Identifying Attack Surfaces in the Evolving Space Industry Using Reference Architectures

Matthew Bradbury
WMG, University of Warwick,
Coventry, CV4 7AL
M.Bradbury@warwick.ac.uk

Carsten Maple
WMG, University of Warwick,
Coventry, CV4 7AL
cm@warwick.ac.uk

Hu Yuan
WMG, University of Warwick,
Coventry, CV4 7AL
H.Yuan.4@warwick.ac.uk

Ugur Ilker Atmaca
WMG, University of Warwick,
Coventry, CV4 7AL
Ugur-Ilker.Atmaca@warwick.ac.uk

Sara Cannizzaro
WMG, University of Warwick,
Coventry, CV4 7AL
Sara.Cannizzaro@warwick.ac.uk

Abstract— **The space environment is currently undergoing a substantial change and many new entrants to the market are deploying devices, satellites and systems in space; this evolution has been termed as NewSpace. The change is complicated by technological developments such as deploying machine learning based autonomous space systems and the Internet of Space Things (IoST). In the IoST, space systems will rely on satellite-to-x communication and interactions with wider aspects of the ground segment to a greater degree than existing systems. Such developments will inevitably lead to a change in the cyber security threat landscape of space systems. Inevitably, there will be a greater number of attack vectors for adversaries to exploit, and previously infeasible threats can be realised, and thus require mitigation. In this paper, we present a reference architecture (RA) that can be used to abstractly model in situ applications of this new space landscape. The RA specifies high-level system components and their interactions. By instantiating the RA for two scenarios we demonstrate how to analyse the attack surface using attack trees.**

TABLE OF CONTENTS

1. INTRODUCTION

The space industry is seeing substantial change as new organisations enter the sector and its associated supply chain. These organisations have entered the industry as technology develops and barriers to entry have fallen, thus expanding the industry beyond the traditional large players and loosening their control [1]. This change to the environment, which has seen commercial space take a more prominent role, has been described as 'NewSpace' by NASA researchers [2]; others talk of 'alt.space' or 'entrepreneurial space'. Examples include SpaceX's SmallSat Rideshare Program, with costs as low as $1 million per satellite, with a payload up to 200 kg [3] (although previous base prices were set at $2.25 million for a payload up to 150 kg [4]) and the use of crowdfunding to decrease barriers to entry [5]. Such developments are allowing many new parties to deploy devices in space. This change is complicated by technological developments such as machine learning-based autonomous space systems [6, 7] and the Internet of Space Things (IoST) [8, 9]. Key advances are centred around CubeSats, and the IoST is facilitating connectivity at low cost.

IoST systems usually rely on satellite-to-x communication and interactions with broader aspects of the ground segment to a higher degree than existing space systems. Further, these IoST systems feature a myriad of components, developed by a range of companies from a number of countries, which are then launched in vehicles carrying multiple payloads. Such developments impact the cyber security threat landscape of space systems. Consequently, there will be a significantly greater number of attack vectors for adversaries to exploit, and previously infeasible threats will now need to be managed.

In this paper, we identify the attack surfaces of this evolving space industry. The developments of New space and IoST are first presented and discussed. These developments bring new challenges and opportunities to more traditional space systems [10], including issues for defence and security [11]. Previous work has shown that standard techniques (such as fault trees) can be improved through appropriate visualisation [12]. Another tool for visualisation is a Reference Architecture (RA) which can support the identification of attack surfaces in the system being described. Such approaches have been used previously for other industries where there are new agile entrants such as smart homes [13] and for connected and autonomous vehicles [14]. The reason for developing these, and a space reference architecture, is to provide a tool to allow attack surface analysis. Since newer entrants in NewSpace and the Internet of Space Things are not traditional companies, a reference architecture can help them understand the ecosystem and some of the threats. An RA can provide a better understanding of the new system and allow abstractly modelling of in situ applications in this new landscape. The RA specifies *high-level* system components and their interactions, and builds upon similar approaches used to understand changes to transport systems and building systems.

We instantiate the RA with concrete components to illistrate how a threat analysis can be performed. We develop and consider use cases, and then identify threat actors and their goals for subverting the system. There are existing analyses of threats to space systems (such as [15] and [16, Appendix E]), and so to avoid repeating existing work, we focus on the changes in threat actors, goals and methods that arise due to

978-1-7281-2734-7/20/$31.00

the changing space environment.

The RAs of satellite systems and space robots are specifically addressed in this paper. By using these abstract RAs, we can analyse the potential attacks against individual components. Threat modelling approaches can then be performed to analyse the threats. We examine our example use cases by developing attack trees for these specific scenarios. Our example use case will focus on autonomous debris collection. Through the use of these instantiations, the methodology for identifying new threats is explained.

In this work we make the following contributions:

1. We present a reference architecture of a space system which includes satellites, planetary robots and the ground segment that can be instantiated to support IoST functionality.
2. We identify changes to the space ecosystem and the changes they will have on adversary goals, motivations and capabilities and their impact on the threats that adversaries can perpetrate.
3. Using an example use case of autonomous debris collection to instantiate the reference architecture, we demonstrate the attack surface of specific scenario which will be facilitated by NewSpace, the IoST and use of autonomy in space systems.

The remainder of this paper is structured as follows: in Section 2 related work will be presented. Section 3 will present an analysis of the changing space ecosystem and the impact that will have on future threats. The abstract reference architecture for modelling these new systems is presented in Section 4. Section 5 describes the methodology used for performing an attack surface analysis on an instantiated reference architecture. Our example use case of autonomous debris collection will be analysed in Section 6. Finally, Section 7 will discuss remaining open challenges and Section 8 will present concluding remarks.

2. Related Work

Future space systems are expected to undergo major changes in terms of how they communicate, operate and the culture around the commercialisation of space. This means that there is an increasing interest in the security of these space systems, not just from existing mature organisations, but also from new entrants that lack experience in developing secure space systems. This section will introduce the existing work on security of space systems, how space systems have been modelled, and how, or indeed if, these modelling approaches can be applied to a security analysis of space systems.

Space Security

Space forms part of a nation's Critical National Infrastructure (CNI) and provides vital services that other CNIs rely upon for a range of services from positioning, navigation and timing to communication. The importance of cyber security in space is not specific to a single country but represents an international concern [17] and is the subject of increasing focus. The authors of [18, 19] proposed a number of policy changes that should be made to improve the state of cyber security in space, from encouraging greater use of encryption to advising space organisations to be more open with respect to working with cyber security researchers and facilitating information sharing.

In both [20] and [21] a USA-centric threat assessment from a military perspective are presented. In these reports counterspace weapons are classified into (i) kinetic physical (e.g., anti-satellite missiles), (ii) non-kinetic physical (e.g., lasers, high-powered microwaves and EMPs), (iii) electronic (e.g., jamming and spoofing radio communications) and (iv) cyber — where attacks focus on the data being transmitted and the data systems themselves. The report also contains details of the capabilities of other countries and independent groups, but focuses on geopolitical rivals to the USA. The authors chose to separate information security (which comprises the cyber category) from electronic security. However, this paper will consider cyber security attacks to be both electronic- and information security-based. State actors, such as France, have announced plans for a greater focus on defending their space systems [22, 23]. This includes surveillance cameras on satellites, greater satellite detection abilities, patrolling nano-satellites and powerful lasers that could be used to blind adversary satellites, with plans to deploy surveillance cameras and patrol nano-satellites from 2023 onwards.

Due to the changing space landscape, new threats are being introduced that need to be considered. In [24] the potential risks posed by equipping small satellites with propulsion systems (which they are not typically equipped with) was considered. The authors identified that these small satellite systems do not always encrypt their "telemetry, tracking, and control (TTC) or mission data communication links". This combination means that an unauthorised actor could send commands to the satellite to manipulate its orbit. The authors propose a solution to require encrypting the command and control links before a satellite is allowed to be launched as part of a *No Encryption, No Fly* regulatory requirement. Depending on the actual requirements of a system, if confidentiality is not required, digital signatures could be used to provide authentication and non-repudiation of the transmitted commands without the need to encrypt them.

The Consultative Committee for Space Data Systems (CCSDS) has also published guides for a variety of purposes such as: mission planning [25], system interconnection [26] and applying security to protocols [27] among others. CCSDS also published a report on current space cyber security threats [15]. In that report, a brief description of threat actors and the types of threats they may perform is presented. The report includes a list of threats in a variety of scenarios, with the impact of the threat described and an "illustrative" likelihood shown for each threat. The authors note that the threats identified, impacts, and mitigations will change when considered under different scenarios compared to the hypothetical scenario presented.

There has been much work on developing technical solutions to mitigate some security threats. For example, in [28] the authors proposed partitioning functionally independent software by time and space to avoid unintended interactions. Other work [29] has looked at techniques to secure the communication links in hybrid satellite networks. However, it is still necessary to have a methodology to represent *what* the space system is and *how* an adversary will compromise the system's components in order to achieve its goals.

Reference Architectures

To better understand the structure of systems, RAs are useful because they allow a system to be defined in a methodological manner. These models are useful in a variety of contexts, such as when teams are working on different components of a system and need to understand how these components will interact. By using an RA the interactions between components are clearly specified. With an instantiated RA (where concrete components and interactions are provided in place of abstract ones) the attack surface of a system can be analysed using

several tools, such as attack trees [30].

In general, RAs contain multiple viewpoints into the system that they represent. Multiple combinations of viewpoints have been used by different RAs, with the viewpoints selected based on the purpose of the RA. Examples of these viewpoints include:

- Functional: how the components work and what their tasks are
- Communication: how the components interact
- Implementation: how the components are implemented
- Enterprise: the relation between organisations and users
- Usage: concerns of expected usage of the system
- Information: the types of information handled by the system
- Physical: the physical objects in the system and their connections

For a cyber security analysis two of these viewpoints are vital: the Functional and Communication viewpoints. These two components need to be specified in order to understand what the system does and which interactions between components are required to provide that functionality. To ensure the usability of a RA for its purpose it is important to focus on the required viewpoints. It is useful to avoid defining viewpoints that are less relevant for a cyber security analysis. For example, including an information viewpoint would be useful if confidentiality is vital for a system. However, for a general RA used for a cyber security analysis, this viewpoint is difficult to define without a priori knowledge of the system.

RAs have been previously applied to space systems in a variety of contexts. Examples include for on-board software (AMASS Reference Tool Architecture [31], ORSA-P [32], [33], SAVOIR OSRA [34]), data systems (RASDS [35]) and mission design [36, 37]. These space-system specific RAs could potentially be adapted to undertake a cyber security analysis of space systems. For example, an RA that focuses on software would be useful as an implementation viewpoint and an RA that focuses on data systems would be useful as an information viewpoint. However, this additional information is typically too detailed for a high-level cyber security analysis of a system. Hence why we argue in this paper that a high-level specification of space systems in terms of their functionality and the interactions of the components that provide this functionality is a better approach to performing the initial cyber security analysis of space system before focusing on the identified areas of interest.

There are also similarities between RAs and approaches such as Model-Based Systems Engineering [38] and Failure Mode, Effects and Criticality Analysis (FMECA). Where failure mode maps to how the system is being attacked, effects maps to what impact the attack has on the system and criticality maps to calculating the risk posed by the threat. Risk may be calculated by the sum of the impacts weighted by the likelihood. For example, in [39] a reliability analysis was performed using FMECA for CubeSats. Part of this work included providing a functional block diagram which is similar to the functional viewpoint of a RA. Also in [40, Section 3.3] produces similar output to a threat modelling of a system. Other approaches, such as the block diagram of the Magellan flight system [41] are useful starting points for a RA. However, additional detail needs to be added for the diagram to be useful for a cyber security attack surface analysis.

UML [42] and SysML [43] is the basis for modelling languages that are useful for describing systems in terms of a model. While UML can be used to describe a variety of systems, its focus is on describing software. SysML, on the other hand, is a subset of UML with several extensions that aims to model systems engineering applications. A downside to both of these modelling languages is that they are complex (although SysML is arguably less complex than UML) and require specifying a broad range of details about the system being modelled. As such, these are useful for a low-level security analysis of a system or systems-of-systems where attack surfaces can be detected [44] and automatic generation of attack trees are performed [45]. However, for a high-level security analysis of a system, these tools require specifying information that is not yet necessarily available. In this case, a reference architecture is a better tool for a security analysis, before using it to guide the design of a UML or SysML model for detailed analysis.

Dimension	*Communication (IoST)*	*Autonomy*	*Culture (NewSpace)*
Satellite-to-satellite communication	↑↑↑	↑	—
Satellite-to-ground communication	↑	↓	—
Space environment sensing	—	↑↑↑	—
Cost of deployment	↓	— / ↑	↓↓↓
Barriers to Entry	↓	↑	↓↓↓
Applications & Capabilities	↑	↑↑↑	↑
Access to data	↑	—	↑↑↑
Component Reuse	↑	—	↑↑↑
Hardware Specialisation	↓	↑	↓
Changes to mission scope	↑	↑↑↑	↑
Mean Deployment lifetime	↓	—	↓

Table 1. Dimensions of Change in Space Ecosystem. The quantity of arrows signifies the magnitude of impact, more arrows signify a greater impact. A dash signifies no impact. Arrow pointing up means increasing arrow pointing down means decreasing.

3. ECOSYSTEM AND ADVERSARY CHANGES

Table 1 presents a high-level summary of the changes to the space ecosystem along several socio-technical dimensions. For each of these changes, a dimension of change is shown as being increased, decreased or remaining unchanged. We focus on three areas impacted by recent developments in technology and culture: (i) connectivity (via the Internet of Space Things), (ii) autonomy and (iii) culture (via NewSpace). We focus on these three areas since they have led to the

most significant changes in the threat landscape of similar systems such as Connected and Autonomous Vehicles [46] and Smart Cities [47]. For example, connected vehicles have, through these advances, introduced new attack surfaces that were hitherto unlikely vectors of attack [48].

Communication between satellites is currently typically performed in order to relay messages from one endpoint to another and there is little need for inter-satellite connectivity. However, the introduction of the IoST and deploying systems with greater autonomy will lead to new applications that require satellite-to-satellite communications [49]. For example, new information may need to be shared with other satellites directly, and how satellites perform tasks may need communication to decide how to allocate these tasks (e.g., via leader election). Conversely, autonomy may lead to a decrease in satellite-to-ground communication as there is a reduced need for human-in-the-loop commands to be received. It is recognised that the IoST is likely to lead to an increase in satellite-to-ground due to the additional telemetry that needs to be reported.

Sensing in the space environment is an important activity for existing space systems. Many are deployed to perform Earth monitoring [50] for reasons of food security, climate science as well as national security reasons. There is also sensing performed of the space environment as space weather events can have adverse effects on hardware in space and on Earth. Future space systems will need to perform increased sensing to support autonomy, as understanding the environment context is an important part of an autonomous decision making process.

The *cost of deployment* dimension amounts to a change in the economic context, driven by new satellites deployment capabilities. This is caused by developments in novel approaches to launch vehicle innovation in terms of construction, design and reuse that have led to a decrease in costs [51]. The cultural shift of NewSpace will have the largest impact on decreasing the cost of deployment in space, however, other changes such as the use of commercial-off-the-shelf components as part of the IoST will also lead to a decrease. Aspects of autonomy may increase the deployment cost due to the new functionality it enables and thus additional testing it will incur.

Lowering the *barriers to entry* in the space ecosystem is the symptom of a deep structural change that occurred when space changed from a sector governed by a centralised organisation to one where organisation is decentralised [52]. This change amounts to a cultural and philosophical shift toward greater private entity participation [53] and is arranged along the business model of a public-private partnership [53] where public bodies (e.g., NASA) share costs, risks and potential economic returns with private sector entities (e.g. Blue Origin).

Applications and capabilities include developments in the satellite industry, human spaceflight for space tourism, platforms, manufacturing, mining and resource utilisation [54]. Technological change in terms of connectivity and autonomy will enable novel applications that can be deployed (e.g., autonomous docking). Changes brought by NewSpace will facilitate these new applications and capabilities by reducing barriers to entry and facilitating commercialisation of these novel deployments.

Access to data is a key dimension of the space ecosystem as it develops concomitantly with the evolution of a global economy that is increasingly data dependent [54]. With easier access to space, information that was previously highly controlled has become accessible to more organisations. This has been seen with Earth observation information [55, 56] and especially satellite maps such as via Google Earth.

Component reuse refers primarily to less expensive and reusable launch vehicles that signifies a change in the economies of space systems. This reuse of systems may be extended further in the future by refuelling and re-purposing satellites in orbit [57].

The use of bespoke or standardised hardware is encompassed by the *hardware specialisation* dimension. The reuse of standardised equipment and hardware can lead to a reduction in costs for launch, development and maintenance of the system. For example NASA's Mars 2020 rover is reusing the template of Curiosity in order to simply the mission design, reduce risks and to save on costs [58].

The *changes to mission scope* comprises a key cultural shift in which power to shape society is transferred from science and scientific exploration to commercialisation — that is, through public-private partnerships. For example, NewSpace will allow organisations such as NASA and ESA to focus on new research as part of deep space missions, while private enterprises can take charge of *routine* flights between Earth and the International Space Station [53] by using knowledge that has already been generated from previous research. Technological developments in connectivity and autonomy will allow novel missions to be designed and executed, such as plans to deploy the autonomous JPL Helicopter Scout on Mars in 2021 [59].

Due to the high cost of deploying hardware into space existing systems are designed to have a long *mean deployment lifetime* to mitigate the cost of deployment. With reduced costs due to the use of commercial off the shelf (COTS) components and NewSpace there will be less pressure on long deployments. A major impact of this change is that more recently developed hardware and software will be deployed in space, compared to the current conservative attitudes that focuses on old and tested hardware and software [60].

These selected dimensions encompass some of the important changes that increase connectivity, autonomy and culture change may bring to the space ecosystem. Many of these changes come with benefits to the functionality that can be provided with space systems. However, these changes to the space ecosystem will also bring changes to the threat actors seeking to compromise space systems. In part, threat actors will be able to benefit from the same space ecosystem changes that the public and private sector benefit from. Threat actors will also benefit from the increased attack surface that these systems expose, especially due to increases in connectivity and autonomy of future space systems.

Threat Actors

These changes to the space ecosystem will lead to the changes in the threat actors trying to attack a space system. This involves changes to their goals, motivations and what they can achieve with the same capabilities and resources. To summarise these changes, abstract threat actors are shown in Table 2. The threat actor categories are derived from [16, Appendix D] and the dimensions to describe the threat actors derived from [61].

This table is provided with an example of how to describe the specific threat actor being considered when analysing

	Threat Actor	Example	Goals & Motivations	Capabilities	Environment	Resources
Individual	Outsider	Hacktivist	Personal satisfaction; Passion; Ideology. Doesn't believe in climate change, wants to impact functioning of climate satellite	Limited	Remote access	Minimal
	Insider	Cleaner	Financial gain; Discontent	Limited	Permission-less internal access	Internal knowledge
	Trusted Insider	Contractor	Financial gain; Discontent	Moderate	Internal access with some permissions	Internal knowledge
	Privileged Insider	Employee	Financial gain; Discontent	High	Internal access with high permissions	Internal knowledge
Group	Ad hoc	A group coming together over a time-critical event (e.g. Brexit, or a collective movement of Extinction Rebellion)	Dependant on group purpose: Ideological, financial, political	Limited to Moderate	Remote access	Limited knowledge and financial
	Established	A group(e.g. the Anonymous group)		Moderate to High	Remote access	Moderate knowledge and financial
Organisation	Competitor	An organisation about to compete for a tender for services	Corporate espionage; Financial gain; Reputation damage	Organisation size related	Remote access	Organisation size related
	Supplier	A supplier who fears their services are soon to be relinquished	Information gain; Financial gain		Remote access; Knowledge of internal structure	
	Partner	A partner with whom a relationship is starting to sour or is soon to end	Information gain; Financial gain		Limited internal access; Knowledge of internal structure	
	Customer	A customer who feels they have had poor or unfair service	Information gain; Financial gain		Remote access; Knowledge of internal structure	
	Nation-State	Geopolitical rival	State rivalry; Geopolitics	Sophisticated; Coordinated; Access to state secrets	Remote and internal access	Extensive knowledge; Extensive financial; Advanced equipment

Table 2. Threat Actors (based on [16, Appendix D] with dimensions from [61]) plus space ecosystem specific examples.

the attack surface of a space system. Identification of a specific threat actor is required to understand the motivations, goals, capabilities and resources available when attacking the system. This table does not consider accidental, structural and environmental threat sources seen in [16, Appendix D] as the focus of this work is on adversarial threat sources. We recognise that these aspects are still important to consider since they can have security implications. For example, the high radiation environment in space can lead to bit flips in security-critical areas of memory. These threats will need to be analysed and mitigated using other techniques.

Changes in Threats to Space Systems

Using the identified threat actor and the high-level changes to the space ecosystem in areas of communication, autonomy and culture, we now present general changes in the threats to space systems these ecosystem changes may lead to. These threats are not for specific space systems but instead target the general space ecosystem. While these can direct threat analysis, threat modelling will need to be performed for specific systems to understand the specific threats they will face.

To begin with, an increase in satellite-to-satellite communication [8] will present an initial increase in risk to systems. This is because there will be an increase in communication through resource-constrained devices vulnerable to a variety

of attacks such as interception, spoofing, replay and others. It is acknowledged that in the future alternate communication methodologies such as laser-based communication in the European Data Relay System [62] will reduce the risk posed by these threats. This is because laser-based communications are harder to intercept and spoof [63].

The inclusion of autonomy in space systems will also impact how the systems can be attacked. The application of autonomy to control satellites will be needed for a variety of use cases from simplifying management of a large swarm to orbit corrections and debris avoidance. There may be simple applications of autonomy (such as via Finite State Machines [64]), but more complicated and less easily analysed techniques such as deep learning are also likely to be applied. In applying autonomy to space systems some parallels can be drawn with autonomous vehicles, where the inclusion of autonomy has led to new ways in which the vehicle and infrastructure can be attacked [46].

With the reduction in barriers to entry, new organisations will increasingly become capable of deploying hardware in space. This will introduce several issues similar to those seen as new organisations enter IoT markets. Firstly, new entrants tend to focus on functionality rather than security. Secondly, if new entrants fail, it could leave uncontrolled devices in orbit that will no longer be updated or maintained. Finally, the cost reductions will extend to new organisations that may wish to deploy hardware for malicious purposes. This increase in ease of deploying malicious hardware will also lead to an increase in the risk of cyber-physical attacks (such as the physical attacks described in [21]).

Technological developments, especially around areas such as Software Defined Radios (SDRs), will increase the ways in which satellites can be interacted with. For example, the r/sdr community[2] involves members capturing transmissions from weather satellites (e.g., NOAA). SDRs are also capable of transmission, so satellite systems with unencrypted/unauthenticated communication channels can be interacted with by unintended entities [65]. Predicting revolutions such as SDRs are difficult but is important to investigate such changes as they alter the outcome of risk analyses.

While not a new threat, the long lifetime of devices can present a threat to space systems that will be compounded by new deployments. For example, over the lifetime of a device how are changes in security standards handled (such as new key length recommendations or hash algorithms being found to be vulnerable). One solution would be for the system to be deployed with above-recommended standards where the aim would be for these standards to be the recommended standards by the system's end of life. An alternate approach would be to support firmware updating and provide additional resources above the mission's requirements to support new and more expensive techniques. However, this will also provide a potential attack vector where an adversary could perform a firmware update to obtain control of the systems (as seen in automotive systems [66]). While these may not be questions that established members of the space sector need to consider, new entrants will need to understand what to plan for based on the length of their deployments. The actions new entrants take will then also have an impact on the established organisations and their deployments.

[2] https://www.reddit.com/r/sdr/

Summary

With this understanding of how the space ecosystem and the general threats it faces will change, we will now present a reference architecture to model space systems. This reference architecture will allow an analysis of how an adversary will attempt to achieve its goal associated with specific threats identified from threat modelling.

4. Reference Architecture

A RA provides an abstract model of a system where multiple viewpoints can be specified, including: functional, communication, physical, information, enterprise and others. For this RA we focus on specifying a hybrid functional-interaction viewpoint to simplify the analysis. Interactions that cross the boundary of the system identify the attack surfaces of the system. The internal interactions between components specify the path an attacker can take to compromise further components.

It is important to consider the specific scenarios that an RA will be used to analyse. The RA presented focuses on space systems in situ once they have been fully deployed. We do not focus on scenarios such as during launch or decent as there will be additional context information that needs to be specified to consider a cyber security analysis. Our future work will aim to investigate these additional scenarios.

Satellite Sub-architecture

Figure 1 specifies the abstract hybrid functional-interaction viewpoint of a satellite or system of satellites, which this work focuses on. Other components such as the ground segment or other space-based deployments (e.g., planetary robots) may be important to specify based on the application of interest.

Band	**Up-link** (GHz)	**Down-link** (GHz)
C	3.7 to 4.2	5.925 to 6.425
Ku	11.7 to 12.2	14.0 to 14.5
Ka	17.7 to 21.7	27.5 to 30.5
L/S	1.610 to 1.625	2.483 to 2.500
X	7.145 to 7.190	8.4 to 8.45

Table 3. Frequency spectrum allocations

Wireless Communications— The wireless communications handle the transmission and reception of data from the ground segment or from other space-based devices. These wireless communications will typically be implemented using radio frequency (RF) wireless communication, the common allocations are shown in Table 3. Based on the purpose the satellite communications can be classified as [67]: Earth-to-space, telecommand, space-to-earth, telemetry, radio metric, spacecraft and space-to-space. However, there is also a move towards laser-based wireless communications in future space systems.

Example Instantiations
- Short Range Omni-directional
- Short Range Directional
- Long Range Directional
- Laser-based Directional [62]

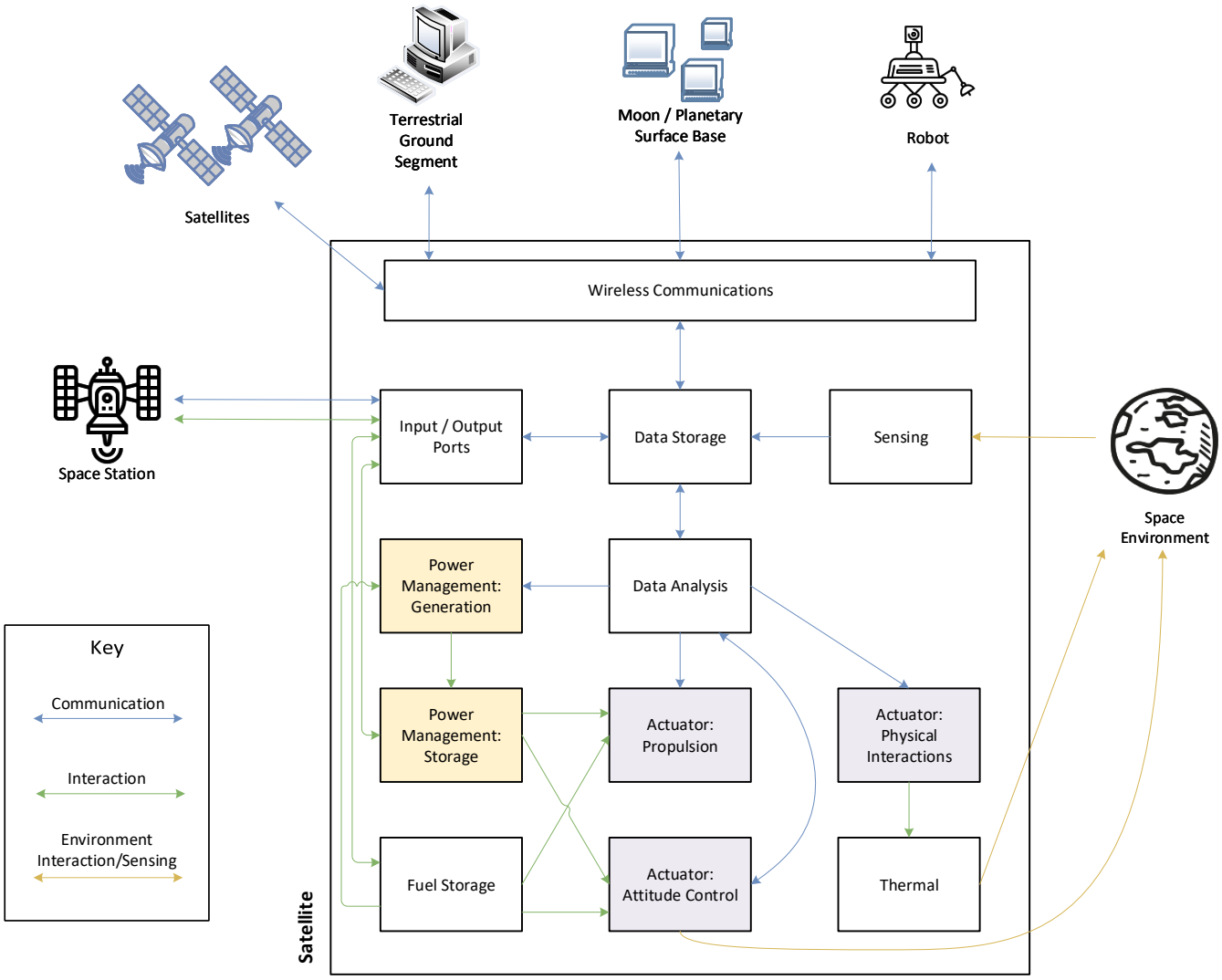

Figure 1. Functional Viewpoint of Satellite Reference Architecture

Example Attacks
1. Denial of Service (via Jamming) [68] [20, p. 4]
2. Sending spurious commands [69]
3. Message modification [69]
4. Eavesdropping [69]
5. Spoofing [20, p. 4]
6. Elevation of Privilege (via crafted messages)

Interactions
↔ */Communications: Sending/Receiving Command
↔ Data Storage: Send/Receiving Data

Input/Output Ports—Input/Output ports allow satellites to interact with a space station or other satellites in both physical and digital ways. Satellites can supply energy and fuel to the connected satellite [70]. Data can also be exchanged with the connected satellite.

Example Instantiations
- Connection with a docked vehicle

Example Attacks
1. Malicious use of ports

Interactions
↔ Space Station/Power Storage, Space Station/Fuel Storage: Receiving energy or fuel (when docked)
↔ Space Station/Data Storage: Receive and send data to the space station (when docked)
↔ Power Storage, Fuel Storage: Providing energy (when docked)
↔ Fuel Storage: Providing fuel (when docked)
↔ Data Storage: Receive and send data to local data storage (when docked)

Thermal—The thermal regulation maintains the temperature of the satellite at correct levels for proper functioning. Cooling can be achieved by radiating the heat that is generated by satellite out into space. Heating components may also be necessary to ensure other sensitive components are not allowed to become too cold to function.

Example Instantiations
- Heaters
- Radiators

- Cryogenic Fuel Cooling

Example Attacks
1. Disabling functionality to prevent components being kept at the correct temperature

Interactions
← Physical Interactions: Orienting the radiators
→ Space Environment: Infrared radiation output

Sensing—Sensing is a key functional component of satellite systems as sensors will need to gather information about the satellite itself, the environment it is operating it and potentially other objects that it is monitoring. This information will typically be stored locally before being transmitted to Earth for further analysis. Future space system may use this information to guide autonomous decision making.

Example Instantiations
- Imaging
- Attitude Determination
- Temperature
- Radiation
- Gyroscope
- Laser altimeter
- LIDAR
- Radar
- Ranging Instrument
- Sounder
- Accelerometer
- Imaging Radiometer
- Radiometer
- Timing (e.g., atomic clocks)

Example Attacks
1. Denial of Service (temporary or permanent blinding of sensors [20, p. 3])
2. Spoofing

Interactions
← Space Environment: Observing the environment state
→ Data Storage: Producing the sensed values

Power Management: Generation—Power generation ensures that the satellite is producing electrical power to continue operating. Depending on the mission context different power generation components will be used. For example, as the distance from the sun increases solar panels become less effective making RTGs or fuel cells more attractive. Ensuring the continued operation of this component is vital for a satellite to continue operating.

Example Instantiations
- Solar Panel
- RTG
- Nuclear Reactor
- Fuel Cell

Example Attacks
1. Resource depletion (Availability)
2. Denial of Service (Damage via high-powered lasers [20, p. 3])

Interactions
← Data analysis: Receiving Commands
← Fuel Storage: Providing fuel for Fuel Cells
→ Power Management: Storage: Storing unused power

Power Management: Storage—The power generated by the satellite will typically need to be temporarily stored. This may be because power generation only occurs for part of a satellite's orbit (such as when not in the shadow of the Earth) or because the power generation does not run continuously. In general, energy storage will typically be via electrical or electrochemical means, but mechanical is also a possible storage mechanism.

Example Instantiations
- Battery
- Flywheel [71]
- (Super)capacitor

Example Attacks
1. Lifetime reduction (Availability)

Interactions
↔ Input/Output Ports: Receiving/Accepting power
← Power Management: Generation: Storing unused power
→ Attitude Control: Proving energy supply
→ Propulsion: Proving energy supply
↔ *: Powering other components

Fuel Storage—Fuel storage acts as a chemical energy store. This fuel can be used for propulsion and power generation.

Example Instantiations
- Storage tanks

Example Attacks
1. Resource depletion (Availability)

Interactions
↔ Input/Output Ports: Sending/receiving from other satellites
→ Propulsion: Proving fuel for use in engines
→ Attitude Control: Proving fuel for use in RCS
→ Power Generation: Proving fuel to be converted to power

Actuators: Attitude Control—This component is concerned with maintaining or altering the satellite's attitude. Ensuring the correct attitude is important for communication, sensing, docking, power generation and other activities as a specific orientation of the satellite may be needed to perform these activities.

Example Instantiations
- Reaction Wheels
- Reaction Control Thrusters (RCS) [72]

Example Attacks
1. Fuel Exhaustion (Denial of Service)
2. Reaction Wheel Saturation (Denial of Service)

Interactions
← Data Analysis: Receiving commands
← Power Storage: Providing power
← Fuel Storage: Providing fuel for RCS
→ Space Environment: Impact the orientation of the vehicle

Actuators: Propulsion—The propulsion component is responsible for the satellite's movement this may be to change orbit or

to perform station keeping activities to maintain a specific orbit. Orbit change may be used to perform rendezvous manoeuvres.

Example Instantiations
- Solid Fuel Rocket Motor
- Liquid Fuel Rocket Motor
- Ion Engine

Example Attacks
1. Incorrect actuation preventing use (Availability)

Interactions
← Data Analysis: Receiving commands
← Power Management: Storage: Providing power
← Fuel Storage: Providing fuel for engines

Actuators: Physical Interactions—Satellites can be equipped with mechanical components which allows physical interactions with other objects in space including non-cooperative objects (such as debris or defunct satellites), supporting docking activities by grabbing onto approaching satellites and others. Some of these physical interactions will be vital for other components, such as ensuring the orientation of solar panels and radiators are correct.

Example Instantiations
- Robotic Grabbing Arm
- Harpoon
- Docking
- One time actuators (e.g., burn wire)
- Orientation of Solar Panels and Radiators

Example Attacks
1. Trigger actuator at an incorrect time

Interactions
← Data Analysis: Receive commands
→ Thermal: Orienting the radiators

Data Storage—Satellites will need to store data, including (i) the firmware and software used to manipulate the satellite, (ii) maps and navigation information, (iii) information received from other systems, and (iv) other information necessary for different use cases. This data will not be stored in a central location on the satellite and will be stored in multiple locations. Data storage should also be segregated based on the purpose of the data. For example, data from other systems should not be stored in the same location as the satellite's software, but implementation details may mean that this is not the case.

Example Instantiations
- Non-volatile Memory (e.g., Solid State Hard Drives)
- Volatile Memory (e.g., RAM)

Example Attacks
1. Privilege Elevation leading to unauthorised access
2. Installation of unauthorised or un-vetted software [15, Section 3.4.9]
3. Corruption due to high-power microwave [20, p. 3]

Interactions
↔ Wireless Communication: Sending/Receiving Data
↔ Input/Output Port: Sending/receiving data from another satellite
↔ Data Analysis: Providing data to be analysed and storing the analysis result
← Sensing: Receiving sensing data

Data Analysis—To make sense of the data obtained from external sources (such as the sensors) and the data stored locally in the satellite analysis will need to be performed on it. This analysis may use simple conditions to trigger actuators (e.g., if temperate rises above a threshold, then turn on the radiators), but more complicated techniques such as machine learning models will also be used. These machine learning models will become prevalent in satellites due to autonomous deployments. Data analysis also includes processing command and control information sent to the satellite.

Example Instantiations
- Machine Learning models [73] (Motion planning [74])
- Error detection
- Safety monitoring
- Telemetry Production
- Command & Control

Example Attacks
1. Adversarial machine learning
2. Elevation of Privilege

Interactions
↔ Data Storage: Receiving/Sending Data
→ Propulsion, Attitude Control: Sending commands
→ Attitude Control: Sending commands
→ Power Management: Generation: Sending commands

Planetary Robot Sub-architecture

Robots are currently used on a planetary environment for scientific activities such as exploration and analysis of the surface. In this case, the stationary robots or rovers perform the exploration of an unstructured terrain to find and categorise several predefined targets (e.g., mineral content, biological markers). Once the target is identified, a specified activity would be performed on the target depending on the mission objectives, such as drilling or sample capture and return. Future applications may include construction on a planetary surface. In this case, the tasks may be controlled and monitored by an operator (planetary surface station) or performed autonomously by a group of collaborating robots. An RA to capture the functional components and interactions between these components is shown in Figure 2.

This sub-architecture reuses the following components from other sub-architectures:

- Satellite/Data Storage
- Satellite/Data Analysis
- Satellite/Fuel Storage
- Satellite/Power Management: Generation
- Satellite/Power Management: Storage
- Satellite/Thermal

Communication—Like the satellite communication component, this wireless communication component for planetary robots deals with information transmission to satellites and other robots. A difference is that this communication component may include much shorter range peer-to-peer communications between planetary robots. Applying wireless ad-hoc network (WANET) will be useful in a decentralised communication scenario because there is no existing infrastructure for the planetary robots to rely upon. This ad-hoc wireless communication could be implemented via Internet of Things

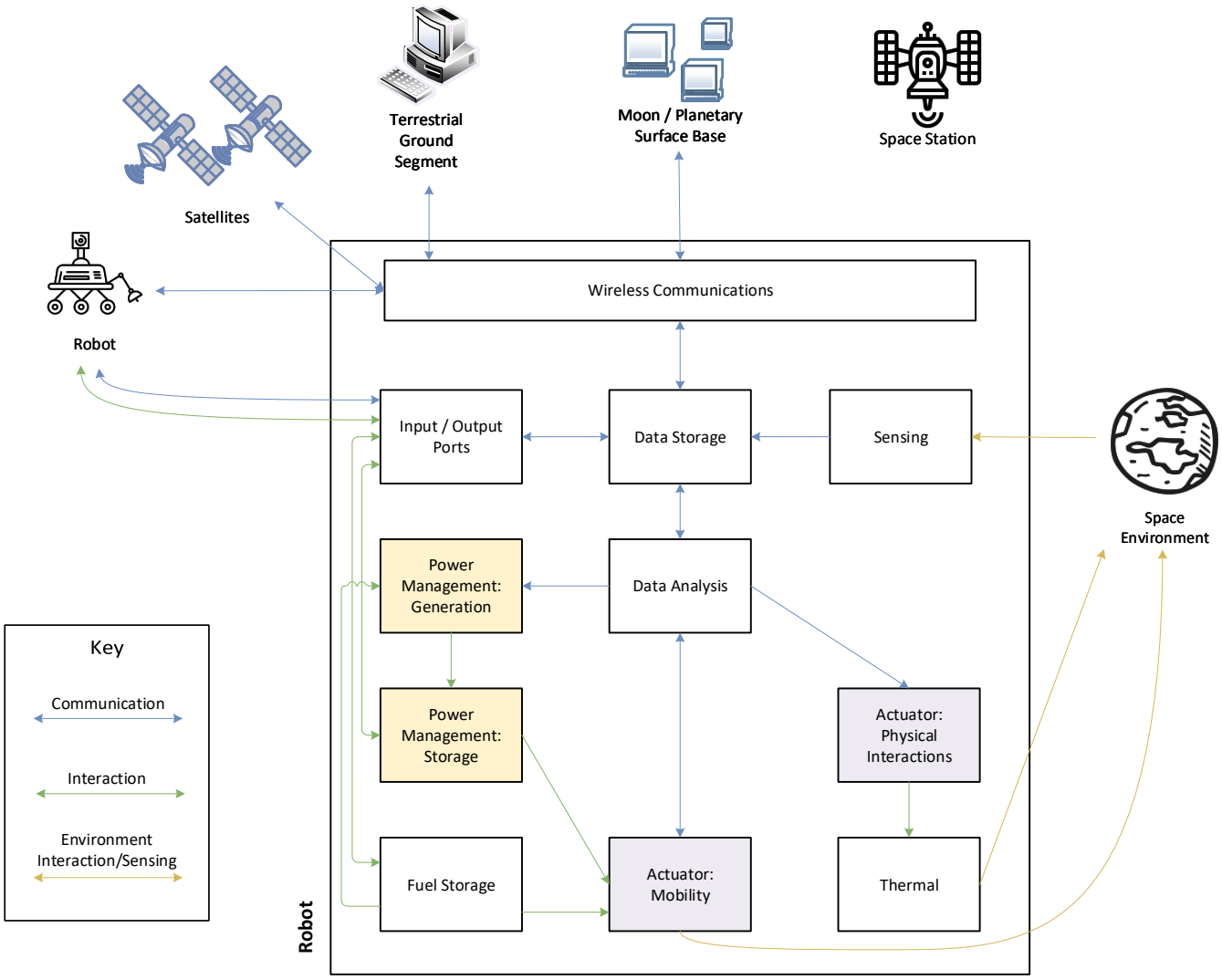

Figure 2. Functional Viewpoint of Robot Reference Architecture

(IoT) technologies [9] such as LoRa [75] or NB-IoT [76]. Reusing this technology could simplify future deployment due to experience gained from terrestrial deployments.

Example Instantiations
- Short Range Omni-directional
- Short Range Directional

Example Attacks
1. Denial of Service (via Jamming)
2. Spoofing
3. Elevation of Privilege (via crafted messages)
4. Replay attacks
5. Sybil attacks

Interactions
↔ Data Storage: Providing the transmission data and reception of data

Sensing—Sensors are one of the key components of planetary robots, as they provide information about the environment that they have been sent to study. Future autonomous planetary robots will be highly reliant on the information collected by the sensors to build a model of the unknown environment. For example, the robot could scan the planet surface to obtain information on the terrain and mineral distribution.

Example Instantiations
- Imaging
- Surface Scanner
- Location
- Radiation

Example Attacks
1. Induce misleading readings (Spoof, Replay, Delay)
2. Blind, Jam
3. Tamper

Interactions
← Environment: Observing the environment state
→ Data Storage: Producing the sensed values

Input/Output Ports— Input/Output ports allow a robot to interact with other robots in both physical and digital ways. They facilitate robots exchanging information in a highly secure manner and also allow resource transfer between them.

Example Instantiations
- Physically Connection between outside devices or inner functional parts.

Example Attacks
1. Pretend to be a robot belonging to a different organisation (Spoofing)

Interactions
↔ Robot/Power Storage, Robot/Fuel Storage: Receiving energy or fuel when physically connected
↔ Robot/Data Storage: Receive and send data to other physically connected robots
↔ Power Management: Storage, Fuel Storage: Providing energy (when physically connected)
↔ Data Storage: Receive and send data to local data storage (when physically connected)

Actuators—This module contains any components that can perform an action with an impact on the physical world. This may include, applying the actuators to grab other robot (arms), mine (drill) and carry objects (cranes).

Example Instantiations
- Robot arms [6]
- Cranes
- Drill [6]
- Sampler [6]
- Wheels

Example Attacks
1. Disable

Interactions
← Data Analysis: Receiving commands
← Power Generation: Providing power
→ Space Environment: Impacting the state of the environment
→ Thermal: Cooling or heating

Mobility—The mobility component provides the capability of physical movement on the planet. This allows a robot to move to and explore different locations of the surface of a planet. Such future application may include goods transportation and mining.

Example Instantiations
- Wheels
- Legs

Example Attacks
1. Disable

Interactions
← Data Analysis: Receiving commands
← Power Generation: Providing power
→ Space Environment: Impact the orientation or position of the vehicle

Ground Segment Sub-architecture

The sub-architecture shown in Figure 3 describes the terrestrial ground segment of a space system, including communication stations, control centres, tracking centres and user terminals (e.g., satellite TV dishes in homes). Aspects such as launch and construction facilities are out of the scope of this reference architecture. As the FAIR-SPACE hub is focusing on orbital, planetary and human-robot interactions, these are the areas in which a security analysis is focused on. A ground segment is a crucial part of that security analysis, hence why it has been included, however other reference architectures or techniques should be used to explore the full range of cyber-physical attacks against the ground segment of space systems.

This sub-architecture reuses the following components from other sub-architectures:

- Satellite/Data Storage

Communications—The ground segment will be capable of communicating with vehicles in space. The terrestrial devices that perform communication will vary in capability, from highly capable devices used by nation states to commercial TV or internet antennas. Changing technology means that more entities have access to devices such as SDRs making it easier to decode satellite communication and also transmit to satellites.

Example Instantiations
- Short Range Omni-directional
- Short Range Directional
- Long Range Directional

Example Attacks
1. Denial of Service (via Jamming)
2. Spoofing
3. Elevation of Privilege (via crafted messages)
4. Replay attacks
5. Sybil attacks

Interactions
↔ Satellite/Communications: Send commands and receive telemetry
↔ Terrestrial Communications:
↔ Data Storage:

Terrestrial Communications—The ground segment will also have communications that interact with local devices (such as via WiFi) and devices across the Internet. Internet connectivity allows multiple physically separate aspects of the ground segment to communicate with each other.

Example Instantiations
- Physical Cable to the Internet
- Wireless LAN

Example Attacks
1. Intrusion into local network [77]

Interactions
↔ Internet: Access to internet
↔ Communications:
↔ Data Storage:

Sensing—The ground segment will perform sensing of the space environment. Some sensing that is performed on Earth will not be trivial to replicate in orbit, so satellites will depend on this information for safe and secure operation. One example application is debris tracking, which provides information on how satellites should alter their orbit to avoid collisions.

Example Instantiations
- Debris Tracking (via optical camera)
- Satellite Tracking

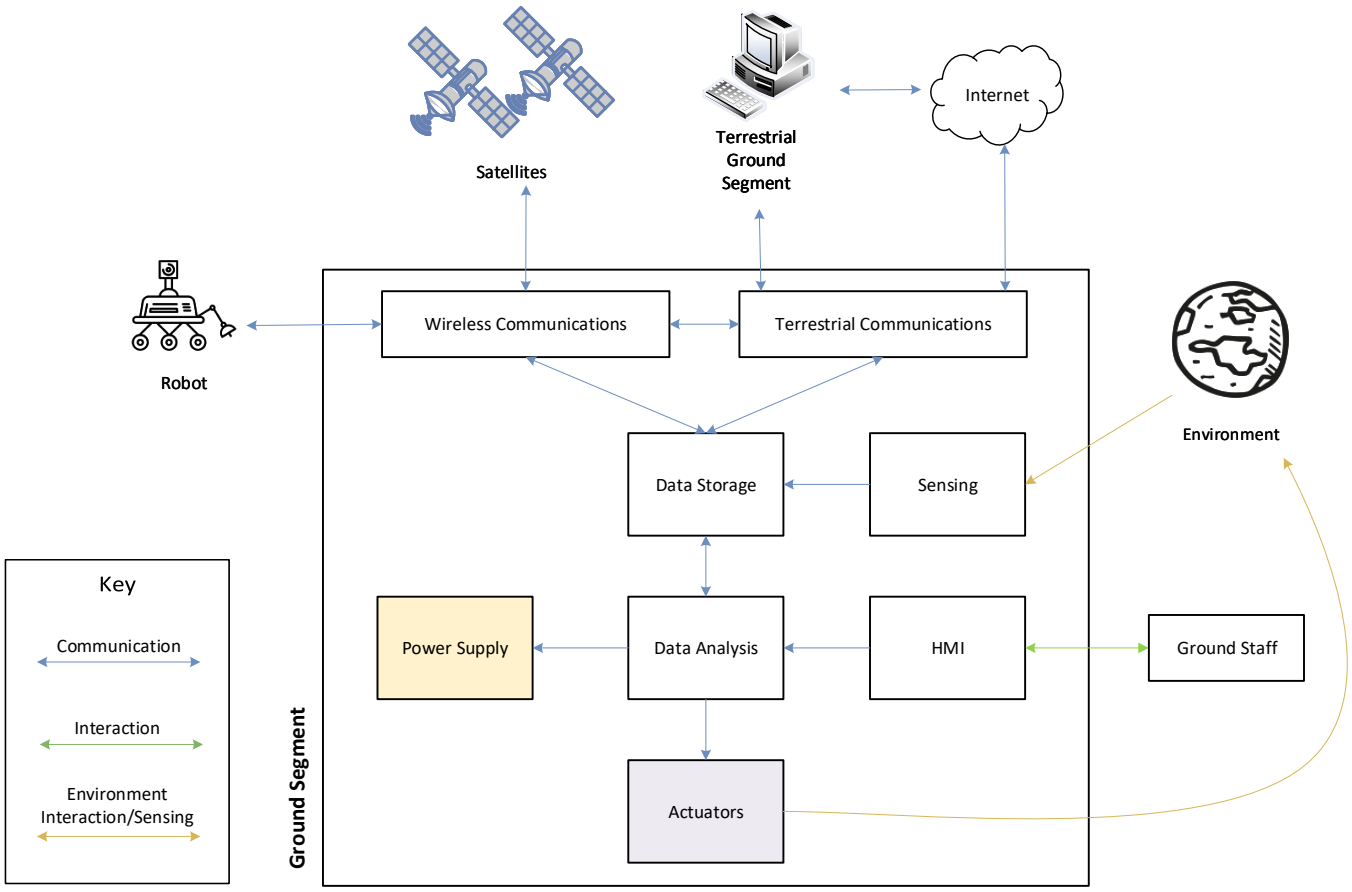

Figure 3. Functional Viewpoint of Ground Segment Reference Architecture

Example Attacks
1. Denial of Service
2. Spoofing

Interactions
← Environment: Observing the state of the space environment
→ Data Storage: Providing the sensed data

Actuators—This module contains any components that can perform an action with an impact on the physical world. One example is a component that changes the angle of the orbital communication antenna in order to adjust the orbital communication window.

Example Instantiations
- Antenna Control

Example Attacks
1. Disable
2. Manipulate

Interactions
← Data Analysis: Receiving commands
→ Environment: Changing environment state

Data Analysis—The data analysis component act as a controlling centre to dealing the information from HMI, sensors and data storage. It acts as a central hub for analysing information and then identification action to perform. As this is a ground station, there will be humans-in-the-loop evaluating and acting on the system analysis and recommendations.

Example Instantiations
- Orbit determination
- Manoeuvre Planning (including debris avoidance)
- Path planning (for non-autonomous planetary robots)
- Calibration Activities[3]

Example Attacks
1. Elevation of Privilege

Interactions
← Data Storage: Providing sensed data for analysis
← HMI: User input
→ Actuators: Controlling actuators

Human Machine Interface (HMI)—The HMI component is a user interface or dashboard that allows a person to provide input to the system and receive information output. While the term can technically be applied to any screen that allows a user to interact with a device, there will be several other ways in which a person can interact with the ground segment system.

Example Instantiations
- User Interface

[3]https://www.esa.int/Our_Activities/Observing_the_Earth/Copernicus/Ground_Segment_overview

Example Attacks
1. Information Disclosure
2. Elevation of Privilege

Interactions
→ Data Analysis: Input commands
← Environment: Receive commands from personnel

Power Supply—The ground segment will be supplied power, typically via a national grid. However, additional power sources such as generators, renewables or batteries in UPSs may be present to supplement mains power for redundancy.

Example Instantiations
- Mains Power
- Generator (e.g., Diesel)
- Renewable Sources (solar, wind, etc.)
- Uninterruptible Power Supply (UPS)

Example Attacks
1. Denial of Service

Interactions
→ *: Providing power to other components

Summary

This section has abstractly described the three sub-architectures of satellites, planetary robots and the ground segment. In order to use this RA to analyse the attack surface of that system it first needs to be defined. The next section will describe the methodology to do the analysis before an example use case is presented.

5. Attack Surface Analysis Methodology

The attack surface of a system comprises of the set of interactions between an internal system component and an external agent. This can be extended to consider the possible attack paths through the system via compromised or vulnerable components. This attack paths provides the sequence of components that needs to be compromised for an adversary to reach its goal. Identifying the components necessary to perform the attack directs system designers to where they need to develop mitigations. In this section, the methodology to use the reference architecture to identify the sequence of components that are necessary to perform the attack is described. This methodology does not perform threat identification. It is necessary to use the output from a threat modelling to supply the list of threats, threat actors and their goals, capabilities and resources. This information is needed to understand if an adversary is capable of performing an attack again a component or interaction between components.

Performing this analysis is broken down into two stages. The first stage builds the concrete system and identifies the environment for the use case. The second stage performs the attack surface analysis which outputs attack trees in the process. These attack trees specify the attack path required for a threat actor to achieve a goal. This is different from a goal-centric approach, where the analysis would start from the compromised components needed to achieve the goal and work backwards. Instead, the analysis starts from outside the system and works inwards towards the goal.

Stage 1:

1. Identify the use case that will be analysed.
2. Identify the environment in which the use case will operate.
3. Instantiate the abstract components with the relevant components to provide the functionality required by the use case.
4. Specify the interactions between concrete components. What data/commands/interactions do they represent?

From a threat modelling, identify the specific threat actors who are interested in attacking this system. For each threat actor, specify its goals, capabilities, motivations, environment and resources.

Stage 2:

1. Identify all interactions that cross the boundary of the system.
2. For each of these components specify how they could be compromised or attacked.
3. Check to see if this attack path achieves one of the goals specified in stage 1.
4. Repeat from step 1, but instead identify interactions that can attacker can take from the compromised or attacked component.

Once stages 1 and 2 are complete attack trees can be created to represent the path of compromise an attacker would need to take through the system to achieve its goals. These attack trees help identify where efforts need to be focused on to develop mitigation to the identified attack.

Threat Modelling

As performing attack surface analysis using a reference architecture requires input from threat modelling, it is necessary for a light threat modelling to be performed for our use case analysis. Therefore, this section will give a brief and high-level description of threat modelling before it is performed for the use case analysis in the next section.

Threat modelling is the structured process of identifying a system's vulnerabilities, threat actors, cyber risks and impacts as well as recommending appropriate countermeasures. An effective threat modelling approach clarifies threat actor capabilities, intentions, and the conditions which should present for the attacks to be realised and create the impacts. It also provides a vision of how the countermeasures may help to mitigate the impact of the attacks. To analyse the attack surface of specific instantiations (i.e., assets or functionality) of the reference architecture, it is necessary to understand primarily who the threat actors are and what their goals are. It is also important to understand other aspects of the threat actor such as their motivations, capabilities, resources and more.

The RA is used as a tool in our threat modelling approach to identify the system's potential entry points and its functionality with respect to functional components, communication and interactions. Thereafter, the assessment of potential threats has been done by considering the examples in the literature and the evolution of the system ecosystem for the system use cases. The potential threats have been classed by using the classification of STRIDE [78] and mapped with the threat actors classification which is presented in Table 2. Finally, the high-level attack trees have been plotted for each threat scenario.

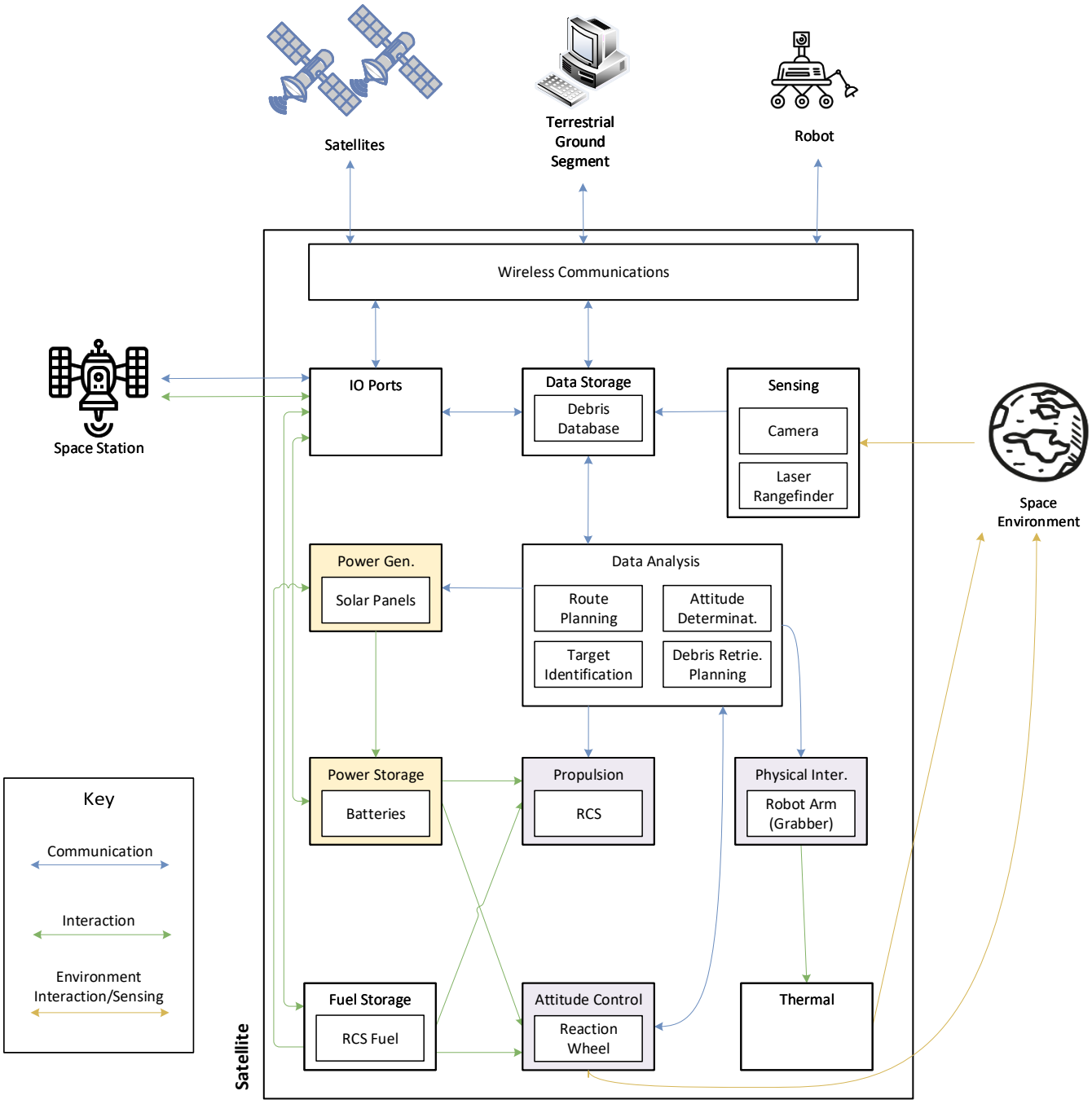

Figure 4. Instantiation of Functional Viewpoint of Satellite Reference Architecture for Autonomous Debris Collection

6. Use Case Analysis

To demonstrate how to perform the attack surface analysis we describe an example system that performs autonomous debris collection. Such a system is used to reduce the potential for collisions with this debris [79]. There have been several different techniques considered to collect and remove debris, from capturing with arms or nets [80] to electro-dynamic tethers [81] and others. For this use case we focus on an autonomous satellite that physically captures and de-orbits debris where there is no human-in-the-loop controlling the satellite. This system could rely upon ground-based debris detection, but autonomous systems might also consider in-orbit sensors [82].

We have used the reference architecture presented in Figures 4 and 5 to model the functional components of autonomous debris collection. Using this instantiated reference architecture and output from a threat modelling, attacks that aim to prevent autonomous debris collection satellite finding/rendezvousing with debris will be analysed.

The European Space Agency (ESA) estimates there are nearly 129 million different pieces of debris in space [83]. Such objects move at high velocity in the Low Earth Orbit (LEO)

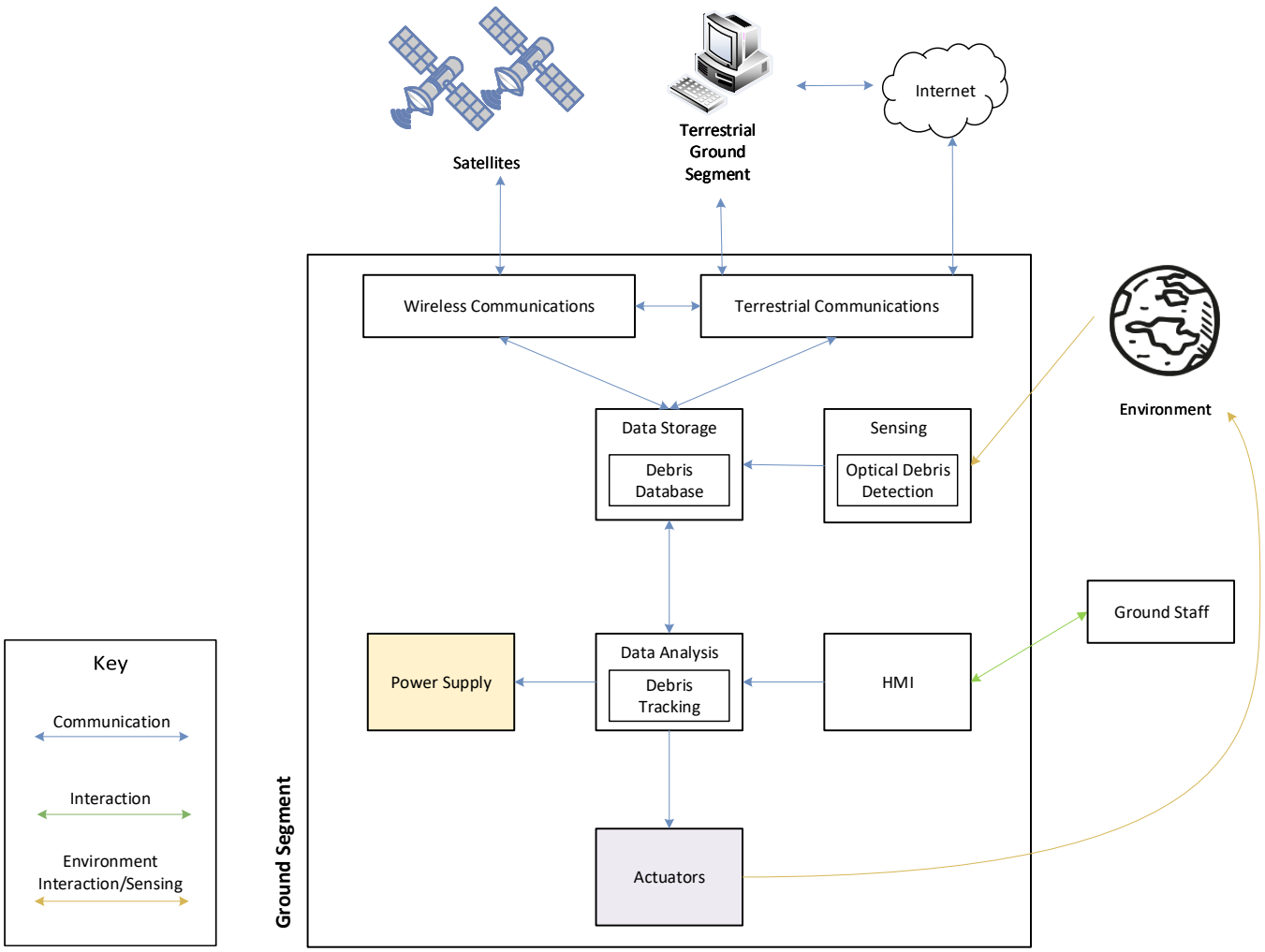

Figure 5. Instantiation of Functional Viewpoint of Ground Segment Reference Architecture for Autonomous Debris Collection

and even very small objects with a size of millimetres can cause damage. Approximately 22000 objects have been catalogued with physical information (mass, size, shape) and are being regularly tracked in ESA's Database and Information System Characterising Objects in Space (DISCOS) [84]. The information in the database is necessary for the task of autonomous debris collection due to the satellites needing to perform target debris identification, route planning, attitude determination, and debris retrieving planning. A potential data poisoning attack on this database before it is sent to the autonomous satellite can hinder such assignments. Furthermore, due to the large quantity of existing space debris, the cooperative space debris collection can be operated collaboratively between satellites. These satellites may be owned by multiple different organisations/companies, but need to cooperate for their mutual benefit. A group of satellites may decide among themselves which of them will collect particular objects and de-orbit them according to the satellite's resources (power, remaining fuel) and distance to the debris. However, it is possible a satellite may misinform others in the group about its operation to gain financial benefit or introduce non-existent debris to cause fuel wastage to rival satellites.

Discussion

Our threat modelling is comprised of two steps: the first step is identifying all system functions with relevant components, and the second step is identifying corresponding threats to these functions with respect to a use case. We focus on autonomous space debris collection as an example in this study due to the growing debris collusion risks in orbits around the planet [85].

The attack surface of autonomous debris collection use-case can be divided into three as (i) space debris database in the ground segment, (ii) satellite-to-ground segment communication, and (iii) satellite. Different attacks can be conducted in these attack surfaces. The classifications of attacks has been borrowed from STRIDE [78]. The brief description of the threat classes are:

- Spoofing: It refers to falsifying the identity of person or data of an object. Threat actors can spoof a configuration, file, machine, sensory data, or the role of a person.
- Tampering: It refers to intentionally changing the content of data to cause an incorrect operation in the system. Threat actors can tamper files, sensory data, or network.
- Reputation: It refers to the actions of threat actors that cannot be traced. It is associated with the logging system.
- Information disclosure: It refers gaining unauthorised

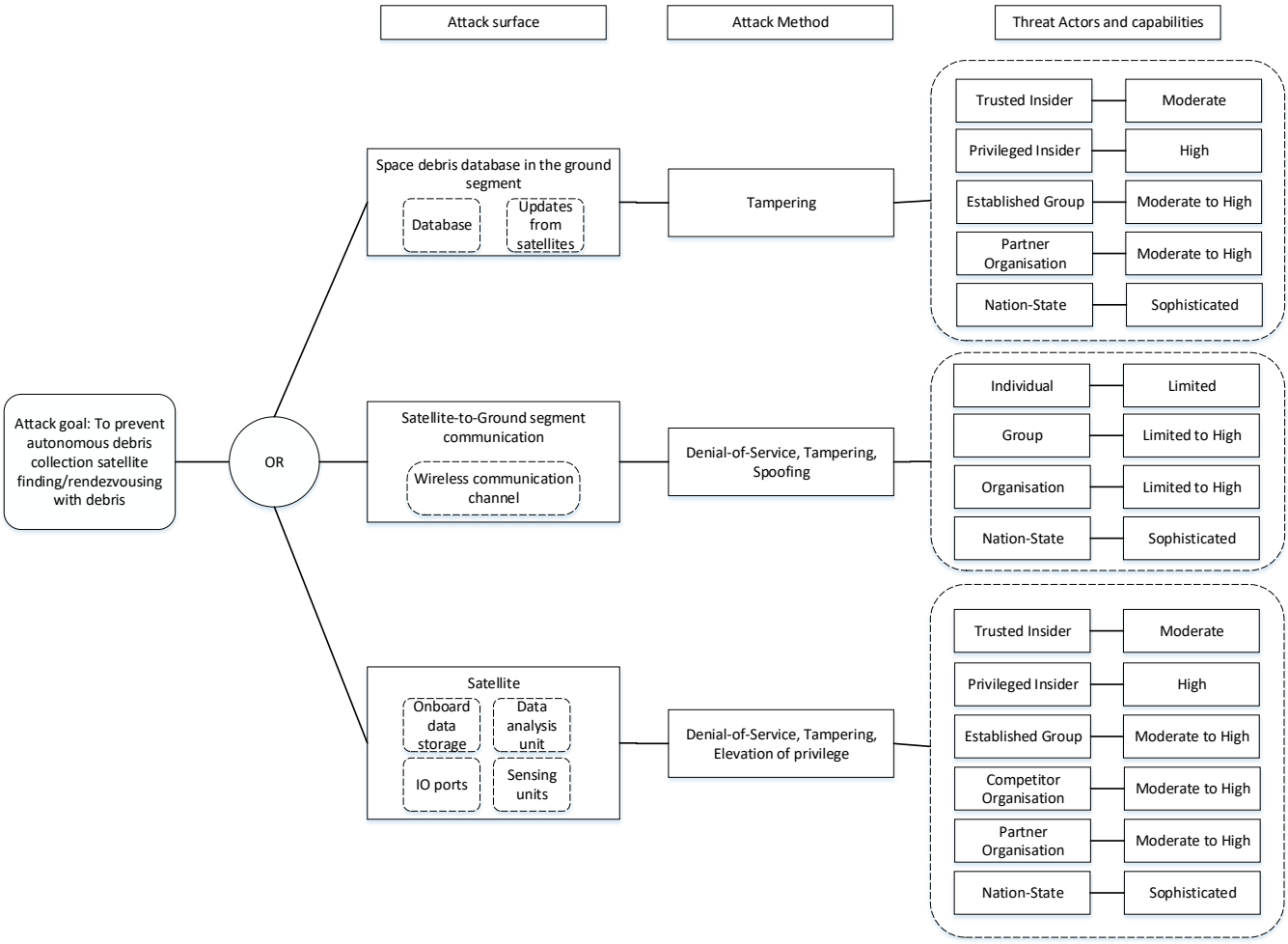

Figure 6. Attack Tree for adversary aiming to prevent autonomous debris collection

access to the data storage or data flow.

- Denial of service: It refers to interrupting the regular operation of the system. It is a common type of cyber-attack, which can be implemented by preventing system resources with fake requests.
- Elevation of privilege: It refers to performing an unauthorised action by a threat actor.

Space debris has been catalogued in databases with identification information such as a unique object identifier, and a set of attributes such as epoch, shape, size, mass, type, and environment solar and geomagnetic activity data [86]. This information is not only necessary for the satellites performing debris collection but also for planning space missions since small object may cause significant damage. In the autonomous debris collection use case being considered, there are a number of threats such as system may be vulnerable to. In order to identify these threats it is first important to understand who the threat actors are (an exploration is shown in Table 2) and what their goals, motivations, resources and capabilities are.

The primary attack surface considered for this use-case is the satellite-to-ground segment wireless communication channel as shown in Figure 6 by an attack tree. The satellites receives information about debris positions from the database in the ground segment, which is then stored in their on-board data storage unit, and the debris database is updated accordingly. Based on this communication, a number of attacks could be made:

- The communication channel can be jammed (DoS) to prevent commands or database updates from being delivered to the satellite, or telemetry received from it.
- Software updates could be maliciously falsified (tampering) cause fuel wastage or financial impact to rivals.
- The communication channel could be remotely spoofed by a threat actor.
- Jamming attacks are possible with limited capabilities and resources, especially when considering the changes in the space ecosystem in terms of increasing connectivity and reducing costs (see Table 1).
- Tampering attacks usually require higher capabilities and resources.

Autonomous debris collection can be also prevented by conducting attacks on the collection satellite in situ. Unlike the other attack surfaces, elevation of privilege can be exploited through entry points such as IO ports and wireless communications. The satellite's on-board sensors can also be blinded (DoS). The likelihood of occurrence of these attacks is fairly low for when considering the majority of existing threat actors (except for nation-state level threat actors). However, as

NewSpace will reduce barriers to deployment, the likelihood of these threats will rise in the near future. Therefore, it is important to consider these threats due to the need for high fault tolerance of space missions [87].

7. Discussion

Further Components for Reference Architecture

In this work we have focused on three core components in a space system, that is, (i) satellites in orbit, (ii) planetary robots and (iii) the terrestrial ground segment. However, these core components have intentionally avoided considering human aspects of spaceflight in order to focus on robotic and computer systems. In future work, this reference architecture will be extended to consider systems such as orbital and planetary stations that support life and also consider other human elements such as spacesuits.

Further Scenarios to Consider

The reference architecture developed in this work has focused on analysing systems that are currently deployed. This work has not considered the period of time where devices are being launched, transferring to the location they will operate, or during descent. These will be vital scenarios to consider cyber security aspects within, due to their mission due to their mission critical nature. However, analysing these scenarios will require specifying additional contextual information. Therefore, we will focus on analysing these scenarios in future work.

This RA has focused on the functionality of system components and interactions between functionality that comprise individual entities in a space system. It has intentionally not considered threats based on system implementations. This means that vulnerabilities in software, supply chain tampering and other implementation issues cannot be analysed using this approach. This is intentional, as this RA is intended to be used for a high-level analysis and other approaches will be more suitable for low-level analyses.

8. Conclusion

In this paper, we have identified that the space industry is currently changing or is likely to change in the future in terms of the connectivity of space systems, the autonomy of those systems and the culture around commercialisation and innovation. These are affecting many dimensions of the space ecosystem, from the cost of deployment to the introduction of novel capabilities, which are having a further impact on the threat landscape for space systems. In order to represent and analyse the path of compromise, an adversary will need to take to achieve their objectives, we propose using a hybrid functional-interaction viewpoint of a reference architecture. This reference architecture has then been demonstrated using an example of future use case of autonomous debris collection. The output of this analysis can then be used to identify key functional aspects of a system where mitigations will need to be employed.

Acknowledgments

The authors would like to thank Chen Gu for assistance in creating early versions of the reference architecture diagrams and Daniel Fowler for proofreading this paper.

This work is supported by grant EP/R026092 (FAIR-SPACE Hub) through UKRI under the Industry Strategic Challenge Fund (ISCF) for Robotics and AI Hubs in Extreme and Hazardous Environments.

References

[1] A. Cornell, "Five key turning points in the american space industry in the past 20 years: Structure, innovation, and globalization shifts in the space sector," *Acta Astronautica*, vol. 69, no. 11-12, pp. 1123–1131, 2011.

[2] G. Martin, "NewSpace: The emerging commercial space industry," 2015, Accessed: 2019-11-19. [Online]. Available: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20160001188.pdf

[3] SpaceX, "Smallsat Rideshare Program," 2019, Accessed: 2019-09-06. [Online]. Available: https://www.spacex.com/smallsat

[4] ——, "Smallsat Rideshare Program," Aug. 2019, Accessed: 2019-09-09, via the Internet Archive. [Online]. Available: https://web.archive.org/web/20190805190003/https://www.spacex.com/smallsat

[5] C. Pomeroy, A. Calzada-Diaz, and D. Bielicki, "Fund me to the moon: Crowdfunding and the new space economy," *Space Policy*, vol. 47, pp. 44–50, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0265964616300418

[6] Y. Gao, D. Jones, R. Ward, E. Allouis, and A. Kisdi, "Space Robotics & Autonomous Systems: Widening the horizon of space exploration," UK Robotics & Autonomous Systems Network, Tech. Rep., 2018. [Online]. Available: https://www.fairspacehub.org/s/space_robotics_autonomous_systems.pdf

[7] A. T. Klesh, J. W. Cutler, and E. M. Atkins, "Cyber-physical challenges for space systems," in *2012 IEEE/ACM Third International Conference on Cyber-Physical Systems*. IEEE, 2012, pp. 45–52.

[8] I. F. Akyildiz and A. Kak, "The internet of space things/cubesats: A ubiquitous cyber-physical system for the connected world," *Computer Networks*, vol. 150, pp. 134–149, 2019.

[9] CORDIS, "Space IoT takes off," Jul. 2018, Accessed: 2019-09-08. [Online]. Available: https://phys.org/news/2018-07-space-iot.html

[10] J. J. Klein, "Rethinking Requirements and Risk in the New Space Age," Center for a New American Security, Jan. 2019, Accessed: 2019-11-19. [Online]. Available: https://www.cnas.org/publications/reports/rethinking-requirements-and-risk-in-the-new-space-age

[11] E. Quintana, "The new space age: Questions for defence and security," *The RUSI Journal*, vol. 162, no. 3, pp. 88–109, 2017.

[12] H. S. Lallie, K. Debattista, and J. Bal, "An empirical evaluation of the effectiveness of attack graphs and fault trees in cyber-attack perception," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1110–1122, 2017.

[13] K. Ghirardello, C. Maple, D. Ng, and P. Kearney, "Cyber security of smart homes: Development of a reference architecture for attack surface analysis," *Living in the Internet of Things: Cybersecurity of the IoT*, 2018.

[14] C. Maple, M. Bradbury, A. T. Le, and K. Ghirardello, "A connected and autonomous vehicle reference architecture for attack surface analysis," *Appl. Sci.*, 2019, To Appear.

[15] CCSDS, "Security Threats against Space Missions," The Consultative Committee for Space Data Systems (CCSDS), Informational Report, Dec. 2015, CCSDS

350.0-G-3. [Online]. Available: https://public.ccsds.org/Pubs/350x1g2.pdf
[16] R. S. Ross, "Guide for Conducting Risk Assessments," National Institute of Standards and Technology, Tech. Rep., Sep. 2012, SP 800-30 Rev. 1.
[17] B. Unal, "Cybersecurity of NATO's Space-based Strategic Assets," Chatham House, resreport, Jul. 2019. [Online]. Available: https://www.chathamhouse.org/publication/cybersecurity-nato-s-space-based-strategic-assets
[18] G. Falco, "Job One for Space Force: Space Asset Cybersecurity," Belfer Center, Harvard Kennedy School, Belfer Center for Science and International Affairs, Harvard Kennedy School, 79 JFK Street, Cambridge, MA 02138, resreport, Jul. 2018. [Online]. Available: https://www.belfercenter.org/sites/default/files/files/publication/CSP%20Falco%20Space%20Asset%20-%20FINAL.pdf
[19] ——, "Cybersecurity principles for space systems," *Journal of Aerospace Information Systems*, vol. 16, no. 2, pp. 61–70, 2019.
[20] T. Harrison, K. Johnson, and T. G. Roberts, "Space Threat Assessment 2018," Center for Strategic & International Studies, techreport, Apr. 2018. [Online]. Available: https://aerospace.csis.org/spacethreat2018
[21] T. Harrison, K. Johnson, T. G. Roberts, M. Bergethon, and A. Coultrup, "Space Threat Assessment 2019," Center for Strategic & International Studies, techreport, Apr. 2019. [Online]. Available: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190404_SpaceThreatAssessment_interior.pdf
[22] Ministére des Armées, *Stratégie Spatiale de Défense*, 2019. [Online]. Available: https://www.defense.gouv.fr/content/download/563617/9727377/Synthe%CC%80se%20strate%CC%81gie%20spatiale%20de%20de%CC%81fense%202019.pdf
[23] C. Mackenzie, "France plans to boost its self-defense posture in space," *Defense News*, Jul. 2019, Accessed: 2019-08-08. [Online]. Available: https://www.defensenews.com/global/europe/2019/07/26/france-plans-to-boost-its-self-defense-posture-in-space/
[24] A. Kurzrok, M. D. Ramos, and F. Mechentel, "Evaluating the Risk Posed by Propulsive Small-satellites with Unencrypted Communications Channels to High-Value Orbital Regimes," in *32nd Annual AIAA/USU Conference on Small Satellites*, 2018, SSC18-XI-05.
[25] CCSDS, "Security Guide for Mission Planners," The Consultative Committee for Space Data Systems (CCSDS), Informational Report, Apr. 2019, CCSDS 350.7-G-2. [Online]. Available: https://public.ccsds.org/Pubs/350x7g2.pdf
[26] ——, "CCSDS Guide for Secure System Interconnection," The Consultative Committee for Space Data Systems (CCSDS), Informational Report, Apr. 2019, CCSDS 350.4-G-2. [Online]. Available: https://public.ccsds.org/Pubs/350x4g2.pdf
[27] ——, "The Application of Security to CCSDS Protocols," The Consultative Committee for Space Data Systems (CCSDS), Informational Report, Mar. 2019, CCSDS 350.0-G-3. [Online]. Available: https://public.ccsds.org/Pubs/350x0g3.pdf
[28] J. Windsor, K. Eckstein, P. Mendham, and T. Pareaud, "Time and space partitioning security components for spacecraft flight software," in *2011 IEEE/AIAA 30th Digital Avionics Systems Conference*, Oct 2011, pp. 8A5–1–8A5–14.
[29] A. Roy-Chowdhury, J. S. Baras, M. Hadjitheodosiou, and S. Papademetriou, "Security issues in hybrid networks with a satellite component," *IEEE Wireless Communications*, vol. 12, no. 6, pp. 50–61, Dec 2005.
[30] B. Schneier, "Secret and lies," *Digital Security in a Networked World*, 2000.
[31] E. Alaña, J. Herrero, S. Urueña, K. Macioszek, and D. Silveira, "A reference architecture for space systems," in *Proceedings of the 12th European Conference on Software Architecture: Companion Proceedings*, ser. ECSA '18. New York, NY, USA: ACM, 2018, pp. 11:1–11:2.
[32] V. Bos, A. Rugina, and A. Trcka, "On-Board Software Reference Architecture for Payloads," in *DASIA 2016 - Data Systems In Aerospace*, ser. ESA Special Publication, vol. 736, Aug 2016, p. 38.
[33] M. Panunzio and T. Vardanega, "On software reference architectures and their application to the space domain," in *Safe and Secure Software Reuse*, J. Favaro and M. Morisio, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 144–159.
[34] European Space Software Repository, "OSRA - Onboard Software Reference Architecture," 2019, Accessed: 2019-09-09. [Online]. Available: https://essr.esa.int/project/osra-onboard-software-reference-architecture
[35] P. Shames and T. Yamada, "Tools for Describing the Reference Architecture for Space Data Systems," Jet Propulsion Laboratory, Tech. Rep., 2004. [Online]. Available: https://trs.jpl.nasa.gov/bitstream/handle/2014/38436/04-0804.pdf?sequence=1&isAllowed=y
[36] *The ISECG Reference Architecture for Human Lunar Exploration*, ISECG International Architecture Working Group, Jul. 2010. [Online]. Available: https://www.lpi.usra.edu/lunar/strategies/ISECGLunarRefArchitectureJuly2010.pdf
[37] B. G. Drake, S. J. Hoffman, and D. W. Beaty, "Human exploration of mars, design reference architecture 5.0," in *2010 IEEE Aerospace Conference*, March 2010, pp. 1–24.
[38] A. W. Wymore, *Model-based systems engineering*. CRC press, 1993.
[39] A. Menchinelli, F. Ingiosi, L. Pamphili, P. Marzioli, R. Patriarca, F. Costantino, and F. Piergentili, "A Reliability Engineering Approach for Managing Risks in CubeSats," *Aerospace*, vol. 5, no. 4, 2018. [Online]. Available: https://www.mdpi.com/2226-4310/5/4/121
[40] R. J. Duphily, "Space Vehicle Failure Modes, Effects, and Criticality Analysis (FMECA) Guide," Space and Missile Systems Center, Tech. Rep., 2009, AEROSPACE REPORT NO. TOR-2009(8591)-13. [Online]. Available: http://aerospace.wpengine.netdna-cdn.com/wp-content/uploads/2015/04/TOR-20098591-13-Space-Vehicle-Failure-Modes-Effects-and-Criticality-Analysis-FMECA-Guide.pdf
[41] NASA, "Magellan Flight System Block Diagram," Accessed: 2019-09-10. [Online]. Available: https://solarsystem.nasa.gov/bosf/images/11_08-Magellan-SF-Func-Block600x631.jpg
[42] *Unified Modeling Language*, Object Management Group, Dec. 2017, Version 2.5.1. [Online]. Available: https://www.omg.org/spec/UML/2.5.1/PDF
[43] *OMG Systems Modeling Language*, Object Management Group, May 2017, Version 1.5. [Online]. Available: http://www.sysml.org/docs/specs/OMGSysML-v1.5-17-05-01.pdf
[44] S. Ouchani and G. Lenzini, "Attacks generation by detecting attack surfaces," *Procedia Computer Science*, vol. 32, pp. 529–536, 2014, the 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014), the 4th International Conference on Sustainable

Energy Information Technology (SEIT-2014).
[45] L. Apvrille and Y. Roudier, "Sysml-sec attack graphs: Compact representations for complex attacks," in *Graphical Models for Security*, S. Mauw, B. Kordy, and S. Jajodia, Eds. Cham: Springer International Publishing, 2016, pp. 35–49.
[46] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, Apr. 2015.
[47] T. Braun, B. C. Fung, F. Iqbal, and B. Shah, "Security and privacy challenges in smart cities," *Sustainable Cities and Society*, vol. 39, pp. 499 – 507, 2018.
[48] M. Hashem Eiza and Q. Ni, "Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity," *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 45–51, June 2017.
[49] A. Budianu, T. J. W. Castro, A. Meijerink, and M. J. Bentum, "Inter-satellite links for cubesats," in *2013 IEEE Aerospace Conference*, March 2013, pp. 1–10.
[50] J. Aschbacher and M. P. Milagro-Pérez, "The european earth monitoring (gmes) programme: Status and perspectives," *Remote Sensing of Environment*, vol. 120, pp. 3 – 8, 2012, the Sentinel Missions - New Opportunities for Science.
[51] H. W. Jones, "The Recent Large Reduction in Space Launch Cost," in *48th International Conference on Environmental Systems*, Albuquerque, New Mexic, Jul. 2018. [Online]. Available: https://ttu-ir.tdl.org/bitstream/handle/2346/74082/ICES_2018_81.pdf
[52] M. Weinzierl, "Space, the Final Economic Frontier," *Journal of Economic Perspectives*, vol. 32, no. 2, pp. 173–192, May 2018.
[53] C. Anderson, "Rethinking public-private space travel," *Space Policy*, vol. 29, no. 4, pp. 266 – 271, 2013.
[54] Bryce Space and Technology, "Global Space Industry Dynamics," Bryce Space and Technology, Alexandria, VA, USA, Tech. Rep., Mar. 2019. [Online]. Available: https://www.industry.gov.au/sites/default/files/2019-03/global_space_industry_dynamics_-_research_paper.pdf
[55] Satellite Applications Catapult, "Accessing Satellite Data," Accessed: 2019-10-15. [Online]. Available: https://sa.catapult.org.uk/work-with-us/our-capabilities/accessing-satellite-data/
[56] ESA, "Observing the Earth: How to Access Data," Accessed: 2019-10-15. [Online]. Available: https://www.esa.int/Applications/Observing_the_Earth/How_to_access_data
[57] L. K. Johnson, J. Hollman, J. McClellan, and P. Fisher, "Utilizing cubesat architecture and innovative low-complexity devices to repurpose decommissioned apertures for rf communications," in *AIAA SPACE 2013 Conference and Exposition*, San Diego, CA, USA, Sep. 2013.
[58] NASA, "Science Team Outlines Goals for NASA's 2020 Mars Rover," Jul. 2013, Accessed: 2019-10-15. [Online]. Available: https://www.nasa.gov/mission_pages/mars/news/mars20130709.html
[59] ——, "Mars Helicopter to Fly on NASA's Next Red Planet Rover Mission," May 2018, Accessed: 2019-10-14. [Online]. Available: https://www.nasa.gov/press-release/mars-helicopter-to-fly-on-nasa-s-next-red-planet-rover-mission
[60] NASA Engineering & Safety Center, "The nesc 2014 technical update," NASA, Hampton, VA, USA, Tech. Rep., 2014. [Online]. Available: https://www.nasa.gov/sites/default/files/atoms/files/techup2014_pdf9-1pageview.pdf
[61] Q. Do, B. Martini, and K.-K. R. Choo, "The role of the adversary model in applied security research," *Computers & Security*, vol. 81, pp. 156–181, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404818306369
[62] *European Data Relay System: The Space Data Highway*, ESA, Dec. 2018, Accessed: 2019-08-07. [Online]. Available: https://esamultimedia.esa.int/docs/telecom/EDRS_factsheet_EN.pdf
[63] H. Kaushal and G. Kaddoum, "Applications of lasers for tactical military operations," *IEEE Access*, vol. 5, pp. 20 736–20 753, Sep. 2017.
[64] I. Rekleitis, E. Martin, G. Rouleau, R. L'Archevêque, K. Parsa, and E. Dupuis, "Autonomous capture of a tumbling satellite," *Journal of Field Robotics*, vol. 24, no. 4, pp. 275–296, 2007.
[65] Q. Yang and L. Huang, *Satellite Communication*. Singapore: Springer Singapore, 2018, pp. 343–369.
[66] S. Nie, L. Liu, and Y. Du, "Free-fall: Hacking tesla from wireless to CAN bus," in *Black Hat*, 2017. [Online]. Available: https://www.blackhat.com/docs/us-17/thursday/us-17-Nie-Free-Fall-Hacking-Tesla-From-Wireless-To-CAN-Bus-wp.pdf
[67] S. P. Protocol, "Recommendation for space data system standards," CCSDS 133.0-B-1. Blue Book, Tech. Rep., 2003.
[68] I. Lasc, R. Dojen, and T. Coffey, "Countering jamming attacks against an authentication and key agreement protocol for mobile satellite communications," *Computers & Electrical Engineering*, vol. 37, no. 2, pp. 160–168, 2011.
[69] A. Roy-Chowdhury, J. S. Baras, M. Hadjitheodosiou, and S. Papademetriou, "Security issues in hybrid networks with a satellite component," *IEEE Wireless Communications*, vol. 12, no. 6, pp. 50–61, 2005.
[70] A. Dutta and P. Tsiotras, "Egalitarian peer-to-peer satellite refueling strategy," *Journal of Spacecraft and Rockets*, vol. 45, no. 3, pp. 608–618, 2008.
[71] R. H. Jansen and T. P. Dever, "G2 Flywheel Module Design," in *Second International Energy Conversion Engineering Conferencesponsored by the American Institute of Aeronautics and Astronautics*, Providence, Rhode Island, Aug. 2016, NASA/CR–2006-213862. [Online]. Available: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20060028492.pdf
[72] J. Si, Y. Gao, and A. Chanik, "Feedback slew algorithms for prolate spinners using single–thruster," *Acta Astronautica*, vol. 144, pp. 39 – 51, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0094576516312358
[73] A. Nanjangud, P. C. Blacker, S. Bandyopadhyay, and Y. Gao, "Robotics and ai-enabled on-orbit operations with future generation of small satellites," *Proceedings of the IEEE*, vol. 106, no. 3, pp. 429–439, March 2018.
[74] Y. Yang, W. Merkt, V. Ivan, and S. Vijayakumar, "Planning in time-configuration space for efficient pick-and-place in non-static environments with temporal constraints," in *2018 IEEE-RAS 18th International Conference on Humanoid Robots (Humanoids)*, Nov 2018, pp. 1–9.
[75] M. Bor, J. Vidler, and U. Roedig, "Lora for the internet of things," in *Proceedings of the 2016 International Conference on Embedded Wireless Systems and Networks*, ser. EWSN '16. USA: Junction Publishing, 2016, pp. 361–366. [Online]. Available: http://dl.acm.org/citation.cfm?id=2893711.2893802
[76] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, and A. Ghosh, "Nb-iot system for m2m communication," in

2016 IEEE Wireless Communications and Networking Conference, April 2016, pp. 1–5.
[77] BBC, "Raspberry Pi used to steal data from NASA lab," Jun. 2019, Accessed: 2019-07-08. [Online]. Available: https://www.bbc.co.uk/news/technology-48743043
[78] A. Shostack, "Experiences threat modeling at microsoft." in *MODSEC@ MoDELS*, 2008.
[79] H. Schaub, L. E. Jasper, P. V. Anderson, and D. S. McKnight, "Cost and risk assessment for spacecraft operation decisions caused by the space debris environment," *Acta Astronautica*, vol. 113, pp. 66 – 79, 2015.
[80] J. L. Forshaw, G. S. Aglietti, N. Navarathinam, H. Kadhem, T. Salmon, A. Pisseloup, E. Joffre, T. Chabot, I. Retat, R. Axthelm, S. Barraclough, A. Ratcliffe, C. Bernal, F. Chaumette, A. Pollini, and W. H. Steyn, "Removedebris: An in-orbit active debris removal demonstration mission," *Acta Astronautica*, vol. 127, pp. 448 – 463, 2016.
[81] S.-I. Nishida, S. Kawamoto, Y. Okawa, F. Terui, and S. Kitamura, "Space debris removal system using a small satellite," *Acta Astronautica*, vol. 65, no. 1, pp. 95–102, 2009.
[82] D. A. Freiwald and J. Freiwald, "Range-gated laser and ICCD camera system for on-orbit detection of small space debris," in *Space Instrumentation and Dual-Use Technologies*, F. A. Allahdadi, M. Chrisp, C. R. Giuliano, W. P. Latham, and J. F. Shanley, Eds., vol. 2214, International Society for Optics and Photonics. SPIE, 1994, pp. 116 – 123.
[83] ESA, "Space debris by the numbers," Accessed: 2019-11-19. [Online]. Available: https://www.esa.int/Safety_Security/Space_Debris/Space_debris_by_the_numbers
[84] R. Jehn, S. Viñals Larruga, and H. Klinkrad, "Discos — The European space debris database," in *44th Congress of the International Astronautical Federation*, Oct. 1993, IAF-93-742.
[85] A. Witze, "The quest to conquer earth's space junk problem," *Nature*, vol. 561, pp. 24–26, Sep. 2018.
[86] H. Klinkrad, "DISCOS - ESA's database and information system characterising objects in space," *Advances in Space Research*, vol. 11, no. 12, pp. 43–52, 1991.
[87] M. Farooq, M. W. Iqbal, T. A. Rana, and N. A. Mian, "Comparative analysis of fault-tolerance techniques for space applications," *VFAST Transactions on Software Engineering*, vol. 3, no. 2, pp. 1–10, 2014.

BIOGRAPHY

Carsten Maple *is Professor of Cyber Systems Engineering in WMG at the University of Warwick, where he is the Director of Research in Cyber Security. Carsten has an international research reputation having published over 200 peer-reviewed papers and his research has attracted millions of pounds in funding and has been widely reported through the media. He is Principal Investigator (PI) at the EPSRC/GCHQ Academic Centre of Excellence in Cyber Security Research, leads various projects on the security of CAVs and is a fellow of the Alan Turing Institute and member of the ENISA CARSEC Expert Group.*

Matthew Bradbury *received his MEng and PhD degrees in computer science from the Department of Computer Science at the University of Warwick, Coventry, UK in 2013 and 2018 respectively. Since 2018 he has been a Research Fellow in WMG, University of Warwick, Coventry, UK. His research interests include security and privacy aspects of Internet of Things, including wireless sensor networks, intelligent transportation systems and space systems. He received the best-in-session award at InfoCom 2017.*

Hu Yuan *is a research fellow in the University of Warwick, where his research focus on the security and privacy aspects of IoT, including internet of bio-nano things, vehicular communication networks, user behaviours identification and further space system. He received his PhD in wireless communications from University of Warwick, UK in 2016, and MSc. in Communications Engineering from University of York, UK in 2012.*

Ugur Ilker Atmaca *received his BSc in electronic and communication engineering from Suleyman Demirel University, Turkey, in 2013. After working in industry, he received his MSc in computer science from the University of Reading, UK, in 2017. He is is currently pursuing the PhD degree at the Warwick Manufacturing Group, the University of Warwick, UK. His research interests include security and privacy in intelligent transportation systems.*

Sara Cannizzaro *Sara Cannizzaro is Research Fellow in WMG at the University of Warwick, where she is carrying out qualitative research on the cybersecurity of Space Systems, the adoption and acceptability of the Smart Home, and trust in Autonomous Vehicles. Prior to this, Sara was a post doc at Middlesex University and the School of Oriental and African Studies (UK), and a lecturer in digital media at London Metropolitan University. She received her PhD in Media and Communications from London Metropolitan University, UK, in 2012. Her research interests include social research methods, digital technology, interdisciplinarity, communication theory, semiotics, pragmatist philosophy.*