver quality services to our clients. Anvil continues to hold these principles to this day and is now known for delivering consistently quality service, and for our transparent and inclusive approach.

Anvil's team is filled with dedicated industry veterans that are experts in fields such as:

- embedded/hardware security
- industrial control systems
- cloud security
- web application security
- mobile security
- AI security
- network security
- operating system security

Several team members come from National labs and other industry recognized consulting firms. The team's technical backgrounds and consulting experiences position Anvil to effectively improve the security posture of leading technology companies and security groups.

Anvil is headquartered in Seattle with an office in Amsterdam as well as several employees located around the globe including France, Spain, Italy and Argentina.

For more information about Anvil and to stay up to date on our latest research and progress, visit our website and social media pages:

- Website
- LinkedIn
- X

For any questions or further information, please reach out via Email or Phone:

- Email: info@anvilsecure.com
- Phone: 206-753-7649

About D-Orbit

D-Orbit is a market leader in the space logistics and transportation services industry with a track record of space-proven services, technologies, and successful missions.

Founded in 2011, D-Orbit is the first company addressing the logistics needs of the space market. ION Satellite Carrier, for example, is a space vehicle that can transport satellites in orbit and release them individually into distinct orbital slots, reducing the time from launch to operations by up to 85% and the launch costs of an entire satellite constellation by up to 40%. ION can also accommodate multiple third-party payloads like innovative technologies developed by startups, experiments from research entities, and instruments from space companies requiring a test in orbit. Finally, ION can also be rented for edge computing applications and space cloud services to provide satellite operators with storage capacity and advanced computing capabilities in orbit. D-Orbit's roadmap includes becoming a relevant player in the in-orbit servicing market, which is forecasted to become one of the largest, growing markets within the space sector.

In April 2025, the company announced a strategic business combination with the Planetek group to integrate new capabilities in cloud-based space applications, AI-powered data processing in orbit, and near real-time data services.

With offices in Italy, Portugal, Greece, the UK, and an experienced US team focused on bus design, manufacturing, and commercialization, D-Orbit is the world's first certified B-Corp space company and a registered benefit corporation.

For more information about D-Orbit, visit the website and social media pages:

- Website
- LinkedIn
- Facebook
- X
- Instagram

For any questions or further information, please reach out via Email:

- Email