Resilience in Space – Throughout a Mission‘s Life Time

Dr. Johanna Niecknig
Bundesamt für Sicherheit in der Informationstechnik
Bonn, Germany
Johanna.Niecknig@bsi.bund.de

Manuel Hoffmann
Thales Deutschland GmbH
Wilhelmshaven,
Germany
Manuel.Hoffmann@thalesgroup.com

Maximilian Roth
Airbus Defence and Space GmbH
Ottobrunn,
Germany
Maximilian.Roth@airbus.com

Sascha Fankhänel
Jade Hochschule Wilhelmshaven
Wilhelmshaven, Germany
Sascha.Fankhaenel@jade-hs.de

Stefanie Grundner
Panaglobo GbR
Berlin, Germany
stefanie@panaglobo.com

Tarsicio Lopez Delgado
Rivada Space Networks GmbH
München, Germany
TLDelgado@rivadaspace.com

Florian Göhler
Bundesamt für Sicherheit in der Informationstechnik
Bonn, Germany
Florian.Goehler@bsi.bund.de

***Abstract*—In 2021, the German Federal Office for Information Security (BSI) initiated a project group with experts from industry, research organizations and government agencies to develop cybersecurity requirements for space systems. The aim of the project group is to provide space information security supporting documents and tools. Effective cooperation between governmental bodies, in particular the federal ministries and authorities, industry and research not only create synergetic effects, but also ensures a joint solution-oriented focus. This approach contributes to the long-term acceptance of the security requirements and processes and promotes transparency. The initiative illustrates how cross-sector cooperation between different interest groups can be organized. As a first step the project group has provided recommendations for minimum security requirements of space systems based on the IT-Grundschutz methodology. They comprehensively cover the entire system's life cycles and are addressed to all stakeholders such as developers, manufacturers, operators, suppliers, etc.**

Keywords—cyber security, space, security requirements, international standardisation, future technologies, regulation, *(key words)***)**

I. Introduction

Security in space has long been a marginal topic. Recent developments, i.e., the massive space's commercialisation, has led to an enormous increase in the number of objects and players; especially in low earth orbit. At the same time, society increasingly relies on space-based services and capabilities that are essential for everyday life, for civilian and military security and for overall resilience. Despite the growing importance of space assets, there is little regulatory framework for assessing and improving their security, especially a lack of uniform regulations/standards on cyber security.

II. Objectives

One of the key objectives of the German Federal Office for Information Security (BSI) is to strengthen the cyber security of space systems relevant to the state, economy and society. The idea is to provide guidance to the industry. BSI decided to found a project group including commercial organisations (IT, cyber security, aerospace and start-ups), universities and governmental authorities (ministries, German armed forces, and BSI). The goal of the project group is to provide a series of documents on qualitative security requirements tailored to all space segments, i.e. space, ground, user and link.

Particularly, the ground segment, is currently subject to key legal requirements arising from the EU NIS2 Directive. Compliance with this directive requires the implementation of internationally recognized standards such as ISO 27001 for information security and ISO 22301 for business continuity management. The development of specific measures to meet these standards is an important part of a comprehensive compliance structure. Using the IT-Grundschutz methodology could be one possible way to do this.

III. Identification of Security requirements

A. IT-Grundschutz

IT-Grundschutz is a standard for the implementation of an Information Security Management System (ISMS). It was first published in 1994 and has been under continuous development since then. IT-Grundschutz consists of four BSI Standards and a Compendium with security requirements for 111 topics (in 2023).

BSI Standard 200-1 describes the general functioning of an ISMS from a management perspective [1].

BSI Standard 200-2 describes the IT-Grundschutz methodology [2]. The methodology consists of a Structure Analysis, a determination of protection needs and the modelling. During the modelling each asset in the scope of the ISMS is mapped to a module from the IT-Grundschutz Compendium. The result is an established security baseline that is tailored to the protection needs of the assets concerned. Beyond the security baseline, a risk assessment may be necessary for particular assets or system specifics. Finally, an implementation plan is laid out. The methodology described in BSI Standard 200-2 is compatible to the ISO 27001 Standard [2]. Hence, an ISMS working on IT-Grundschutz is also compliant to ISO 27001.

BSI Standard 200-3 provides a methodology for risk assessments [3]. It uses the well-known matrix approach and focuses on a qualitative evaluation of risks. BSI Standard 200-4 describes a Business Continuity Management System [4].

The core of the IT-Grundschutz is the IT-Grundschutz Compendium. The compendium contains 111 IT-Grundschutz modules. Each module is a collection of security measures for a specific topic. The modules cover technical, infrastructural, personal and organizational aspects of information security. For example, there are modules for Unix servers, Windows clients, server rooms, (security) awareness and training or security incident handling. Since the BSI performs a general risk assessment for each module, implementers only need to do a risk assessment themselves in case special conditions apply.

In practice, the IT landscape of many institutions inside the same industry looks similar. Therefore, the BSI developed the concept of IT-Grundschutz profiles.

IT-Grundschutz profiles are examplary descriptions of the individual steps of the IT-Grundschutz methodology for a specific domain. They describe a reference architecture and then apply each step of the methodology, including the modelling. They can also be expanded to include additional industry-specific security requirements.

This requires knowledge about typical IT infrastructures inside the domain at hand. Therefore, profiles are written by stakeholders from the corresponding industry, whereas the BSI provides support and guidance.

B. *IT-Grundschutz Profile for Space Infrastructures*

Based on the IT-Grundschutz methodology the project group developed an IT-Grundschutz profile for Space Infrastructures. The document defines a recommended minimum level of protection for the information security of satellites that should be taken into account throughout the satellite's life cycle. It is a manual supporting organisations to approach information security for space assets and offers a shortcut for organisations aiming to define a security baseline based on the IT Grundschutz methodology.

To this end, the different phases along a satellite's life cycle have been used for the so-called business processes. The business processes examined are:

- Conception and design
- Production
- Testing
- Transportation
- Commissioning
- Operation
- Decommissioning

The profile considers space specific system-oriented applications, IT systems and infrastructures, such as the on-board computer software, the checkout system, electrical and mechanical ground segment equipment, simulator, assembly and integration room, etc. These applications are assigned to the corresponding IT systems and environments, which leads to the protection requirements and the security measures for each of the selected modules in the IT-Grundschutz compendium.

C. *Technical Guideline TR-03184 - Information Security for Space Systems*

After the release of the IT-Grundschutz profile for Space Infrastructures, the Technical Guideline TR-03184 Information Security for Space Systems was published in July 2023.

Generally, the objective of technical guidelines by the BSI is to provide security measures and implementation notes for a specific context. They can also provide criteria for conformity tests of implemented security measures.

The TR-03184 provides a more detailed analysis of the security requirements derived from the IT-Grundschutz profile for Space Infrastructures. Additionally, this technical guideline contains a list of potential threats showing their impact on a space segment and defines security measures accordingly. This information helps the users to assess their needs for protection, but requires a mission- or project-specific adaptation (tailoring). Existing standards (e.g. protection profiles according to Common Criteria or interoperability standards, such as ISIS-MTT) are referenced and supplemented where necessary.

The logic, as shown in Figure 1, is to take the so-called elementary threats from the IT-Grundschutz Compendium and tailor them to space segment specific threats. The document lists a number of security measures that can be used to combat one or more threats. For each of the applications defined in the space infrastructure profile, there is an assignment of which threats apply to the individual application and which security measures can be used to mitigate them. Ultimately, one or several security measures are assigned to each threat.

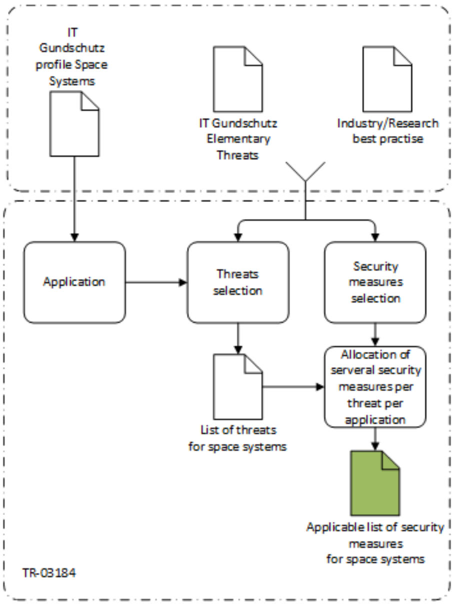
IT Gundschutz profile Space Systems
IT Gundschutz Elementary Threats
Industry/Research best practise
Application
Threats selection
Security measures selection
List of threats for space systems
Allocation of serveral security measures per threat per application
Applicable list of security measures for space systems
TR-03184

Figure 1: Workflow for assigning security measures to the list of threats

This enables the technical guideline user to formulate project-specific requirements: from the space segment threats defined in the technical guideline, the user can choose the threats applicable to a specific mission. As there are security measures already described for these threats, the user can select the appropriate measures and choose the strength accordingly to reduce the risk to an acceptable level.

This Technical Guideline is designed for high and very high protection requirements and is recommended by the BSI for the consideration of space systems with this protection level. Compared to the IT-Grundschutz profile, it also enables greater depth and refinement of the requirements for the satellite.

D. IT-Grundschutz Profile for the Ground Segment

While the scope of the two prior documents is the space segment, the next IT-Grundschutz profile, which will be published shortly, provides support for the protection of the ground segment. The IT-Grundschutz profile for the ground segment is considered a further step towards achieving information security for the entire system. The profile contains industry-specific notes for best practices and serves as a template for satellite manufacturers, integrators or operators and suppliers to perform all required steps of the IT-Grundschutz methodology.

IV. Outlook

From BSI's key objective, to strengthen the cybersecurity of space systems a comprehensive implementation strategy including objectives, fields of action and measures has been developed. In addition to drafting documents, the group pursues other activities to promote the exchange of information and knowledge between national and international bodies. In this way, incidents and changes in the threat situation can be recognized and preventive measures can be continuously updated and implemented.

In addition to the IT-Grundschutz profiles and technical guidelines already published, a number of other documents are planned, as shown in Figure 2.

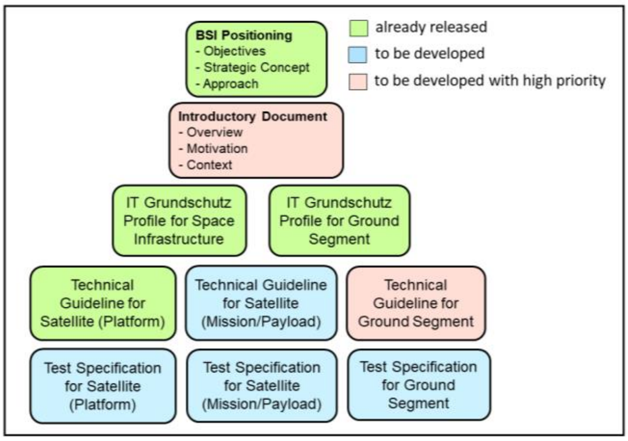
BSI Positioning
- Objectives
- Strategic Concept
- Approach
already released
to be developed
to be developed with high priority
Introductory Document
- Overview
- Motivation
- Context
IT Grundschutz Profile for Space Infrastructure
IT Grundschutz Profile for Ground Segment
Technical Guideline for Satellite (Platform)
Technical Guideline for Satellite (Mission/Payload)
Technical Guideline for Ground Segment
Test Specification for Satellite (Platform)
Test Specification for Satellite (Mission/Payload)
Test Specification for Ground Segment

Figure 2: Implementation Plan for Identification of Security Requirements

Furthermore, it is the declared goal of the project group to regularly revise the documents taking into account state of the art and perform conformity check. Further work will be put into adaptation of the technical guidelines with regard to more recent developments in standardisation, e.g. ECSS, SPACE-SHIELD, CCSDS, MITRE, SPARTA, NIST, etc., regulations, or legal requirements, such as the national and EU Space Law, Cyber Resilience Act, etc. Continuous review and improvement of these documents will establish a sustainable and effective security and compliance structure for the space systems.

With respect to BSI's challenging key objective the organisational structure of the project group has been adjusted and expanded accordingly. Next to project group 1 for the identification of security requirements three more project groups have been added. Goal of project group 2 is to monitor and support the international standardisation activities, as well as second the national contribution to the committee work of programs such as Secure Connectivity, Galileo and Copernicus. In exchange with project group 1, national recommendations and best practices shall be discussed and made available to European and international initiatives. An inventory of existing standards and standardisation developments for cyber security in space will be carried out. The project group is planning to perform a gap analysis, in order to identify missing fields of standardisation, determine compatibility conflicts, and possibly propose adjustments to existing standards and regulations.

The goal of project group 3 is to monitor new developments, technology and applications and evaluate their risks for cyber security.

Project group 4 focuses on the topic of regulation and will develop a concept for multi-level, standardised safety requirements for space systems, which could be implemented as a voluntary or mandatory directive by the industry. Finally, project group 4 plans to draw up a catalog of instructions on which set of security requirements may or should be used under certain conditions; e.g. which ESA requirements catalog or which Space Sustainability Rating (SSR) must be complied with for the respective case.

V. Conclusion

The working group is not aiming for another standard, but to provide users with an applicable, easy-to-use and adjustable tool kit. They are complementary to very specific frameworks, such as MITRE, SPACE SHIELD, NIST and ISO. Once the space applicable threats have been identified within the tailoring of the BSI documents to a certain space mission, the user can apply those frameworks to decide on security measures' implementation.

By using the BSI standard and methodology, the tailoring and adaptation of the profiles and technical guidelines to a certain space mission results in a comprehensive security approach that covers all information security domains along the mission's life cycle. This takes into account not only the compliance aspects, but also the space systems' individual requirements. The continuous application and improvement of these documents will ensure a sustainable and effective security and compliance structure for the space systems. In cooperation with all stakeholders this joint effort could build the basis for the development of a well-established and accepted label or seal of security/quality, thereby enhancing the transparency and comparability of implemented security standards.

Ultimately, the goal of the working group is to actively participate in the discussion on international standards (ECSS, CCSDS, IEEE, NIST, etc.), share expertise and know-how and jointly develop common standards on a European and/or international level.

References

[1] Information Security Management Systems, BSI Standard 200-1, 2017, Federal Office for Information Security.

[2] IT-Grundschutz Methodology, BSI-Standard 200-2, 2017, Federal Office for Information Security.

[3] Risk analysis based on IT-Grundschutz, BSI-Standard 200-3, 2017, Federal Office for Information Security.

[4] Business Continuity Management, BSI-Standard 200-4, 2023, Federal Office for Information Security.