Available online at www.sciencedirect.com

ScienceDirect

Advances in Space Research 70 (2022) 2208–2226

ADVANCES IN SPACE RESEARCH (a COSPAR publication)

www.elsevier.com/locate/asr

Challenges in threat modelling of new space systems: A teleoperation use-case

Al Tariq Sheik *, Ugur Ilker Atmaca, Carsten Maple, Gregory Epiphaniou

Secure Cyber Systems Research Group, Warwick Manufacturing Group, University of Warwick, Coventry CV4 7AL, United Kingdom

Received 14 February 2022; received in revised form 18 June 2022; accepted 6 July 2022
Available online 15 July 2022

Abstract

A growing number of adversaries are targeting space missions, and as such, there have been increasing academic and industrial efforts in identifying threats and risks through modelling techniques. In parallel, the research communities are collaborating to lower the entry barriers for space activities to deliver more innovative and cost-effective space missions. This evolution has been termed as New Space. However, this transformation of the space ecosystem has led to changes in the threat landscape, introducing new threat vectors and threat actors intent on compromising space systems and missions. As a result, it is expected that cyber threats could increase against space systems. Furthermore, teleoperation, a significant use case for building extraterrestrial habitats, has already been shown vulnerable in other domains as well. For example, teleoperated robots developed for remote surgery have been shown to be vulnerable to threats, such as malicious control due to an elevation-of-privilege attack. Threat modelling is a systematic and structured method to determine associated system vulnerabilities, possible attack entry points and vectors, and potential impacts on the system. In this work, we examine the efficacy of the de facto threat modelling methods such as STRIDE/DREAD in capturing highly adaptive security requirements and threats from a system-centric perspective for the teleoperation mission scenario. Understanding and protecting these hardware-software assets and their interaction in the mission is of foremost importance since security breaches threaten human safety across the broader New Space ecosystem. This research presents the limitations of existing threat modelling approaches in capturing hardware-software interaction in space systems, which is an open area for scientific enquiry. Moreover, research challenges are raised to improve the safety and security of the teleoperation mission. The output of this work can then be used to develop more appropriate threat modelling approaches to support security requirement engineering for different New Space mission scenarios.
© 2022 Published by Elsevier B.V. on behalf of COSPAR.

Keywords: Threat modelling and risk assessment; New space systems; Teleoperation systems; Internet of space things

1. Introduction

Planetary exploration is a key element of national space strategies. Countries such as the U.S, the U.K, China, Russia and India are discovering opportunities to explore and commercialise space. We are entering a new era – one in which international space agencies are working alongside private industries such as SpaceX, Virgin Galactic and Blue Origin to investigate planetary surfaces and their resources. We are on a mission to build extraterrestrial habitats with base stations. International companies and government-funded agencies would only succeed in deploying space technologies if safe and secure. These initiatives would encourage a new crop of space landers and evolve the business model for space exploration - the one in which private firms could exploit business opportunities. The teleoperation use case is one such technology that would aid in this exploration of planetary surfaces.

* Corresponding author.
E-mail addresses: t.sheik@warwick.ac.uk (A.T. Sheik), ugur-ilker.atmaca@warwick.ac.uk (U.I. Atmaca), cm@warwick.ac.uk (C. Maple), gregory.epiphaniou@warwick.ac.uk (G. Epiphaniou).

https://doi.org/10.1016/j.asr.2022.07.013
0273-1177/© 2022 Published by Elsevier B.V. on behalf of COSPAR.

The use case aims to help manufacturing and assembling on a planetary environment commanded by a remote operator located in a planetary surface base or an orbiting space vehicle. With advancements, connected systems such as these could become vulnerable. To help understand the threats, a reference architecture is illustrated, and then decomposed to hardware and software components using data flow diagrams (DFDs). From this, we aimed to analyse how the teleoperated robot could be a vulnerable system. To do this, threat modelling and risk assessment (TMRA) is performed using STRIDE/DREAD methodology by identifying and evaluating the systems' trust domains.

Threat modelling is a systematic technique to model space systems. It helps determine the robot's strengths and weaknesses by determining their outcomes on their existing controls. Discovering threats and countermeasures is an important objective, where the confirmation of the findings is also achieved to understand the validity and effectiveness of the process. In space systems, both targeted and multi-staged attacks can influence different physical, natural and software components, and it is only over time that we can perceive that sophisticated attacks can impact the system scenarios. Cyber attacks in space systems challenge our ability to comprehend the impact of physical and control procedures; thus, TMRA helps deploy safeguards optimally. Due to the sophistication, criticality and variety of technologies in New Space ecosystems, it is hard to find, examine and assess attack pathways. However, an in-depth understanding of attacks and vulnerabilities is essential for protecting these environments. The process of decomposing the system's responses to attacks can also be another way to monitor and study the system by adversaries. One way to assess this is to demonstrate using DFDs to analyse threats systematically. Alternatively, experimental methods have also been discussed to model threats using discrete-time Markov chains (Abraham and Nair, 2014), state-space (Yang et al., 2016) models and Bayesian networks (Shin et al., 2015).

This paper has identified that telecommunication is the most vulnerable asset for the use case, and universities and research institutions are already exploring ways to secure telecommunication technologies. By performing a systematic risk assessment, the study observes that Jamming, Spoofing, and Man-in-the-middle attacks could cause severe impacts on the system. The paper has identified similarly 97 threats and has classified them based on the risk, which is a result of Damage, Reproducibility, Exploitability, Affected Users and Discoverability of the threats.

Threat modelling informs the management and organisations about perspectives to allocate and invest resources to secure the systems. Such process would further encourage increased efforts in security research in New Space systems to benefit a commercial fleet of space landers and encourage healthy competition for space exploration. This paper explores the teleoperation use case by initially introducing the readers to the motivation and aims. Next, it discusses the related works in which the importance of the New Space era is analysed while explaining its vulnerabilities, hence creating a necessity for space security and security requirements for the teleoperation use case from literature. Next, prominent TMRA methods are analysed for identifying the appropriate approach for the study. Later, this paper summarises the results from TMRA of the teleoperated robot, which helps locate the vulnerabilities in the system and recommend security solutions. Finally, it discusses the limitations of the TMRA methodology.

2. Related work

Nations traditionally controlled the space industry for various technological applications. This era is known as the "Old Space". We are experiencing advanced private companies entering the industry with a more significant investment to compete for space resources (Cornell, 2011). However, security in space is an area that has had limited research in the past. We are currently witnessing space systems being developed with advanced communication and operation for commercialising space. This transition of space for commercialisation is described as the "New Space" (Martin, 2015). Consequently, former security practices may not be suitable for the New Space systems as trust domains are expanding for novel applications such as teleoperated robots use cases (Malik, 2019). Teleoperated robots have various applications, and one such application is that they could be used to build extraterrestrial habitats where the operator can be remotely located. This section will introduce ongoing changes in space and the existing works on the security of the space system and teleoperated robots.

2.1. Security of space systems

Space Systems provide services such as positioning, navigation, timing, and communication. Due to this, any threats to the system may impact the critical operations of a nation that depends on these services. Thus, securing space systems is vital for maintaining a nation's security (Unal, 2019). Prior investigations on space security have revealed that space systems can be vulnerable and targeted by motivated attackers such as adversarial nation-states (Falco, 2018; Falco, 2019; Falco, 2020). As a result, serious considerations have been undertaken to improve the space systems' security (encryption, collaboration, facilitating cyber knowledge sharing, etc.).

Satellite safety and protection could be threatened by technologies such as: (i) kinetic physical, (ii) non-kinetic physical, (iii) electronic equipment (e.g., jamming and spoofing communications), and (iv) cyber attacks, where the adversaries could target the data systems and transmitted data (Harrison et al., 2020; Harrison et al., 2019). On the contrary, defence technologies such as surveillance

cameras, detection abilities, patrolling nano-satellites, and powerful lasers that can be used to blind potential adversaries are being researched for future deployments. As such, offence and defence technologies are being innovated for the New Space era, and it is evident that there exists a greater cyber risk in progressive cyber-physical technologies (Ministére des Armées, 2019; Mackenzie, 2019).

With such evolution in space technologies, new threats must be assessed, and their respective risks are to be quantified systematically. Kurzrok et al. (2018) discuss small satellites systems that do not always encrypt their mission communication links, including telemetry, tracking and control (TTC) data. Therefore, an unauthorised actor could transmit commands to the satellite to manipulate its operation, which may also cause damage for the other dependent satellites that are in contact. In this scenario, either encryption or digital signatures could be used, if required, for ensuring confidentiality and authenticity, respectively.

There has been various guidelines and reports for security applications such as: mission planning (CCSDS, 2019b), systems inter-connectivity (CCSDS, 2019a), application of security protocols (CCSDS, 2019c), and current space cyber security (CCSDS, 2015). However, this paper performs a threat analysis and risk assessment to indicate the drawbacks of the security practices suggested. To do so, these threats, impacts, and mitigation schemes are identified. However, developing a methodology to detect system's compromises in order to achieve security goals remains an open research challenge for emerging space systems such as teleoperated robots.

2.2. Security of teleoperated robots

Teleoperated robots are used as an extension of a human operator in various application domains such as robotic surgery, search and rescue missions, bomb disposal missions, all of which benefit from remotely operated robot arms. They are mainly used for operations where dexterity is important or if there exists a danger for a human. Likewise, teleoperated robots are employed in space systems for a variety of missions, from repairing to exploring. Security impacts on these systems can cost financially where human reach for maintenance of the robot and its associated systems is of a greater challenge, especially on unknown terrain. Thus, securing these systems in advance is essential for space missions' broader security, especially when they are in communication with other New Space systems (Lum et al., 2007; Harnett et al., 2008).

The communication channel is one of the most vulnerable modules in teleoperated robots. The studies in (Amin et al., 2009; Cárdenas et al., 2008) analysed threats and mitigation schemes for network-controlled systems, which could be used for the analysis of teleoperated robots. Moreover, Mo and Sinopili (Mo and Sinopoli, 2009) proposed a Kalman filter based optimal controller for detecting replay and false data injection attacks in the communication link of cyber-physical system (CPS). Coble et al. (2010) proposed a lightweight onboard security mechanism for a robot to verify its received data. Furthermore, Lee and Thuraisingham (2012) utilised the Transport Layer Security (TLS) protocol to ensure confidentiality and authenticity; they also authorised access in the communication link. Lastly, Bonaci et al. (2015) performed an experimental study on threat detection and impact assessment on teleoperated surgical robots, including DoS (Denial-of-Service). However, there is limited research exploring the details of security attacks on teleoperated robots in space systems.

Threat modelling is the structured methodology for identifying a system's vulnerabilities, threat actors, potential risks and impacts, and recommending appropriate countermeasures. The motivation of threat modelling is to analyse the system in a broader view and manage its risks. This includes decision-making by mitigating, avoiding, transferring and accepting risk. The work by CCSDS (2015) has focused on identifying and analysing threats against traditional space systems. Then, Bradbury et al. (2020) analysed emerging threats in New Space Systems. The work by Maple et al. (2020) proposed a methodology to integrate formal verification of functional and safety properties with results of threat modelling to allow quicker convergence to maximise efficiency in the verification of space systems. It is currently evident that the field is in the early stage of analysing cyber risks in the New Space system. These works add further value to the limited research contributions in the field. Furthermore, threat modelling informs new entrants of space scientists interested in protecting the novel technologies in the future.

The implementation of a threat modelling methodology depends on various aspects. Space systems are a sophisticated type of CPS that depends on collaborative computation for physical activities to achieve the objectives of a space mission, such as exploring and observing an extraterrestrial environment (Klesh et al., 2012). In contrast with information systems, CPS in space contains hardware, software, network, and human aspects. Thus, threat modelling should address these aspects during the analysis. Among prominent methodologies, STRIDE (Khan et al., 2017), PASTA (Lee et al., 2021), Composite Threat Modelling (Winsen, 2017), OCTAVE have been considered for our CPS applications. However, there exists a range of limitations in these methodologies.

Jamil et al. (2021b) conducted a validated study on the challenges of threat modelling in CPS, which highlights the following: (i) developing a broad knowledge of threats against physical components in CPS, (ii) limitation of existing methodologies to comprehend multiple hardware and software components of the systems, (iii) limitations of the automated tools, and (iv) current security practices in the organisation considering the publicly known threats. This paper seeks to address the first two challenges by capturing threats that emerge from hardware-software interac-

tion. To do so, we perform a threat analysis and risk assessment on a teleoperated robot system for New Space.

3. Threat modelling methods

Threat modelling methods can be broadly classified into formulae and model-based methods. Formulae based methods consist of asset, vulnerability, and attacker based methods. Model-based methods consist of graph and attacker based methods. This section explains formulae based methods that industries have prominently practised for applied CPS TMRA (Bolovinou et al., 2019; Luo et al., 2021). Model-based methods are not considered since they are beyond the scope of our research.

3.1. STRIDE/DREAD

3.1.1. STRIDE

It is a commonly used method that is developed and used by Microsoft to identify threats as a part of the Security Development Lifecycle (Shostack, 2008). It aids businesses by adapting to the changes during the lifecycle. The name STRIDE is an acronym formed from the initial letters of the threat classes, which are briefly explained below:

- Spoofing: It is the process of falsifying the identity of a person or data. It can be targeted to a configuration, file, machine, sensory data, or a person's role.
- Tampering: It is the process of altering data to cause an incorrect operation in the system. It can be targeted to files, sensory data, or networks.
- Repudiation: It is a process of preventing the trace of actions in the system associated with the log files.
- Information disclosure: It is a process of achieving unauthorised access to a system's data storage or data flow.
- Denial of service: It is a process of interrupting or disrupting the regular operation of the system.
- Elevation of privilege: It is the process of performing an unauthorised action in the system.

Khan et al. (2017) adapted STRIDE to CPSs by decomposing them into logical and physical components, including the interaction between the internal and external units. Then, the authors formulated data flow diagrams (DFDs) for these components. It extends the traditional CIA (Confidentiality, Integrity, and Availability) with Authenticity, Non-repudiation, Safety and Authorisation. Table 1 demonstrates the link between these threat classes and the security requirement.

Table 1
STRIDE threat classes and respective security requirements.

Threat	Security Requirement
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privileges	Authorisation

3.1.2. DREAD

It is developed by Microsoft to support STRIDE with risk assessment. It provides a classification scheme for quantifying risks based on five attributes with the following equation, $risk = (D + R + E + A + D)/5$. They are briefly explained below:

- Damage (D): It is the analysis of the harm caused to the system by a cyber attack.
- Reproducibility (R): It is the analysis of how possible it is to re-produce a cyber attack. For instance, if an attack can be performed repetitively, it is a significant risk for the system.
- Exploitability (E): It is the analysis of the feasibility for executing successful cyber attack.
- Affected users (A): It is the analysis that considers the number of users that could be impacted by the attack.
- Discoverability (D): It is the analysis that considers the ease of discoverability of the attack in the system.

3.2. OCTAVE

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a risk-based method by the CERT-Division of the Software Engineering Institute (Alberts et al., 2003). It has three main variations known as the OCTAVE, OCTAVE-S, and OCTAVE Allegro. It focuses on addressing the organisational risks by performing workshops and discussions among interdisciplinary participants from the organisation, such as senior managers, operational managers, and security specialists. The methodology has three main stages: (i) building asset-based threat profiles for organisational security evaluation, (ii) identifying infrastructure vulnerabilities, and (iii) developing cyber security strategy based on the identified risks against the critical assets.

3.3. PASTA

The PASTA method aims to address the business objectives and security requirements in parallel by identifying the most feasible threats for a system. It provides a structured framework with rich documentation. However, it has been considered an extensive labour inducing process compared to the majority of the other threat modelling methods (UcedaVelez and Morana, 2015). The main steps are:

- Defining the security and business objectives, and impact of security measures on the business

- Defining the technical scope
- Security decomposition of the system
- Creating DFDs
- Analysing threats based on security decomposition and DFDs
- Analysing system's vulnerabilities and weaknesses
- Modelling possible cyber attacks
- Analysing the risks and the impacts on business

3.4. Composite threat modelling

Composite Threat Modelling method is specifically developed by the US Department of Transportation and National Highway Traffic Safety Administration for future vehicles, which is a CPSs (McCarthy et al., 2014). This method has two main steps: (i) identifying critical components and (ii) analysing respective threats on the critical components. This enables security measures to be tailored to the criticality of the affected components.

The methodology requires representing DFDs considering all the physical or networked components, entry/exit points, and data types. Then, the threats can be identified based on analysing the DFDs based on identifying: (i) critical data flows needed for the mission, (ii) direct/indirect data flow that can be used to affect a critical component, (iii) the components changing the data in the network, (iv) the physical/wireless threat entry points, and (v) the security properties of the system.

3.5. Discussion

This section presents four potentially applicable methods for the teleoperated robot use case in the New Space systems. These systems include distributed units with some degree of autonomous functions. However, it is difficult to cover all aspects of such use cases by using a single method Jamil et al. (2021a). Thus, the methods are evaluated for the selection in our study, based on the metrics derived from the work in Shevchenko et al. (2018). These are the following:

- Maturity: Is it well defined and applied in prior studies?
- Adaptability: Is it flexible to be tailored for the specific requirements of the use case?
- Safety and security dependency coverage: Does it cover the impacts on safety?
- Hardware and software threats: Does it cover both hardware and software threats in the analysis?
- Documentation: Does it have rich documentation?

Table 2 summarises our consideration based on defined metrics. Composite Threat Modelling, PASTA, and STRIDE utilise DFDs in their frameworks which helps analyse attack paths and affected components in CPSs. STRIDE and PASTA demonstrate higher adaptability for the new use cases, and both are capable of capturing the threat modelling challenges due to hardware and software interaction. However, PASTA requires extensive organisational consultation. Thus, STRIDE is chosen for the rest of this study.

4. Teleoperation: Use case

This section will discuss the teleoperation use case. Firstly, we examine the teleoperation robot system. Later, we demonstrate the use case on the Reference Architecture for Attack Surface Analysis in Space Systems (RASA). The respective architecture was proposed for performing TMRA for autonomous space debris collection (Bradbury et al., 2020). This work makes use of RASA due to the maturity of the architecture and to investigate the model's limitations. We begin by representing a New Space Ecosystem, which gives a high-level view. We use RASA to decompose the teleoperated robots and planetary surface base/ orbital space vehicles with clustered trust domains. Next, we further demonstrate the hardware and software components of the respective systems. This would aid in the TMRA process to determine the threats and draw further analysis from the process.

4.1. Reference Architecture for Attack Surface Analysis in Space Systems (RASA)

A practical method to analyse the attack surface or trust domains is by basing it on a system's reference architecture (RA) and instantiating it with components applicable for a specific use-case or scenario. In other domains such as the Internet of Things, RAs have been used to analyse system changes. Similarly, we draw inspiration from other CPSs when conducting our analysis of the New Space system. We are interested in exploring the components of the teleoperated robots from a system-centric perspective.

RAs can model the system from different viewpoints, and the particular type is decided based on the use case. Typical viewpoints of RAs include (Weyrich and Ebert, 2016; Lin et al., 2015): (i) Functional (ii) Communication (iii) Implementation (iv) Enterprise (v) Usage (vi) Information (vii) Physical. In our use case, we adopt the functional and communication viewpoints for analysing the system's attack surface as adversaries could communicate and influence the system (Schneier, 2000). This is because, from an attack surface analysis perspective, it is not strictly required to specify the information flow, but it is needed to know which functional components have access to information. Since cyber threats can influence the physical components, it is an essential perspective to be included. However, other perspectives are not considered in this study as it adds further complexity for TMRA (Maple et al., 2019; Sheik and Maple, 2019; Bradbury et al., 2020).

The hybrid functional-communication viewpoint Fig. 1 will describe two main architectures from the New Space high-level view: (i) planetary surface base/ orbiting space vehicle (ii) teleoperation robot. The planetary surface base

Table 2
Evaluation of the threat modelling methods (M: Maturity, Adpt: Adaptability, Sf-S: Safety and security dependency coverage, Hw-Sw: Hardware and software threats, Doc: Documentation).

Method	M	Adpt	Sf-S	Hw-Sw	Doc
Composite Threat Modelling (McCarthy et al., 2014)	✓		✓	✓	✓
OCTAVE (Alberts et al., 2003)	✓				✓
PASTA (UcedaVelez and Morana, 2015)	✓	✓		✓	✓
STRIDE (Shostack, 2008)	✓	✓		✓	✓

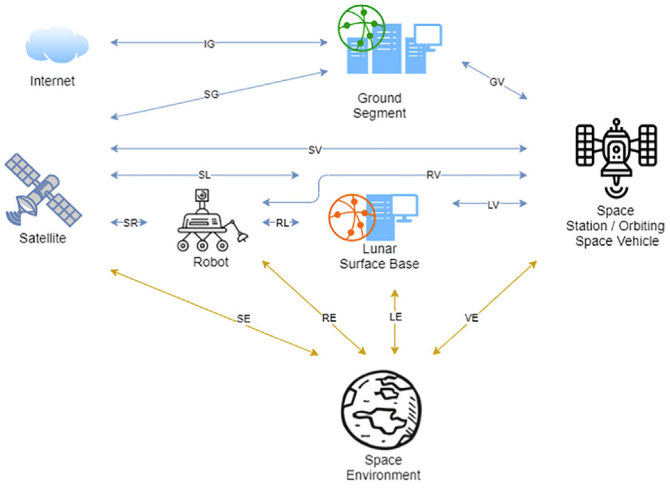

Fig. 1. High-level New Space ecosystem.

would contain the main components such as life support needed for the operator who commands the teleoperated robot remotely. These systems interact with space and the planetary environment whilst communicating with each other. This environment is sometimes unknown, or it could be unexpected conditions. In order to consider different forms of communication and interaction, we have colour-coded the arrows in the diagram. These are: (i) communication, (ii) sensing and (iii) environment interaction. Moreover, each sub-reference architecture is further decomposed into respective hardware and software components that can be further considered for analysis.

The system diagram has been provided by the FAIR-SPACE Hub as a part of an internal project report to explore the trust domains. Using these, we abstracted the components by incorporating them into RASA. As a result, Fig. 2 guided us to formulate Figs. 3 and 5. This would further help understand the use case. The next section will discuss the teleoperation robot and its components.

4.2. Teleoperation robot

The teleoperation robots use case aims to address tasks related to manufacturing and assembly performed in a planetary environment such as the Moon or Mars. The mission scenario is to construct a habitat model on the surface of a planet using blocks. Other applications include:

- Exploration of a planetary surface: In this case, the teleoperated robot would explore an unknown terrain to learn and categorise some predetermined locations. Upon discovery of the location, a specific task could be performed.
- Construction on a planetary surface: In this case, the tasks are controlled and monitored by an operator located in an orbital vehicle. Unlike other use cases, the robot is influenced by a remote human operator who uses haptic devices to receive feedback. These would be used by the operator to direct the robot arm located on the planetary surface. This is further illustrated in Fig. 2, 4, and explained in Table 5.

The system model (Fig. 2) under discussion is one in which a teleoperated robot on the planet's surface communicates with an operator in orbit or on the planet's surface over a secure communication channel that may include relay satellites. However, since relay satellites increase the system's latency, selecting the efficient security mechanism is crucial for system's operation. Twin Panda Franka robotic arms are used to equip the teleoperated robots. The robot receives orders through the network from the operator's haptic device, which is capable of transferring data in real time or in discrete commands. During teleoperation, the human operator may sense the interaction of the force-torque sensors. On the user's hand, the haptic device measures, transmits, and mimics these feelings. The operator's performance is also influenced by the mental load estimator, which analyses and corresponds to the task's demands.

The key challenges highlighted for teleoperated robots are as follows: (1) Space visualisation of operation and state estimation, (2) Autonomous object capture, (3) Transition between autonomous and teleportation modes, (4) Haptic and assembly jobs, and (5) Biomonitoring of Mental Load. To accomplish these demanding goals, the communication channel must remain stable.

4.2.1. Wireless communication

In Fig. 2, 3 and 5, the wireless communication component transmits and receives signal. It can receive signals from various terrestrial sources and relay them to other units in the ecosystem. This module operates over: (i) Microwave frequency band (ii) Ultra high frequency (UHF) (iii) Very high frequency (VHF). Examples include

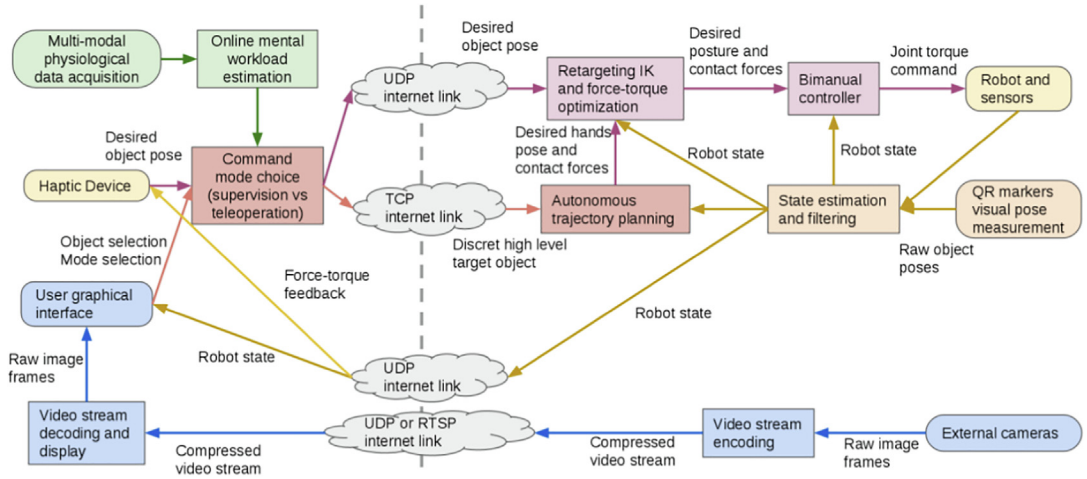

Fig. 2. Teleoperated robot system architecture.

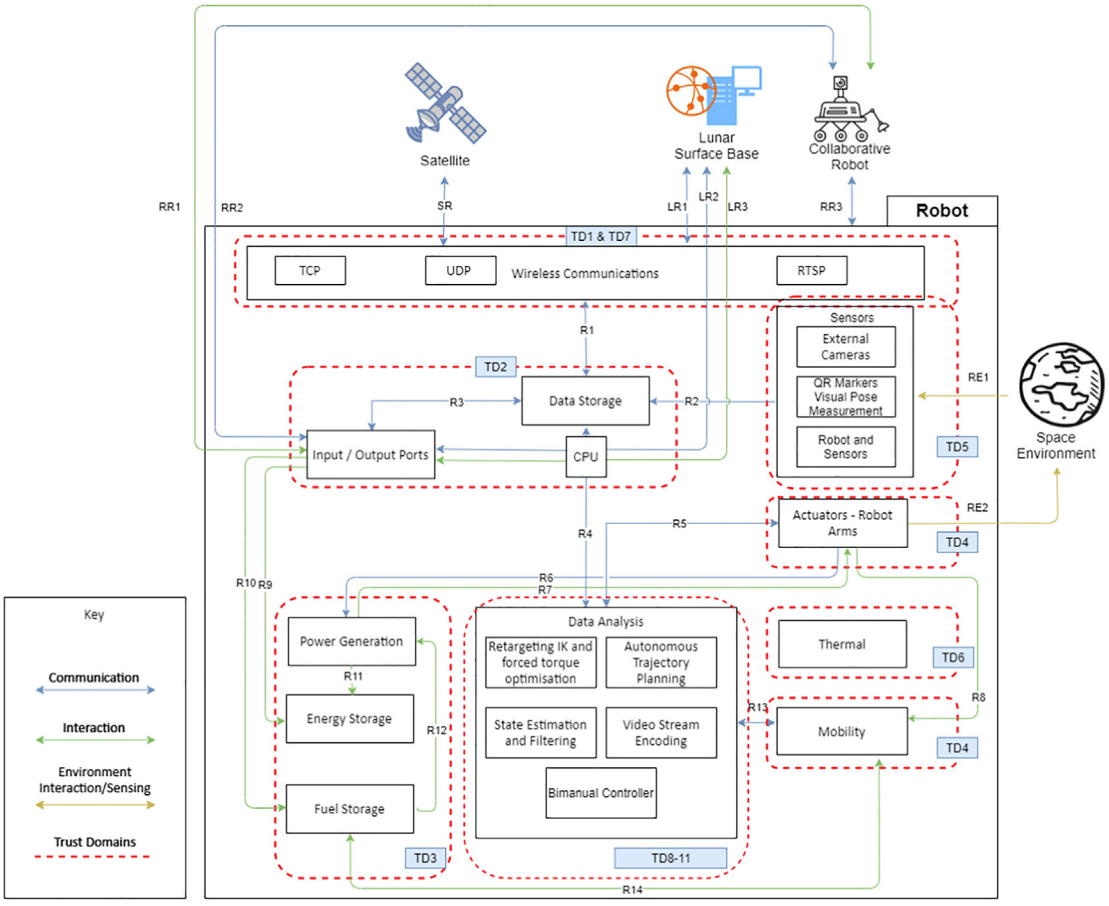

Fig. 3. Robot RASA.

C-band, k-band, Ka-band, Ku-Band, L-band, S-band and X-band. Each teleoperated robot acts as an individual node and regularly communicates with neighbouring nodes and respective orbital vehicles.

4.2.2. Input/output ports

This module enables a system, such as a robot or an orbital vehicle, to connect with other systems physically or digitally.

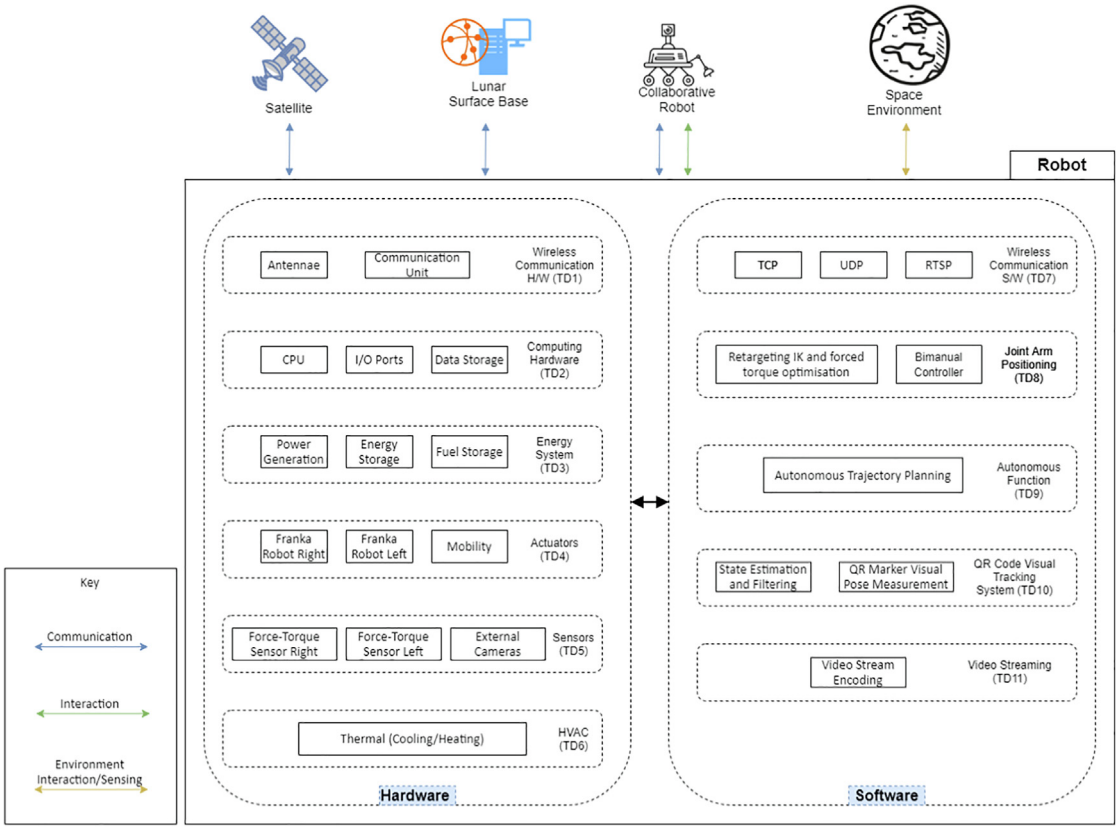

Fig. 4. Robot H/W S/W Interaction.

4.2.3. Sensing

The sensing module in the robot consists of QR visual pose markers, external cameras, robotic sensors. These are the key components to sense the environment for building awareness. They are usually hardwired to the processor and storage units. The planetary (Lunar) surface base operator interacts with haptic device sensors, G.Tech 32Ch EEG cap, Flexible Wearable Sensors, and PupilLabs Wearable Eye Tracker.

4.2.4. Power management, energy storage, fuel storage and thermal

The energy source ensures that the robot and other systems can operate adequately without failures. The energy could be generated either by solar panels or various other technologies and stored in batteries. These technologies differ from traditional systems/vehicles that depend on combustible fuel, which is not producible in space ecosystem. As a result, supporting functions such as propulsion and mobility in robots and orbital vehicles may need careful handling. The energy generated can also help regulate the system's temperature while interacting with the Thermal Module.

4.2.5. Actuators, physical interactions and mobility

The actuator module encompasses any components influencing the physical environment. It would include mobility, and in our use case, it would represent the robot arms and haptic devices. Planetary surface bases and robots are developed to interact with nature in space. This is accomplished by the use of a variety of mechanical components. This would enable the robot to manoeuvre on the planetary surface physically.

4.2.6. Data storage and analysis

Robots and planetary base stations would receive much information in the space environment, including data related to the maps and navigation, collaborative data from neighbouring robots and satellites, maintenance data, firmware and software data. The data would be stored centrally and in different locations, considering the relative latency of wireless communication and secure segregation. Further, with a large amount of data stored, useful *data analysis* would help support and aid the missions. The analysis could include trivial to critical tasks. Examples include toggling an update, time analysis, or even performing complicated machine learning algorithms.

4.2.7. Mobility

The mobility function provides the ability of physical movement on the planet. Thus, the robot can explore a planetary surface or achieve specific objectives such as transporting goods or mining on a planet.

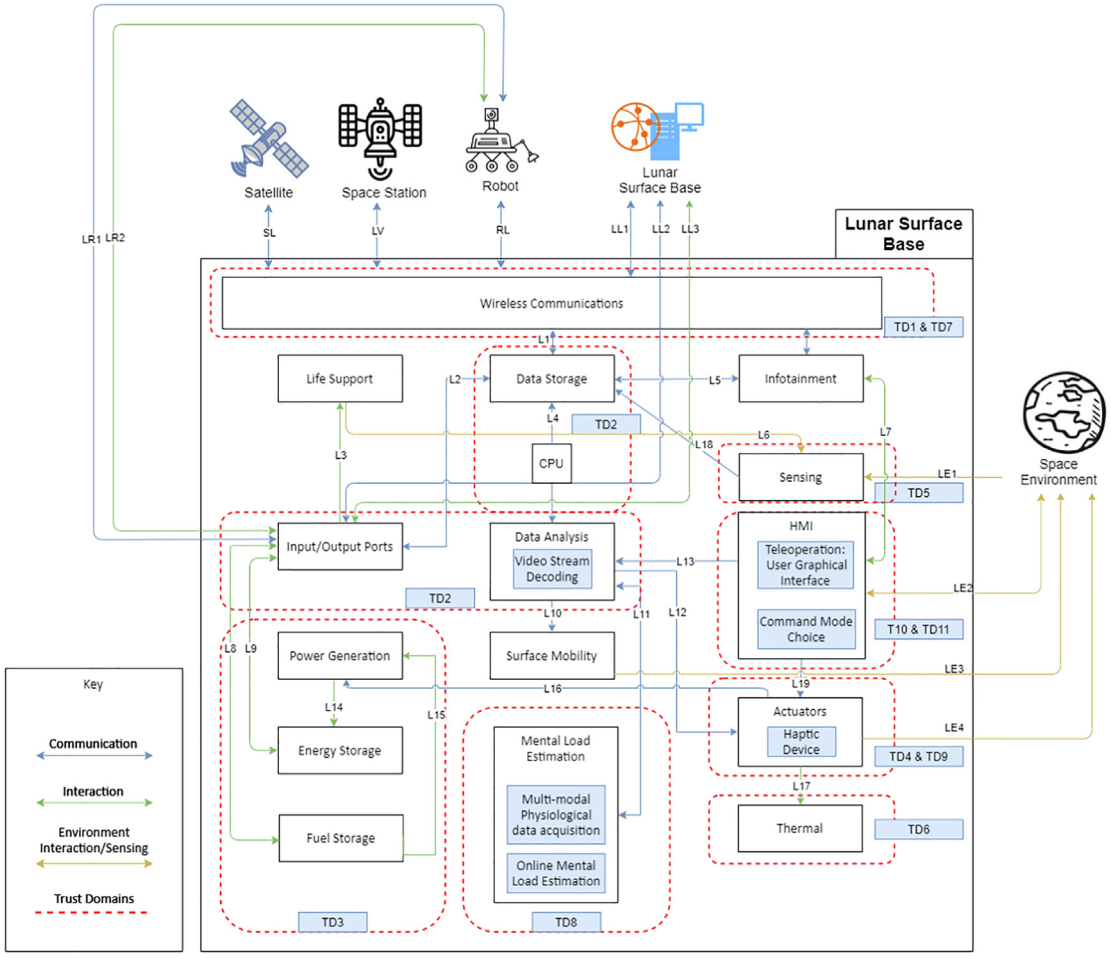

Fig. 5. Planetary (Lunar) Surface Base RASA.

4.3. Planetary (Lunar) surface base

This sub-architecture reuses the following components from the robot sub-architectures: (i) Robot/Data Storage (ii) Robot/Communication (iii) Robot/Power Management (iv) Robot/Fuel Storage (v) Robot/Thermal (vi) Robot/Data Analysis (vii) Robot/I/o Ports. Further information concerning planetary surface area can be referred from Fig. 5, 6, and Table 6.

4.3.1. Human Machine Interface (HMI)

HMI is a user interface or dashboard that connects a person on the planet to a machine, system, or robot. At the same time, the term can technically be applied to any screen that allows a user to interact with a device.

4.3.2. Actuators

This module refers to components in the orbital vehicle that can impact the environment. This may include, a variety of robot arms from the teleoperated system.

5. Teleoperation: Threat modelling

The space systems are evolving, and the substantial changes introduce unknown amendments to the existing threat landscape (Bradbury et al., 2020). Security of these systems requires careful consideration due to their following characteristics (Yang et al., 2010; Hall, 2016):

- Ease-of-access by threat actors: The accessibility to space technologies is becoming easier and cheaper, which also helps threat actors to find it easier to access these systems and identify their vulnerabilities.
- Variety of locations: Space systems can be deployed in a broad distant location in space and collaborate to accomplish missions.
- Link to the Critical National Infrastructure (CNI): Space systems and their associated infrastructure are considered a part of the CNI since they provide services for critical applications.
- Wireless communication: Space systems communicate through various wireless communication protocols.

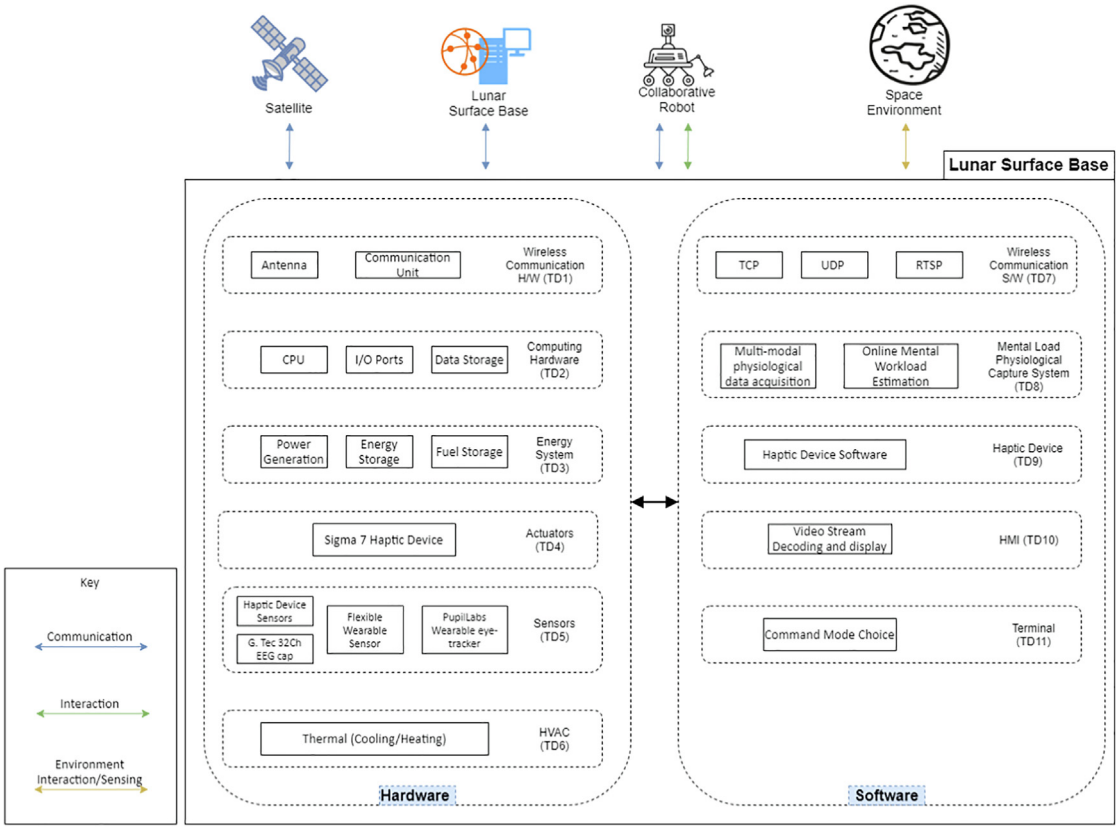

Fig. 6. Planetary (Lunar) Surface Base H/W S/W Interaction.

- Sensory data: Space systems rely on various forms of sensory data for their applications, such as surveillance, environmental monitoring, and planetary exploration. It is expected that robotic space systems will deploy more autonomous functions which require higher dependency on the sensory data.
- Extreme environmental conditions: Space systems are exposed to various environmental challenges that may deteriorate the physical components and obstruct operation. These include vacuum, intense ultraviolet radiation, ionising radiation, electrostatic charge, micrometeoroids, space debris, and extreme thermal cycling.
- Human-in-the-loop: Many space missions include human-in-the-loop for their operations and decision-making process.
- Very low fault tolerance: Space missions usually have very low fault tolerances due to the high cost of operations.
- Long lifespan: Space systems usually have long life spans. Thus, resilience and recoverability need to be considered for developing security mechanisms in the evolving space ecosystem.

5.1. Cyber security requirements

Traditional security requirements for information systems are usually represented with the CIA triad (Confidentiality, Integrity, Availability). However, unlike other CPSs, it does not reflect the security needs of space systems, which encompass both physical and information security. The security requirements are further expanded into the following:

- Confidentiality: It refers to the security property that helps prevent the disclosure of information to an unauthorised actor (Pham et al., 2010). It may be ensured by encrypting the messages during transmission or/and limiting access to the critical components such as databases, log files, backups.
- Integrity: It refers to the security property that ensures the data is not being altered by an unauthorised actor (Madden et al., 2010).
- Availability: It refers to the security property of the system to meet its operational objectives. The system's availability can be jeopardised through various attacks, including jamming the communication links or power outages (Work et al., 2008).

- Authenticity: It refers to the security property that enables the system to use digital signatures to authenticate the data from/to the system and its services (CCSDS, 2019a).
- Safety: It is a crucial property that can be influenced by security properties if compromised in CPSs (Banerjee et al., 2011). Safety is also dependent on other engineering properties, which are out of the scope of this research.

Due to the nature of space systems, a diverse range of threat actors can compromise one or multiple security requirements.

5.2. Threat actors

The term threat actor denotes an individual or a group who can execute a threat. The threat actors can vary from an insider to organised groups or state-sponsored actors. According to Parker (2007), analysing the motivations and characteristics of possible threat actors is vital in understanding the level of risks that may emerge. Do et al. (2019) specified three characteristics of threats actors: (i) assumptions about resources, presence and connectivity, (ii) motivations and the goals, and (iii) capabilities and knowledge. Bradbury et al. (2020) categorised these emerging threat actors against New Space systems. The list of threat actors against the teleoperated robot use case, presented in Table 3, is derived from Bradbury et al. (2020) and Falco et al. (2021) and provides a related example for clarity.

5.3. Trust domains

A system's trust domain comprises the set of interactions between an internal system component and entry points for the external actors. It is usually utilised to analyse potential cyber-attack paths through the entire system via vulnerable entry points and compromised components.

The cyber-attack paths demonstrate the sequence of components that need to be compromised by a threat actor to achieve malicious objectives. Thus, identifying the trust domain is vital for system security designers to decide appropriate countermeasures and where to place them in the system. Table 5 and Table 6 demonstrate trust domains in the robot and planetary (Lunar) surface base/orbiting space vehicle. The tables also provide denoted data flows, the data process that occurs within the trust domain, and threat entry/exit points for each trust domain.

5.4. Threats to teleoperated robot in new space

These systems may encounter threats from a wide range of sources. Space threats can be classified into four categories kinetic physical, non-kinetic physical, electronic, and cyber threats (Harrison et al., 2020; Falco and Boschetti, 2021). Kinetic physical threats refer to the weapons which can directly strike or detonate a space system, including ballistic and nuclear missiles. Non-kinetic physical threats contain direct-energy weapons which can physically damage or prevent the operation without physical contacts. These could be lasers, high-powered microwave weapons, and electromagnetic pulse weapons, which can have physical effects on satellites and ground stations (Suloway et al., 2020; Falco and Boschetti, 2021).

This work analyses threats from the cyber security perspective. Thus, we will classify kinetic and non-kinetic threats as physical threats and include them in the definition of DoS attacks. Electronic threats cover jamming and spoofing. First, jamming aims to jeopardise wireless communication by propagating noise signals in the same frequency band of the target antenna, which is counted in DoS threats. Second, spoofing aims to falsify the target system by fraudulent signals (Harrison et al., 2020).

Tables 5 and 6 demonstrate the possible threat entry points for cyber threats, and DFDs are used to track the cyber attack paths (see Fig. 3 and 5). Harrison et al. (2020) classified the existing cyber attacks in three broad categories: (i) data intercept or monitoring, (ii) data corruption, and (iii) seizure of control. However, evolving space systems can encounter more cyber threats due to the lowered entry barriers to space and increased variety of applications (Manulis et al., 2021). Thus, our consideration contains common modern-day cyber threats, see Table 7 for details.

6. Results and analysis

This section will discuss the results and explore the limitations of STRIDE/DREAD in capturing the threats due to hardware-software interaction. The section concludes with the recommended countermeasures.

Through the systematic TMRA process, we modelled the threats by analysing the interactions of hardware and software components in the systems. We identified 97 different threats resulting from eleven Trust Domains among 3 systems (Robot, Planetary Surface Base, and Space Station/Orbiting Vehicle). Then, respective risks have been assessed, quantified, and discussed to determine the identified threat's likelihood. Finally, countermeasures have been suggested to overcome future cyber threats. Due to the limitations, this paper has considered the critical risks. Further information on the complete TMRA process can be accessed in the following hyperlink (https://bit.ly/3DMyZXZ).

After analysing cyber security requirements, threats and adversaries, TMRA is performed to identify vulnerabilities and impacts to understand the system's security controls. STRIDE/DREAD is used in this work, see Section 3.1 for details of the method. Identified threats are represented with the initials (e.g., S, T, R, I, D, and E), and the associated risk is calculated as an average of *Damage*, *Reproducibility*, *Exploitability*, *Affected Users*, and *Discoverability*. Each parameter is normalised between 1–

Table 3
Threat actors for the teleoperated robot use case, derived from Bradbury et al. (2020) and Falco et al. (2021).

	Threat Actor	Example	Goals & Motivations	Capabilities	Environment	Resources
Individual	Outsider	Hacktivist	Personal satisfaction; Passion; Ideology. Doesn't believe in extra terrestrial habitat fabrication, alter functioning of robot/ lunar orbital vehicle	Limited	Remote access	Minimal
	Trusted Insider	Contractor/Astronaut	Financial gain; Discontent	Moderate	Internal access with some permissions	Internal knowledge
	Privileged Insider	Operator/Astronaut	Financial gain; Discontent	High	Internal access with higher permissions	Internal knowledge
Group	Ad hoc	A group coming together over a time-critical event	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 4
DREAD Risk Analysis Table (R = Robot, V = Orbiting Vehicle, S = Spoofing, T = Tampering, D = Denial of Service, I = Information Disclosure, E = Elevation of Privilege).

Trust Domains	Low	Medium	High	Critical	Total
TD1 & TD7	0	2	2 (T, I)	2 (D, S)	6
TD2	2	6	4 (S,T, I, E)	1 (D)	13
TD3	0	0	1 (D)	4 (D)	5
TD4	4	0	0	1 (D)	5
TD4 & TD9	7	4	0	0	11
R- TD5	4	0	0	1 (D)	5
V- TD5	4	0	0	1 (D)	5
TD6	4	0	0	1 (D)	5
R-TD8	3	4	0	0	7
V-TD8	3	4	0	0	7
TD9	3	4	0	0	7
TD10	3	4	0	0	7
V-TD10 &11	3	4	0	0	7
V-TD11	3	4	0	0	7

5, where 1 is the lowest and 5 is the highest impact. The risks are quantified into 4 categories: Low, Medium, High, and Critical. They are indicated with the colour codes Blue, Green, Yellow, and Red. Table 7 presents the clustered threats with 'Critical' and 'High' risks to articulate the system's vulnerabilities better. Among these, 11 are *critical* threats, 10 of which are related to DoS, and 1 is Spoofing. In addition to these, the system is *highly* vulnerable to tampering, information disclosure, DoS, and elevation of privilege attacks. The total counts of the threats are summarised in Table 4. The DoS attack is observed to be the critical threat to which the system may be vulnerable. While various jammer detection techniques are being developed, it is still a significant research problem because they are not advanced enough to accurately classify the type of jamming attack. This classification is vital for building appropriate countermeasures.

From this, we observed that similar types of analysis could be carried out for other New Space applications that may need to communicate and interact in the space environment. While different applications evolve, novel techniques such as adaptive risk and threat analysis may need to be developed. However, the overall approach is still applicable, and it is at the early stages of research (Grover et al., 2014).

The limitation of these methods is that they lack a precise representation of adversarial behaviours, especially in targeted or multi-stage cyber attacks that use physical components as the attack agents. Traditional approaches such as STRIDE and DREAD are being used; however, their efficacy is being questioned. Irrespective of the advancement in threat modelling approaches, a gap still exists for automated and systematic security analysis of a CPS. Additionally, questions are being raised on current approaches concerning the analyses of systems in isolation rather than a group of interactive hardware and software components. This challenges the security researchers to characterise a system accurately for its conformance to developed security requirements. Moreover, security requirements is another challenge as it is difficult to establish the system's performance with many assumptions. Such challenges have often led to developing defectively set security requirements. However, it is imperative to protect the system despite the limitations against the identified threats. The following sub-section will explain the recommended countermeasures.

6.1. Recommended countermeasures

While the cyber security risks cannot be entirely eliminated, it is advantageous to understand the likelihoods and potential impacts of identified risks. TMRA aims to provide further clarity in this direction for the system security designers. The key is to focus the countermeasures on the most critical assets, which will minimise the impacts on the system. They should, however, be designed in such a way that they can function together by protecting space mission systems (Tsamis et al., 2021).

Emerging technologies for space operations, such as cube satellites, commercial ground segments, and launches, have drastically lowered the entrance barrier into space exploration (Bailey, 2020). As a result, the security concerns of space systems are intensifying. The report on Threats to the United States Space Capabilities emphasised the importance of reliable threat analysis, mobile ground control stations, increased autonomous capabilities, and onboard redundancy (Wilson, 2001). Jamming the wireless communication module is observed to have the highest risks as a result of TMRA. Jamming instruments tend to be more accessible and affordable. Likewise, the growing jamming risk is noted in a report on global navigation systems by The Royal Academy of Engineering in 2011 (Thomas et al., 2011). The report recommended (i) to raise awareness and analyse impacts, (ii) develop policy as a response to commercial availability of jamming equipment, and (iii) increase system's resilience (Thomas et al., 2011). The works in Grover et al. (2014) and Elghamrawy et al. (2020) presented techniques to increase the system's resilience against jamming, including adaptive time-domain filtering, time–frequency domain processing, subspace processing, and adaptive antennas. These can be deployed to secure the teleoperated robots in space systems.

DoS attacks can be achieved by targeting onboard computing hardware, energy system, actuators, and sensors by conducting electronic warfare or physical attack such as a directed energy weapon, see Table 7. Deploying Space Surveillance System is recommended against cyber weapons in space (Pavur and Martinovic, 2019). Falco et al. (2022) proposed a system which can employ security mechanisms to safeguard the communication channel and maintain space mission resilience against radio frequency threats. Moreover, spoofing satellite communication is another critical risk. Researchers experimentally conducted GNSS spoofing for the proof-of-concept. A yacht is misdirected by spoofing the GNSS receiver by commercially available inexpensive equipment (Humphreys, 2013;

Psiaki and Humphreys, 2016). Similar attacks can have higher feasibility for teleoperated robots in the evolving space. Research has suggested anti-spoofing methods to provide signal-level or data-level protection against spoofing attacks. However, it is still an open research area (Wu et al., 2020). Finally, it is also predicted that modern-day threats against software systems will be more applicable. Evolving space systems should include methods to encrypt communication data optimally utilising AES and IDEA algorithms to meet the requirements of data critical teleoperated applications, while considering the authenticity of the data using suitable hash algorithms (Saha et al., 2019). In addition, updated communication protocols and data packet structures are necessary to meet the security requirements for novel applications (Saha et al., 2019). Moreover, such complex characteristics must be supplemented by redundant systems to provide resilience in the event of a component failure (Saha et al., 2019). Other measures include data sanitisation, data segmentation, adaptive authentication and access controls (Maple et al., 2022).

7. Conclusion

This paper presents a detailed study using TMRA on the teleoperated robot. We show how cyber security threat analysis techniques can be used to analyse the robot's security properties, particularly as they may impact its safety. To do so, we follow the STRIDE/DREAD methodology. By abstracting the hardware and software components for the Planetary Surface Base/Orbital Space Vehicle and Teleoperated Robots, we investigate the security properties related to the STRIDE. In particular, it helps examine the high-level and low-level properties of the New Space systems. On the other hand, the use of STRIDE also highlights various limitations of the TMRA. Our risk analysis allows us to examine various properties of the communication protocol and interaction at different levels of abstraction. Future research will likely provide a better understanding of which STRIDE properties should be verified against the system's assets.

An important aspect here is that the component analyses do not necessarily highlight the combined threats that need to be mitigated at the system level, although they could be helpful. The deployed methods develop TMRA for a specific teleoperated scenario, quantified by the expected risk within a range of 1–5, where one indicates low risk and five indicates high risk. However, an interesting avenue of future work might involve proving that different threat modelling techniques do not, in fact, capture all the threats in the same system. We could also apply TMRA techniques such as simulation-based methods to mitigate certain threats and further explore the teleoperated robot's vulnerabilities in relation to safety and reliability for a collaborative manufacturing task.

This work is the first step towards analysing how TMRA has limitations on capturing and quantifying all the threats in the interactions among the hardware and software components in teleoperated systems. Our future work aims to develop a tailored TMRA methodology for capturing emerging threats in New Space systems considering hardware-software components from the observations of this study. Although our deployment of STRIDE/DREAD has been motivated by our analysis and experience with these tools, it is undoubtedly the case that other methods may have been a better choice for our study. We intend to investigate this further in future work.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

The work presented has been funded by Grant EP/R026092/1 (FAIR-SPACE Hub) through UK Research and Innovation (UKRI) under the Industry Strategic Challenge Fund (ISCF) for Robotics and AI Hubs in Extreme and Hazardous Environments.

Appendix A. Trust domains and TMRA tables

See Tables 5–7.

Table 5
Data flow and data process for the respective threat entries in Robot.

Trust Domain	DF ID	Data Process	DF Description	Threat Entry/Exit
TD1 (H/W) & TD7 (S/W): Wireless Communication	SR, LR1, LR3, RR3	Data Transmission	The robot is in continuous communication with the Lunar Surface Base or Space Station/ Orbiting Vehicle, depending on where the operator is located. TCP, UDP and RTSP protocols are used for command mode choice and video streaming in the demonstration, respectively.	Communication Unit (wireless modules), Antenna
	LR1, RR3	Application Framework Access	The robots communicate with neighboring robots and lunar surface base regularly. This communication occurs through a secure and trusted application framework.	Database (eg. SQL), I/O Ports
TD2: Computing Hardware (Data Storage, I/O ports and CPU	R1, R2, R3, R4	Database Access	The internal components (wireless communication module, sensors, I/O ports and CPU analysis) can access data stored in the Database in robots through respective application frameworks	Database (eg. SQL)
	RR1, R9, R10	Physical Interaction	The on-board hardware in robot physically interacting with the space environment and depending on the on-board energy system.	Space Env. (eg. Radiation, Magnetic waves, Thermal, Lunar elements)
	RR2, LR2	Data Transmission and Database Access	The external (collaborative robots, operators located in lunar surface base and satellite station) can access data stored in the Database in robots through respective application frameworks	Communication module
	R7, R9, R10, R11, R12	Physical Interaction	The on-board energy system may be vulnerable to space environmental challenges.	Space Env. (eg. Radiation, Magnetic waves, Thermal, Lunar elements)
	R6	Data Processing	The on-board energy system provides required energy for the operations in robot.	Data Analysis (TD8-11)
TD4: Actuators	R5, R13	Data Processing	Actuators in continuous communication with the internal computation units.	Data Analysis (TD8-11)
	R7, R8, RE2	Physical Interaction	The robot arms receiver their power from the the energy unit to interact with the environment	Space Env ((eg. Radiation, Magnetic waves, Thermal, Lunar elements)
TD5: Sensors	R2	Data Processing	The on-board sensors are communicating with the internal computation unit and the operator though the internal computation and communication units.	Data Analysis (T8-11)
	RE1	Physical Interaction	The on-board sensors may be open to space environment specific threats	External Cameras, Force-Torque Sensor (Right/Left), Space Env. (eg. Radiation, Magnetic waves, Thermal, Lunar elements)
TD6: HVAC	R8	Physical Interaction	HVAC aims to keep on-board units in the range of appropriate temperature	Cooling/Heating System, Space Env. (eg. Radiation, Magnetic waves, Thermal, Lunar elements)
TD8: Joint Arm Positioning	R4, R5, R13	Data Processing	The robot arms is in continuous communication with the bimanual controller software	Bimanual Controller
TD9: Autonomous Functions			The autonomous functions are in continuous communication with the sensors and actuators for control and optimisation during the operation.	Sensors, Actuators
TD10: QR Code Visual Tracking System			The implementation relies on visual recognition of QR code markers with on-board cameras to determine the pose of the objects.	Camera, QR Pose Visual Measurement Application
TD11: Video Streaming			The operator receives video stream from the cameras on the robots. The video stream needs to be encoded with the required protocol.	Video Encoding Application, Camera

Table 6
Data flow and data process for the respective threat entries in Planetary Surface Base/ Orbiting Space Vehicle.

Trust Domain	DF ID	Data Process	DF Description	Threat Entry/Exit
TD1 (H/W) & TD7 (S/W): Wireless Communication	SV, LV	Data Transmission	The space station/orbiting vehicle and lunar surfce base is in continuous communication with the teleoperation robots. TCP, UDP and RTSP protocols are used for Command Mode Choice and video streaming in the demonstration, respectively.	Communication Unit (wireless modules), Antenna
	RV	Application Framework Access	The space station/orbiting vehicle and lunar surface base is in continuous communication with robots. This communication occurs through a secure and trusted application framework.	Database (eg. SQL), I/O Ports
TD2: Computing Hardware (Data Storage, I/O ports and CPU	V2, V7, V3	Database Access	The internal components (wireless communication module, sensors, I/O ports and CPU analysis) can access data stored in the Database in Space Station/Orbiting Space Vehicle and Lunar Surface Base through respective application frameworks	Database (eg. SQL)
	V1	Data Transmission and Database Access	The external (collaborative robots, operators located in lunar surface base and satellite station) can access data stored in the Database in Space Station/Orbiting Vehicle and Lunar Surface Base through respective application frameworks	Communication module
	V8, V9, V10, V13, V14, V15, V16,	Data Processing	The external (robots, operators located in lunar surface base and space station/ orbiting vehicle) can support for data analysis such as for video stream decoding through respective application frameworks	Communication module
	V4, V5, V6	Physical Interaction	The on-board hardware in Space Station/ Orbiting Vehicle and Lunar Surface Base physically interact with the space environment whilst depending on the on-board energy system such as solar power and fuel.	Space Env. (eg. Radiation, Magnetic waves, Thermal, Lunar elements)
	V4, V5, V11, V12, V19, V20, V21, V22	Physical Interaction	The on-board energy system may be vulnerable to space environmental challenges.	Space Env. (eg. Radiation, Magnetic waves, Thermal, Lunar elements)
	V10	Data Processing	The on-board energy system provides required energy for the operations in Space Station/Orbiting Vehicle and Lunar Surface Base.	Data Analysis (TD8-11)
TD4(H/W) and TD9 (S/W): Actuators	V9, V17	Data Processing	Actuators are in continuous communication with the internal computation units	Data Analysis
	V18	Physical Interaction	Actuators receive their power from the energy unit to interact with the environment	Space Env ((eg. Radiation, Magnetic waves, Thermal, Lunar elements)
TD5: Sensors	V3	Data Processing	The on-board sensors are communicating with the internal computation unit and the operator through the internal computation and communication units.	Data Analysis (T8-11)
	V23, V24	Physical Interaction	The on-board sensors may be open to space environment threats	External Cameras, Force-Torque Sensor (Right/Left), Space Env. (eg. Radiation, Magnetic waves, Thermal, Lunar elements)
TD6: HVAC	V18	Physical Interaction	HVAC aims to keep on-board units in the range of appropriate temperature	Cooling/Heating System, Space Env. (eg. Radiation, Magnetic waves, Thermal, Lunar elements)
TD8: Mental load psycological capture system	V15	Data Processing	This module helps to experiment with human mental workload recognition, which is analysed and correlated to the operators performance on teleoperation docking tasks. The real time feedbacks on mental workload, attention, and stress levels for astronauts are supported by real-time data analysis.	Bimanual Controller
TD10: HMI and TD11: Command Mode Choice	V9, V17	Data Processing	The Human Machine Interface(HMI) gives the operator the ability to visualise the task. The module requires regular data analysis and feedbacks from sensors.	Camera, QR Pose Visual Measurement Application
	V18	Physical Interaction	The on-board sensors may be open to space environment specific threats	External Cameras, Force-Torque Sensor (Right/Left), Space Env. (eg. Radiation, Magnetic waves, Thermal, Lunar elements)

Table 7
Threats with Critical or High Risks (Red: Critical Risk, Yellow: High Risk).

Trust Domain	DF ID	Data Process	DF Description	Threat Entry/Exit
TD1 (H/W) & TD7 (S/W): Wireless Communication	SV, LV	Data Transmission	The space station/orbiting vehicle and lunar surfce base is in continuous communication with the teleoperation robots. TCP, UDP and RTSP protocols are used for Command Mode Choice and video streaming in the demonstration, respectively.	Communication Unit (wireless modules), Antenna
	RV	Application Framework Access	The space station/orbiting vehicle and lunar surface base is in continuous communication with robots. This communication occurs through a secure and trusted application framework.	Database (eg. SQL), I/O Ports
TD2: Computing Hardware (Data Storage, I/O ports and CPU	V2, V7, V3	Database Access	The internal components (wireless communication module, sensors, I/O ports and CPU analysis) can access data stored in the Database in Space Station/Orbiting Space Vehicle and Lunar Surface Base through respective application frameworks	Database (eg. SQL)
	V1	Data Transmission and Database Access	The external (collaborative robots, operators located in lunar surface base and satellite station) can access data stored in the Database in Space Station/Orbiting Vehicle and Lunar Surface Base through respective application frameworks	Communication module
	V8, V9, V10, V13, V14, V15, V16,	Data Processing	The external (robots, operators located in lunar surface base and space station/orbiting vehicle) can support for data analysis such as for video stream decoding through respective application frameworks	Communication module
	V4, V5, V6	Physical Interaction	The on-board hardware in Space Station/ Orbiting Vehicle and Lunar Surface Base physically interact with the space environment whilst depending on the on-board energy system such as solar power and fuel.	Space Env. (eg. Radiation, Magnetic waves, Thermal, Lunar elements)
TD3: Energy System	V4, V5, V11, V12, V19, V20, V21, V22	Physical Interaction	The on-board energy system may be vulnerable to space environmental challenges.	Space Env. (eg. Radiation, Magnetic waves, Thermal, Lunar elements)
	V10	Data Processing	The on-board energy system provides required energy for the operations in Space Station/Orbiting Vehicle and Lunar Surface Base.	Data Analysis (TD8-11)
TD4(H/W) and TD9(S/W): Actuators	V9, V17	Data Processing	Actuators are in continuous communication with the internal computation units	Data Analysis
	V18	Physical Interaction	Actuators receive their power from the energy unit to interact with the environment	Space Env ((eg. Radiation, Magnetic waves, Thermal, Lunar elements)
TD5: Sensors	V3	Data Processing	The on-board sensors are communicating with the internal computation unit and the operator through the internal computation and communication units.	Data Analysis (T8-11)
	V23, V24	Physical Interaction	The on-board sensors may be open to space environment threats	External Cameras, Force-Torque Sensor (Right/Left), Space Env. (eg. Radiation, Magnetic waves, Thermal, Lunar elements)
TD6: HVAC	V18	Physical Interaction	HVAC aims to keep on-board units in the range of appropriate temperature	Cooling/Heating System, Space Env. (eg. Radiation, Magnetic waves, Thermal, Lunar elements)
TD8: Mental load psycological capture system	V15	Data Processing	This module helps to experiment with human mental workload recognition, which is analysed and correlated to the operators performance on teleoperation docking tasks. The real time feedbacks on mental workload, attention, and stress levels for astronauts are supported by real-time data analysis.	Bimanual Controller
TD10: HMI and TD11: Command Mode Choice	V9, V17	Data Processing	The Human Machine Interface(HMI) gives the operator the ability to visualise the task. The module requires regular data analysis and feedbacks from sensors .	Camera, QR Pose Visual Measurement Application
	V18	Physical Interaction	The on-board sensors may be open to space environment specific threats	External Cameras, Force-Torque Sensor (Right/Left), Space Env. (eg. Radiation, Magnetic waves, Thermal, Lunar elements)

References

Abraham, S., Nair, S., 2014. Cyber security analytics: a stochastic model for security quantification using absorbing markov chains. J. Commun. 9 (12), 899–907.

Alberts, C., Dorofee, A., Stevens, J., Woody, C., 2003. Introduction to the OCTAVE Approach. Technical Report Carnegie Mellon University Software Engineering Institute.

Amin, S., Cárdenas, A.A., Sastry, S.S., 2009. Safe and secure networked control systems under denial-of-service attacks. In: International Workshop on Hybrid Systems: Computation and Control. Springer, pp. 31–45.

Bailey, B., 2020. Establishing space cybersecurity policy, standards, and risk management practices. Aerospace Corporation.

Banerjee, A., Venkatasubramanian, K.K., Mukherjee, T., Gupta, S.K.S., 2011. Ensuring safety, security, and sustainability of mission-critical cyber–physical systems. Proc. IEEE 100 (1), 283–299.

Bolovinou, A., Atmaca, U.-I., Ur-Rehman, O., Wallraf, G., Amditis, A., et al., 2019. Tara+: Controllability-aware threat analysis and risk assessment for l3 automated driving systems. In: 2019 IEEE Intelligent Vehicles Symposium (IV). IEEE, pp. 8–13.

Bonaci, T., Herron, J., Yusuf, T., Yan, J., Kohno, T., Chizeck, H.J., 2015. To make a robot secure: An experimental analysis of cyber security threats against teleoperated surgical robots. arXiv preprint arXiv:1504.04339.

Bradbury, M., Maple, C., Yuan, H., Atmaca, U.I., Cannizzaro, S., 2020. Identifying attack surfaces in the evolving space industry using reference architectures. In: 2020 IEEE Aerospace Conference. IEEE, pp. 1–20.

C. Yang, J., de Groh, K., 2010. Materials issues in the space environment. MRS Bull., 35, 12–19.

Cárdenas, A.A., Amin, S., Sastry, S., 2008. Research challenges for the security of control systems. HotSec 5, 15.

CCSDS, 2015. Security Threats against Space Missions. Informational Report The Consultative Committee for Space Data Systems (CCSDS). URL: https://public.ccsds.org/Pubs/350x1g2.pdf CCSDS 350.0-G-3.

CCSDS, 2019a. CCSDS Guide for Secure System Interconnection. Informational Report The Consultative Committee for Space Data Systems (CCSDS). URL: https://public.ccsds.org/Pubs/350x4g2.pdf CCSDS 350.4-G-2.

CCSDS, 2019b. Security Guide for Mission Planners. Informational Report The Consultative Committee for Space Data Systems (CCSDS). URL: https://public.ccsds.org/Pubs/350x7g2.pdf CCSDS 350.7-G-2.

CCSDS, 2019c. The Application of Security to CCSDS Protocols. Informational Report The Consultative Committee for Space Data Systems (CCSDS). URL: https://public.ccsds.org/Pubs/350x0g3.pdf CCSDS 350.0-G-3.

Coble, K., Wang, W., Chu, B., Li, Z., 2010. Secure software attestation for military telesurgical robot systems. In: IEEE Military Communications Conference (MILCOM). IEEE, pp. 965–970.

Cornell, A., 2011. Five key turning points in the american space industry in the past 20 years: Structure, innovation, and globalisation shifts in the space sector. Acta Astronaut. 69 (11–12), 1123–1131.

Do, Q., Martini, B., Choo, K.-K.R., 2019. The role of the adversary model in applied security research. Comput. Security 81, 156–181.

Elghamrawy, H., Karaim, M., Tamazin, M., Noureldin, A., 2020. Experimental evaluation of the impact of different types of jamming signals on commercial gnss receivers. Appl. Sci. 10 (12), 4240.

Falco, G., 2018. Job One for Space Force: Space Asset Cybersecurity. Technical Report Belfer Center, Harvard Kennedy School.

Falco, G., 2019. Cybersecurity principles for space systems. J. Aerospace Informat. Syst. 16 (2), 61–70.

Falco, G., 2020. When satellites attack: Satellite-to-satellite cyber attack, defense and resilience. In: ASCEND 2020, p. 4014.

Falco, G., Boschetti, N., 2021. A security risk taxonomy for commercial space missions. In: ASCEND 2021, p. 4241.

Falco, G., Gordon, N., Byerly, A., Grotto, A., Siegel, J., Zanlongo, S., 2022. The space digital dome: Autonomous defense of space vehicles from radio frequency interference. In: 2022 IEEE Aerospace Conference. IEEE.

Falco, G., Viswanathan, A., Santangelo, A., 2021. Cubesat security attack tree analysis. In: 8th IEEE International Conference On Space Mission Challenges for Information Technology.

Grover, K., Lim, A., Yang, Q., 2014. Jamming and anti–jamming techniques in wireless networks: a survey. Int. J. Ad Hoc Ubiquitous Comput. 17 (4), 197–215.

Hall, L., 2016. Human-in-the-loop decision support. URL: https://www.nasa.gov/directorates/spacetech/esi/esi2016/Human-in-the-loop_Decision_Support/.

Harnett, B.M., Doarn, C.R., Rosen, J., Hannaford, B., Broderick, T.J., 2008. Evaluation of unmanned airborne vehicles and mobile robotic telesurgery in an extreme environment. Telemedicine and e-Health 14 (6), 539–544.

Harrison, T., Johnson, K., Moye, J., Young, M., 2020. Space threat assessment 2020. Center for Strategic and International Studies (CSIS).

Harrison, T., Johnson, K., Roberts, T.G., Bergethon, M., Coultrup, A., 2019. Space Threat Assessment 2019. In: techreport Center for Strategic & International Studies, URL: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190404_SpaceThreatAssessment_interior.pdf.

Humphreys, T., 2013. Ut austin researchers spoof superyacht at sea. URL: https://cockrell.utexas.edu/news/archive/7649-superyacht-gps-spoofing.

Jamil, A.-M., Khan, S., Lee, J.K., Othmane, L.B., 2021a. Towards automated threat modeling of cyber-physical systems. In: 2021 International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM). IEEE, pp. 614–619.

Jamil, A.-M., ben Othmane, L., Valani, A., 2021b. Threat modeling of cyber-physical systems in practice. arXiv e-prints, (pp. arXiv–2103).

Khan, R., McLaughlin, K., Laverty, D., Sezer, S., 2017. Stride-based threat modeling for cyber-physical systems. In: 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe). IEEE, pp. 1–6.

Klesh, A.T., Cutler, J.W., Atkins, E.M., 2012. Cyber-physical challenges for space systems. In: 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems. IEEE, pp. 45–52.

Kurzrok, A., Ramos, M.D., Mechentel, F., 2018. 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, SSC18-XI-05..

Lee, C.C., Tan, T.G., Sharma, V., Zhou, J., 2021. Quantum computing threat modelling on a generic cps setup. In: International Conference on Applied Cryptography and Network Security. Springer, pp. 171–190.

Lee, G.S., Thuraisingham, B., 2012. Cyberphysical systems security applied to telesurgical robotics. Comput. Stand. Interfaces 34 (1), 225–229.

Lin, S.-W., Miller, B., Durand, J., Joshi, R., Didier, P., Chigani, A., Torenbeek, R., Duggal, D., Martin, R., Bleakley, G. et al., 2015. Industrial internet reference architecture. Industrial Internet Consortium (IIC), Tech. Rep,.

Lum, M., Friedman, D., King, H., Broderick, T., Sinanan, M., Rosen, J., Hannaford, B., 2007. Field operation of a surgical robot via airborne wireless radio link. In: IEEE Int. Conf. on Field and Service Robotics. Citeseer.

Luo, F., Jiang, Y., Zhang, Z., Ren, Y., Hou, S., 2021. Threat analysis and risk assessment for connected vehicles: A survey. Security Commun. Networks, 2021.

Mackenzie, C., 2019. France plans to boost its self-defense posture in space. Defense News, URL: https://www.defensenews.com/global/europe/2019/07/26/france-plans-to-boost-its-self-defense-posture-in-space/. Accessed: 2019-08-08.

Madden, J., McMillin, B., Sinha, A., 2010. Environmental obfuscation of a cyber physical system-vehicle example. In: 2010 IEEE 34th Annual Computer Software and Applications Conference Workshops. IEEE, pp. 176–181.

Malik, W.J., 2019. Attack vectors in orbit: The need for iot and satellite security. In: RSA Conference, pp. 4–8.

Manulis, M., Bridges, C.P., Harrison, R., Sekar, V., Davis, A., 2021. Cyber security in new space. Int. J. Inf. Secur. 20 (3), 287–311.

Maple, C., Bradbury, M., Le, A.T., Ghirardello, K., 2019. A connected and autonomous vehicle reference architecture for attack surface analysis. Appl. Sci. 9 (23), 5101.

Maple, C., Bradbury, M., Yuan, H., Farrell, M., Dixon, C., Fisher, M., Atmaca, U.I., 2020. Security-minded verification of space systems. In: 2020 IEEE Aerospace Conference. IEEE, pp. 1–13.

Maple, C., Ilker Atmaca, U., Epiphaneou, G., Sheik, A.T., Hathal, W., Cruickshank, H., Falco, G., 2022. The impact of message encryption on teleoperation for space applications. In: 2022 IEEE Aerospace Conference. IEEE.

Martin, G., 2015. Newspace: The emerging commercial space industry.

McCarthy, C., Harnett, K., Carter, A. et al., 2014. Characterization of potential security threats in modern automobiles: A composite modeling approach. Technical Report United States. National Highway Traffic Safety Administration.

Ministére des Armées, 2019. Space Defence Strategy. URL: https://www.defense.gouv.fr/english/layout/set/print/content/download/574375/9839912/version/5/file/Space+Defence+Strategy+2019_France.pdf.

Mo, Y., Sinopoli, B., 2009. Secure control against replay attacks. In: 2009 47th annual Allerton conference on communication, control, and computing (Allerton). IEEE, pp. 911–918.

Parker, D.B., 2007. Risks of risk-based security. Commun. ACM 50 (3), 120.

Pavur, J., Martinovic, I., 2019. The cyber-asat: On the impact of cyber weapons in outer space. In: 2019 11th International Conference on Cyber Conflict (CyCon), pp. 1–18, IEEE volume 900.

Pham, N., Abdelzaher, T., Nath, S., 2010. On bounding data stream privacy in distributed cyber-physical systems. In: 2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing. IEEE, pp. 221–228.

Psiaki, M.L., Humphreys, T.E., 2016. Gnss spoofing and detection. Proc. IEEE 104 (6), 1258–1270.

Saha, S.S., Rahman, S., Ahmed, M.U., Aditya, S.K., 2019. Ensuring cybersecure telemetry and telecommand in small satellites: Recent trends and empirical propositions. IEEE Aerosp. Electron. Syst. Mag. 34 (8), 34–49.

Schneier, B., 2000. Secrets & Lies: Digital Security in a Networked World. John Wiley & Sons Inc, New York, NY, USA.

Sheik, A.T., Maple, C., 2019. Edge computing to support message prioritisation in connected vehicular systems. In: 2019 IEEE Global Conference on Internet of Things (GCIoT), pp. 1–7.

Shevchenko, N., Frye, B., Woody, C., 2018. White paper: Threat Modelling for Cyber-Physical System-of-Systems: Methods Evaluation. Technical Report Software Engineering Institute. Carnegie Mellon University, URL: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=526365.

Shin, J., Son, H., Heo, G., et al., 2015. Development of a cyber security risk model using bayesian networks. Reliab. Eng. System Saf. 134, 208–217.

Shostack, A., 2008. Experiences threat modeling at microsoft. In: MODSEC@ MoDELS.

Suloway, T., Kordella, S., Visner, S.S., 2020. An attack-centric viewpoint of the exploitation of commercial space and the steps that need to be taken by space operators to mitigate each stage of a cyber-attack. In: ASCEND 2020, p. 4015.

Thomas, M., Norton, J., Jones, A., Hopper, A., Ward, N., Cannon, P., Ackroyd, N., Cruddace, P., Unwin, M., 2011. Global navigation space systems: reliance and vulnerabilities. The Royal Academy of Engineering, London.

Tsamis, N., Bailey, B., Falco, G., 2021. Translating space cybersecurity policy into actionable guidance for space vehicles. In: ASCEND 2021, p. 4051.

UcedaVelez, T., Morana, M.M., 2015. Risk Centric Threat Modeling: process for attack simulation and threat analysis. John Wiley & Sons.

Unal, B., 2019. Cybersecurity of NATO's Space-based Strategic Assets. Technical Report Chatham House. URL: https://www.chathamhouse.org/publication/cybersecurity-nato-s-space-based-strategic-assets.

Weyrich, M., Ebert, C., 2016. Reference architectures for the internet of things. IEEE Softw. 33 (1), 112–116.

Wilson, T., 2001Threats to united states space capabilities. URL: https://spp.fas.org/eprint/article05.html#23.

Winsen, S., 2017. Threat modelling for future vehicles: on identifying and analysing threats for future autonomous and connected vehicles. Master's thesis University of Twente.

Work, D., Bayen, A., Jacobson, Q., 2008. Automotive cyber physical systems in the context of human mobility. In: National Workshop on High-confidence Automotive Cyber-physical Systems, pp. 3–4.

Wu, Z., Zhang, Y., Yang, Y., Liang, C., Liu, R., 2020. Spoofing and anti-spoofing technologies of global navigation satellite system: A survey. IEEE Access 8, 165444–165496.

Yang, L., Cao, X., Li, J., 2016. A new cyber security risk evaluation method for oil and gas scada based on factor state space. Chaos, Solitons Fractals 89, 203–209.