



Federal Office  
for Information Security

# IT-Grundschutz Profile for Space Infrastructures

Minimum Protection for Satellites Covering their Entire Life Cycle



# Document history

Table 1: Document history

<b>Version</b>	<b>Date</b>	<b>Editor</b>	<b>Description</b>
1.0	30.06.2022		First publication

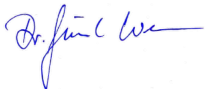
# Preface by the Department Head of Crypto-Technology and IT Management

In 2021, the Federal Office for Information Security (BSI) initiated a joint working group with experts from OHB Digital Connect and Airbus Defence and Space as well as the German Space Agency at the German Aerospace Center (DLR) to develop minimum cybersecurity requirements for satellites. In a first step, this working group has set up a first set of measures to achieve the security objectives specified in the BSI publication “Cybersecurity for Space Infrastructures”. The overall goal is to strengthen the cybersecurity of space infrastructures relevant to the state, economy and society. Of primary focus are the availability of space related services and the protection, integrity and authenticity of the communication between satellites and base stations.

Hence, this document represents a first company-specific IT-Grundschatz profile based on common minimum security requirements, which were derived in the series of BSI organised workshops with the joint working group. The profile intends to serve as a recommendation and guidance, which allows space actors effectively implementing an up-to-date security concept. Although company and mission-specific adaptations may be necessary, this profile serves as a template for individually adjusted security concepts based on the at any time similar underlying processes over the complete lifetime of a satellite.

In order to address the deviating protection needs of different satellite missions, BSI intends to detail the requirements in various technical guidelines after the creation of the IT-Grundschatz profile with the aim to establish these in an international context on the long-term, as well.

I would like to thank the members of the working group for their willingness to participate in the preparation of this IT-Grundschatz profile. I deem this work as very valuable.



Dr. Günther Welsch

Head of Cryptotechnology and IT Management

# Publisher

Federal Office for Information Security, OHB Digital Connect GmbH, Airbus Cybersecurity GmbH, Space Agency of the German Aerospace Center

Version: 1.0

Revision cycle: bi-yearly

Version IT-Grundschutz-Compendium 2022

# List of Abbreviations

Table 2: List of Abbreviations

<b>Abbreviation</b>	<b>Meaning</b>
AIT	Assembly, Integration and Test
AIV	Assembly, Integration and Verification
ASW	Application Software
BDSG	Federal Data Protection Act
BSI	Federal Office for Information Security
CCPA	California Consumer Privacy Act
CCSDS	Consultative Committee for Space Data Systems
DLR	German Aerospace Center
DMS	Document Management System
DNS	Domain Name System
DPA	Data Processing Agreement
ECSS	European Cooperation for Space Standardisation
EGSE	Electrical Ground Support Equipment
ERP	Enterprise Resource Planning
FPGA	Field Programmable Gate Array
GEO	Geostationary Earth Orbit
GDPR	General Data Protection Bill
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
IC	Integrated Circuit
IDE	Integrated Design Engineering
IDS	Integrated Detection System
IoT	Internet of Things
IPS	Integrated Prevention System
ISMS	Information Security Management System
KRITIS-V	KRITIS Regulation
LDAP	Lightweight Directory Access Protocol
LEO	Low Earth Orbit
MDM	Mobile Device Management
MEO	Medium Earth Orbit
MGSE	Mechanical Ground Support Equipment
NIST	National Institute of Standards and Technology
OBC	On Board Computer
OTRS	Open Ticket Request System
PDPB	Personal Data Protection Bill
PL	Payload
Requirements-Eng/Mgt	Requirements Engineering and Management System
RT-OS	Real Time Operating System
SatDSiG	Satellite Data Security Act
SCM	Supply Chain Management
SQL	Structured Query Language
PCS	Systems Tool Kit
TK	Telecommunications

# Table of Contents

1	Introduction.....	8
2	Formal Aspects.....	9
3	Disclaimer.....	10
4	List of Authors.....	11
5	Management Summary.....	12
5.1	Target Group.....	12
5.2	Objectives.....	12
5.3	Tasks of the Management Level.....	12
6	Definition of the Scope.....	14
6.1	Target Group.....	14
6.2	Description of the Protection Needs.....	14
6.3	IT-Grundschutz Procedure.....	14
6.4	Compatibility with Other Standards.....	14
6.5	Framework Conditions Taken into Account.....	15
7	Delimitation of the Information Domain.....	16
7.1	Components of the Information Domain.....	16
7.2	Parts not Considered.....	16
8	Reference Architecture.....	17
8.1	Processes.....	17
8.2	Applications.....	18
8.4.1	Network Plan.....	22
8.5	Buildings and Rooms.....	23
8.6	Assumptions and Explanations.....	24
8.7	Handling of Deviations.....	26
9	Requirements to be Met and Measures to be Implemented.....	27
9.1	Determination of the Protection Needs.....	27
9.1.1	General Conditions.....	27
9.1.2	Methodology.....	27
9.1.3	Example Missions.....	28
9.1.4	Protection Needs, Regulatory and Scenarios.....	28
9.1.5	Result of the Generic Protection Needs Analysis.....	30
9.1.6	Guidance for Developing an Individual Protection Needs Determination.....	30
9.2	Selection of the Relevant Modules.....	30
9.2.1	Higher-Level Modules (entire Information Domain).....	31
9.2.2	Modules per Target Object.....	33
9.3	Requirements for Satellites.....	35

---

9.3.1	General Requirements.....	35
9.3.2	Requirements for Transport.....	36
9.3.3	Launch Facility.....	36
9.3.4	Intersection in Orbit Phase and Ground Segment.....	37
9.3.5	Decommissioning.....	37
10	Residual Risk .....	39
11	Application Notes .....	40
12	Checklist – Minimum requirements for IT security in space infrastructures.....	41

# 1 Introduction

Protecting satellites by means of technical and organisational measures is recommended for each satellite mission. Protection is mandatory only for partial aspects of some missions. Missions covered by the KRITIS Regulation must be secured according to the state of the art. To date, this only concerns the European Satellite Navigation System GALILEO and is limited to its ground infrastructure only. At present, there are no regulations in place being considered for the implementation of information security concerning the satellite itself during its manufacturing (in particular with respect to the security-by-design concept) and operation. Hence, the realisation of information security by the involved industry is tied to each company's own responsibility or respective customer's specifications. The present document "IT-Grundschutz profile for space infrastructures – Minimum protection for satellites covering their entire life cycle" provides assistance in formulating requirements for minimum protection measures during planning, manufacturing and operation of a satellite and its end of mission.

Protection needs of different satellite missions range from "Normal" to "Very high". In order to cover at least the basic protection requirements for all types of satellite missions, the category of protection needs "Normal" was used. The described security measures protecting confidentiality, availability and integrity of information aim to minimise material loss and intangible damage across a satellite's lifetime. These security measures determined for the realisation of the above mentioned protection objectives must be adapted to each mission. If necessary, they need to be extended or complemented depending on the mission's criticality.

In close cooperation, the Federal Office for Information Security (BSI), together with OHB Digital Connect, Airbus and the German Space Agency at the German Aerospace Center (DLR) have developed this IT-Grundschutz profile with the aim to provide recommendations for information security to be implemented by manufacturers, operators and suppliers of satellites and their components.

An IT-Grundschutz profile serves as guidance for the structured creation of an IT security process. It is a prototype security concept that is intended to serve as a template for institutions applying this concept under comparable framework conditions. For this prototype the steps to be taken are expressed in general terms, following the IT-Grundschutz methodology. As a result, all interested satellite manufacturers and operators are able to increase information security within their context.

Based on the different phases of a satellite's life cycle, the IT Grundschutz profile comprises six business processes considered relevant. These are defined in Chapter 7.1. The present IT-Grundschutz profile includes:

- a list of relevant target objects (applications, IT systems and premises) to be protected;
- an assignment of the corresponding IT-Grundschutz modules including requirements and implementation instructions, as well as
- requirements that, due to their common satellite specific goals, go beyond IT-Grundschutz. For this purpose, a checklist is provided to support the implementation of those security requirements deemed necessary for the respective mission. This checklist is not intended to be exhaustive and may be adapted to mission-specific needs.

The IT-Grundschutz profile remains to be consistent with the requirements catalogue of the German Space Agency in DLR (Tailoring Catalogue – Product Assurance, Safety & Sustainability Requirements for DLR Space Projects, DLR-RF-PS-001), which envisages the IT-Grundschutz methodology as an applicable methodology.



---

## 2 Formal Aspects

Table 3: Formal Aspects

<b>Aspect</b>	<b>Description</b>
Title:	IT-Grundschutz profile for space infrastructures – Minimum protection for satellites covering their entire life cycle <sup>1</sup>
Authorship:	See chapter 4 “List of authors”
Editorship:	BSI, OHB Digital Connect, Airbus CyberSecurity, German Space Agency at DLR
Version status:	Published on 30.06.2022, Version 1.0 Finalised in May 2022
It-Grundschutz- Compendium	This IT-Grundschutz profile is based on the IT-Grundschutz Compendium of the BSI 2022 Edition
Revision cycle:	The relevance of the document is to be reviewed twice a year.
Confidentiality:	The document in this version is openly accessible.

---

<sup>1</sup> For the exact definition, see chapter 6.1.

### 3 Disclaimer

This document has been prepared with great care, but does not claim completeness or accuracy in all its details. The authors have no influence with regard to the application of this IT-Grundschutz profile by users and do not know the individual requirements for the respective security concepts, so that, by their nature, they cannot assume any liability for the effects on the legal position of the parties.

---

## 4 List of Authors

All participants of the workshop series “Minimum requirements for cybersecurity for satellites”, organized and moderated by the BSI, were involved in the preparation of the document. From this group a team of authors was built to create this document whom are listed in the following table.

Table 4: List of Authors

<b>Name</b>	<b>Organisation</b>
Dr. Johanna Niecknig	Federal Office for Information Security
Wim Fleischhauer	OHB Digital Connect GmbH (temporary)
Manuel Hoffmann	OHB Digital Connect GmbH
Miriam Goellner	Airbus CyberSecurity GmbH

All other participants involved in the creation of this profile have contributed to various work packages (e.g. for structural analysis, modeling, preparing the checklist), providing their expertise in fruitful discussions as well as proofreading this profile. They can be found in the table below.

Table 5: List of other Stakeholders in the Preparation of the IT-Grundschutz Profile

<b>Name</b>	<b>Organisation</b>
Birger Klein	Federal Office for Information Security
Wendel Lohmer	Federal Office for Information Security
Frank Christophori	Federal Office for Information Security
Stefanie Grundner	PanaGlobo – Geospatial Consultancy
Dr. Sabine Philipp-May	German Space Agency at DLR
Johannes Stahl	German Space Agency at DLR
Lukas Ellenrieder	Airbus Defence and Space GmbH
Erwin Hirschmüller	Airbus Defence and Space GmbH
Karel Kotarowski	Airbus Defence and Space GmbH
Prof. Dr. Steffen Kuntz	Airbus Defence and Space GmbH
Andreas Kopper	Airbus CyberSecurity GmbH
André Penzien	OHB Digital Connect GmbH
Niek van Dael	OHB System AG

## 5 Management Summary

### 5.1 Target Group

The IT-Grundschutz profile for satellites is aimed to support those responsible for information security in space facilities (manufacturing and operating satellites), see Chapter 6.

### 5.2 Objectives

This IT-Grundschutz profile is designed to help users to ensure information security in all processes related to the satellite lifecycle and to adapt their processes to satellite-specific needs. It is intended to serve as a template to implement the IT-Grundschutz of the BSI in an appropriate way.

This IT-Grundschutz profile defines a recommended minimum level of protection for satellite information security, which should be considered throughout the satellite's life cycle. For this purpose, business processes based on the life cycle of the satellite are defined. According to the approach of standard IT-Grundschutz protection, security requirements that should be met are described. The business processes examined are:

- Conception and design
- Production
- Test
- Transports
- Commissioning
- Operation
- Decommissioning

In addition, a common IT infrastructure has been defined as a cross-sectional process that combines all IT infrastructure that is used in all above-mentioned processes. This cross-sectional process simplifies the application of the BSI Grundschutz within the Grundschutz profile.

The BSI recommends the application of this IT-Grundschutz profile as an introduction to an information security concept. However, the actual application of recommended requirements has to be verified mission-specific.

Many satellite systems will be subject to a higher level of protection. In this case, the requirements exceeding the minimum protection as described here need to be applied.

Similarly, in some cases, a user of the profile may decide not to implement certain measures. These decisions should be documented and may be addressed in a risk assessment approach.

### 5.3 Tasks of the Management Level

The authors recommend to the management of space facilities to use this IT-Grundschutz profile as a basis for an information security concept in manufacturing and operating satellites (in addition to already established terrestrial requirements for the ground segment and general infrastructures).

The authors would also like to highlight the importance to thoroughly consider and handle information security risks in the supply chain. Therefore, the management must ensure that, in addition to the implementation of protection requirements for supply chain following IT-Grundschutz, any supplier is carefully selected according to its trustworthiness.

---

In the case of outsourcing of IT or processes, the authors recommend that the corresponding service providers guarantee a minimum protection (e.g. on the basis of this IT-Grundschatz profile).

## 6 Definition of the Scope

### 6.1 Target Group

The IT-Grundschatz profile for satellites is aimed to support decision-makers responsible for information security, information technology, infrastructure security and project managers of space facilities (manufacturing and operation of satellites). The focus is on the satellite itself, while the associated ground infrastructure or the launch segment, the supply chain etc. is not fully considered in this profile.<sup>2</sup> Within the supply chain, it will also help manufacturers and suppliers of satellite components to secure the planning and development of their systems and applications.

### 6.2 Description of the Protection Needs

The protection needs of satellite systems are determined according to missions, i.e. the need for protection depends on the task, size and criticality of the planned mission. Depending on the mission, there may be low to very high protection requirements.

Since this IT-Grundschatz profile targets recommendations for a *minimum* protection applicable to all types of satellites, the lowest level of protection needs was determined in a generic protection needs analysis, using five sample missions defined in Chapter 9.1.3. For this purpose, the scenarios relevant for information security were derived using various sample missions. On the other hand, regulatory requirements from norms, standards and laws were examined.

Based on the sample missions with the lowest damage impact, no scenarios have been identified that would exceed the protection needs category “Normal”.

For this IT-Grundschatz-Profile, the category of protection needs “Normal” was used as minimum level of protection to meet the security objectives confidentiality, integrity and availability. As a consequence this IT-Grundschatz profile is aiming at least for a Standard Protection in terms of the IT-Grundschatz approach.

### 6.3 IT-Grundschatz Procedure

The IT-Grundschatz of the BSI offers the IT-Grundschatz methodology basic, standard or core protection. Depending on the chosen IT-Grundschatz methodology, the requirements described in the modules must be implemented accordingly. The requirements described in this IT-Grundschatz profile meet at least the standard protection of the BSI standard 200-2. This corresponds to the recommended IT-Grundschatz methodology. It aims to provide comprehensive protection for all processes and sectors of the institution and may also serve as a basis for higher protection levels. Since the need for protection of each satellite mission is determined individually, it is recommended to also implement individual mission-specific requirements from a higher level of protection needs.

### 6.4 Compatibility with Other Standards

Implementing the standard protection approach compatibility with ISO 27001<sup>3</sup> is established. In addition, those requirements that go beyond the modules of IT-Grundschatz are based on common standards in the field of space and IT security, such as standards of the CCSDS, ECSS and NIST.

---

<sup>2</sup> It can be assumed that IT-Grundschatz is applicable to the ground segment without any space specific features and therefore a basic protection is provided, anyhow. Interfaces that are directly linked to the satellite and imply satellite specific features are included in this profile.

<sup>3</sup> <https://www.beuth.de/de/norm/din-en-iso-iec-27001/269670716> (accessed 01.07.2019)

---

## 6.5 Framework Conditions Taken into Account

According to §8a or §8f BSIG operators and manufacturers operating under the KRITIS or UBI Regulation have to follow obligations related to their facilities, e.g. the reporting of IT malfunctions and security incidents, or the protection of the systems according to the current state of the art or the self-commitment to IT security. In this regard, the KRITIS Regulation is limited to the ground segment of selected missions only.<sup>4</sup> However, there are currently no specific legal frameworks or legally binding standards for information security applicable to satellite missions.

---

<sup>4</sup> According to the BSI KritisV in Annex 7, Part 3, point 1.7.2, only the following segment exists as Critical Infrastructure (as of 2022): 1.7.2. Ground station of a satellite navigation system (measurement criterion: Classification of the installation in accordance with Regulation (EU) No 1285/2013 (threshold: Ground station))

## 7 Delimitation of the Information Domain

The interconnected components of an institution or a specific area of application are referred to as an information domain. The next section defines the components of the information domain “satellite” relevant to the IT-Grundschutz profile. Subsequently, the components of the information domain which are not taken into account in this IT-Grundschutz profile are listed.

### 7.1 Components of the Information Domain

The information domain “satellite” includes all processes and procedures relevant to the satellite directly or via interfaces throughout the entire life cycle, as well as all technical components such as applications, IT systems, rooms and buildings that support these processes and procedures.

### 7.2 Parts not Considered

The focus of this profile is on the satellite itself. Therefore, the ground segment, such as the ground control centre, or supporting infrastructure, e.g. for satellite launch, is not fully covered and only the interface directly related to the information security of the satellite is included in the information domain. However, the manufacturer/operator of a system is required to ensure that a comparable level of security can also be demonstrated in these facilities by their operators.



---

## 8 Reference Architecture

The reference architecture defines which applications, IT systems and spatial infrastructures (rooms, buildings, satellites, space) are relevant to the essential processes in the lifecycle of a satellite and should be secured in terms of IT-Grundschatz. The reference architecture and processes described below should also be used in an appropriately adapted form for other models, e.g. EM, Flatsat, of satellite development.

### 8.1 Processes

The business processes that are considered in this IT-Grundschatz profile are based on the life cycle phases of a satellite.<sup>5</sup> In the following, these processes are briefly described and labelled by an identifier.

#### G00 Common IT infrastructure

In addition to the phases corresponding to the life cycle of the satellite, a cross-sectional process is defined which describes the common IT infrastructure needed. Here, general IT infrastructures that are used in all business processes are summarised.

#### G01 Conception and Design

All activities preparatory to the manufacturing phase (system analysis, system definition, system design, mission analyses, in particular risk analyses, etc.) up to the complete determination of the system are summarised in this process. Technical pre-developments are excluded.

#### G02 Manufacture

In the “manufacture” process, developments of hardware and software, integration and assembly of all components, as well as the implementation of the corresponding security requirements are considered. This process also includes necessary pre-developments (including SCM management), as well as intermediate tests/integration tests (laboratory tests, etc.).

#### G03 Test

This phase includes functional tests and qualification tests. Similarly, this process looks after environmental tests carried out to ensure that the satellite works perfectly even after launch under space conditions.

#### G04 Transports

In this process, the transport of the satellite as well as special components (e.g. the crypto unit), to environmental tests or to the launch site, etc., is considered. The delivery of the system components is also included.

#### G05 Commissioning

The “commissioning” process involves the preparation of the satellite launch. These preparations include the final checks and, if necessary, the activation of instruments, ensuring the check of the launch rocket as well as all necessary facilities for launch, keying, and the launch of the satellite into the orbit. The launch and early orbit phase are also part of this process. Commissioning is typically completed by a Commissioning Results Review or a Flight Qualification Review.

---

<sup>5</sup> With regard to the definitions of ECSS standards the chosen life phases have been combined according to practicality or supplemented by further phases/processes.

## G06 Operation

This phase describes the operation of the satellite. The process typically includes the following subprocesses: Monitoring, maintenance, quality control of data streams, command transfer, command implementation, acceptance of control data from control center.

## G07 Decommissioning

During this phase the decommissioning of the system will be carried out.

## 8.2 Applications

In addition to the processes, the information domain also includes applications that support the editing of the processes. Besides general applications or services (e.g. e-mail service or data exchange service) also space specific applications and services (e.g. analysis tools, EGSE, simulators) have to be considered in the satellite life cycle, as well as applications, components, devices and services on board the satellite (e.g. platform, payload, SAT controller). These applications mentioned above are listed in the following table, labelled by an identifier. The right column indicates which processes are supported by the applications.

Table 6: Applications of the Information Domain “Satellite”

<i>Identifier</i>	<i>Applications of the information domain</i>	<i>Supported processes</i>
<b>A101</b>	Directory service	G00
<b>A102</b>	Storage service	G00
<b>A103</b>	DNS service	G00
<b>A104</b>	Central time service	G00
<b>A105</b>	Web Service	G00
<b>A106</b>	File Service	G00
<b>A107</b>	Virtualisation service	G00
<b>A108</b>	Containerisation service	G00
<b>A109</b>	Data exchange service	G00
<b>A110</b>	Telephony	G00
<b>A111</b>	Printing service	G00
<b>A113</b>	Mobile phones	G00
<b>A114</b>	E-mail service	G00
<b>A115</b>	Office incl. video and email client	G00
<b>A201</b>	CAD Server	G01, G02
<b>A202</b>	CAD Client/Standalone	G01, G02
<b>A203</b>	Ticket System Server	G01, G02, G03, G05, G06, G07
<b>A204</b>	Ticket System Client	G01, G02, G03, G05, G06, G07

<i>Identifier</i>	<i>Applications of the information domain</i>	<i>Supported processes</i>
A205	DMS-KonfigMgmt Server	G01, G02, G03, G05, G06
A206	DMS-KonfigMgmt Client	G01, G02, G03, G05, G06
A207	Source code management, Buildchain, UnitTests Server	G01, G02, G03
A208	IDE Client/Standalone	G01, G02, G03
A209	Requirements-Eng/Mgmt Server	G01, G02, G03
A210	Requirements-Eng/Mgmt Client	G01, G02, G03
A211	Analysis tools	G01, G02, G03, G05, G06, G07
A212	ERP Server	G02
A213	ERP Client	G02
A214	Soft/Hardware Test Tools	G02, G03, G05, G06
A215	Simulators	G02
A216	Production systems	G02
A217	Checkout system	G02, G03, G05
A218	EGSE	G02, G03, G04, G05
A219	MGSE	G02, G03, G04, G05
A220	Applications/Tools of the Test Center	G03
A221	Transport container software	G04
A301	Sat ASW Platform	G02, G03, G04, G05, G06, G07
A302	Sat ASW Payload	G02, G03, G04, G05, G06, G07
A303	Sat Control Unit/Controller	G02, G03, G04, G05, G06, G07
A304	Sat Communication	G02, G03, G04, G05, G06, G07
A305	SAT GNSS	G02, G03, G04, G05, G06, G07
A306	Sat Autonomy Systems	G05, G06, G07

A101-A115 are general applications and services, A201-A221 specific applications and services and A301-A306 satellite specific applications and services.

## 8.3 IT Systems

Table 7: IT Systems of the Information Domain "Satellite"

<i>Identifier</i>	<i>IT-Systems of the information domain</i>	<i>Abhängige Anwendungen</i>	<i>Abhängige Prozesse</i>
S101	Storage platform	A101	G00

S102	DNS	A102	G00
S103	Time synchronisation	A103	G00
S104	Web server	A104	G00
S105	Fileservers	A105	G00
S106	Virtualisation platform	A106	G00
S107	Container platform	A107	G00
S108	Win/Linux/DB	A108	G00
S109	Data exchange server Win/Linux/DB	A109	G00
S110	TK system	A110	G00
S111	Print server Win/Linux	A111	G00
S112	Printer	-	-
S114	Email Server Win/Linux	A114	G00
S115	Office client all OS, tablet, laptop and desktop	A115	G00
S201	Win/Linux/DB	A201	G01, G02
S202	CAD Client Win/Linux, Laptop and Desktop	A202	G01, G02
S203	Win/Linux/DB	A203	G01, G02, G03, G05, G06, G07
S204	Ticket Client Win/Linux, Laptop and Desktop	A204	G01, G02, G03, G05, G06, G07
S205	Win/Linux/DB	A205	G01, G02, G03, G05, G06
S206	DMS-KonfigMgmt Client Win/Linux, Laptop and Desktop	A206	G01, G02, G03, G05, G06
S207	Win/Linux/DB	A207	G01, G02, G03
S208	IDE Client All OS, Laptop and Desktop	A208	G01, G02, G03
S209	Win/Linux/DB	A209	G01, G02, G03
S210	Requirements Client Win/Linux, Laptop and Desktop	A210	G01, G02, G03
S211	Analysis Tool Client Win/Linux, Desktop, Laptop, Tablet	A211	G01, G02, G03, G05, G06, G07
S212	ERP Server Win/Linux/DB	A212	G02
S213	ERP Client Win/Linux, Desktop	A213	G02
S214	Proprietary systems partly based on Win/Linux/RT-OS, possibly laptop, tablet	A214	G02, G03, G05, G06
S215	Proprietary systems partly based on Win/Linux/RT-OS	A215	G02

S216	Proprietary systems partly based on Win/Linux/RT-OS, possibly supplemented by proprietary and open process control technology	A216	G02
S217	Win/Linux/DB	A217	G02, G03, G05
S218	EGSE hardware with controller PC Win/Linux, laptop, tablet	A218	G02, G03, G04, G05
S219	Proprietary systems from proprietary microcontroller base to industrial PC with Win/Linux/RT-OS, laptop, tablet	A219	G02, G03, G04, G05
S220	Proprietary systems partly based on Win/Linux/RT-OS	A220	G03
S221	Proprietary systems of proprietary microcontroller base	A221	G04
S301	On-board computer platform with RT-OS (processor module)	A301	G02, G03, G04, G05, G06, G07
S302	On-board computer payload with RT-OS (processor modules)	A302	G02, G03, G04, G05, G06, G07
S303	Microcontrollers	A303	G02, G03, G04, G05, G06, G07
S304	Telemetry Tracking & Command System (TT&C), Crypto Unit, On-Board Computer/Data Handling System	A304	G02, G03, G04, G05, G06, G07
S305	Proprietary Controller	A305	G02, G03, G04, G05, G06, G07
S306	On-board computer platform with RT-OS (processor or special module)	A306	G05, G06, G07

## 8.4 Networks and Network Components

Applications and IT systems of the information domain “satellite” are integrated into various networks. Although the number and structure of the networks cannot be generalised in detail, it is assumed that the architecture of many sample missions is at least similar with regard to networks and network components.

For this reason, individual modules have been selected for the architecture of a sample mission, which will be implemented within the framework of the “Satellite” information domain. These are system modules of the layer NET, which include networking aspects in relation to network connections and communication.

The following modules of the NET layer have been selected:

- Network Architecture and Design (NET.1.1)
- Network Management (NET.1.2)
- Wi-Fi Operation (NET.2.1)
- Wi-Fi Usage (NET.2.2)
- Routers and Switches (NET.3.1)
- Firewall (NET.3.2)
- VPN (NET.3.3)

The module network architecture and design is applied to the overall network of an example mission, including all subnetworks. Subnetworks of the information domain “satellite” are, for example, the

subnetwork of the server room or the subnetwork of the office space, as shown in the chart of the network plan in section 8.4.1.

In addition to the module network architecture and design, the module network management is also applied to this information domain. As part of network management, the various network components are comprehensively integrated. Appropriate measures are also implemented to protect the communication and infrastructure of the network management.

Other relevant modules are the modules WLAN operation and Wi-Fi usage. WLAN operation and Wi-Fi usage are foreseen for the subnetworks of satellite integration, the launch centers, and the test centers, where, for example, mobile devices monitor or control the integration of the satellite.

Network components are also considered as part of the information domain. For this reason, also the modules routers and switches as well as the module firewall of the layer NET have been selected. Routers and switches are not mapped in the network plan because the IT infrastructure is different from mission to mission. However, firewalls and key devices for the segmentation of the entire network and for establishing a VPN connection are shown.

### **8.4.1 Network Plan**

Figure 1 below shows the network plan of the “satellite” information domain. It is a general presentation of the entire ground and space infrastructure of an example mission, including all life cycles of the development process.

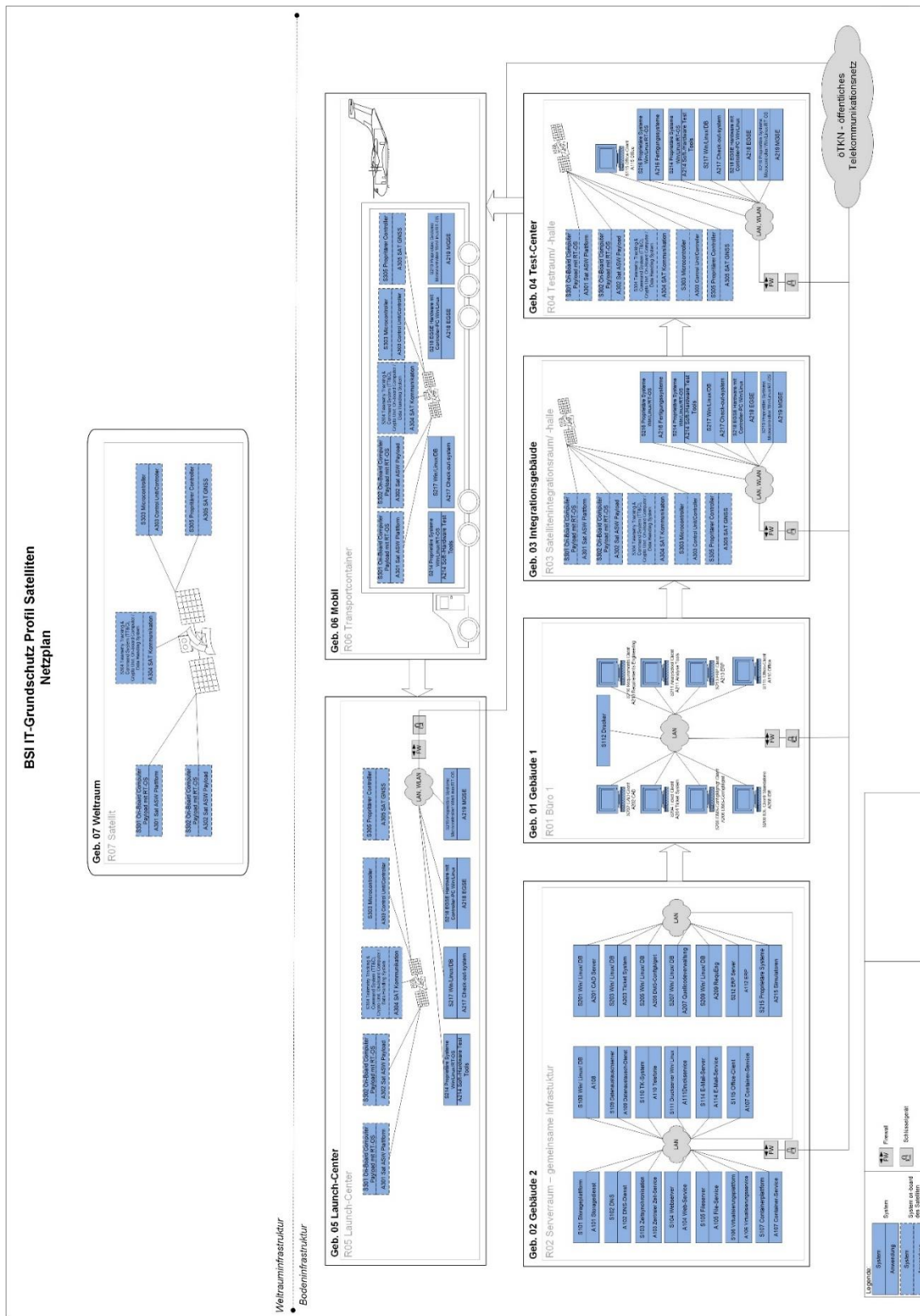


Figure 1: Network Plan of the Information Domain „Satellite“

## 8.5 Buildings and Rooms

Not only the components of information technology play an important role in information security. The security of buildings and rooms in which the satellite or systems or components of the satellite’s life cycle

are manufactured, tested, transported and operated, or where employees are active, must also be taken into account following the IT-Grundschutz protection. The special characteristics of the satellite is that the satellite itself can also be regarded as “room”, and space as a “building”.

Table 8: Rooms of the Information Domain “Satellite”

<b>Identifier rooms</b>	<b>Rooms of the information domain</b>	<b>Identifier building</b>	<b>Buildings of the information domain</b>	<b>IT systems or processes installed in the rooms</b>
<b>R01</b>	Office 1	G01	Building 1	S112, S114, S202, S204, S206, S208, S210, S211, S213
<b>R02</b>	Server room	G02	Building 2	S101, S102, S103, S104, S105, S106, S107, S108, S109, S110, S111, S114, S201, S203, S205, S207, S209, S212, S215
<b>R03</b>	Satellite integration room/-hall	G03	Integration buildings	S214, S216, S217, S218, S219, S301, S302, S303, S304
<b>R04</b>	Test room/– hall	G04	Test center	S214, S217, S218, S219, S220
<b>R05</b>	Launch hall	G05	Launch center	S214, S217, S218, S219
<b>R06</b>	Rack/transport container	G06	Transport container (truck, aircraft)	S218, S221
<b>R07</b>	Satellite	G07	Space	S214, S301, S302, S303, S304, S305, S306
<b>R07</b>	Satellite	G03, G04	Integration - building, Test center	S214, S301, S302, S303, S304, S305
<b>R07</b>	Satellite	G05	Launch center	S301, S302, S303, S304, S305, S306
<b>R07</b>	Satellite	G06	Transport container (truck, aircraft)	S301, S302, S303, S304

## 8.6 Assumptions and Explanations

In the following, the assumptions made for the structure analysis in order to select the reference architecture are summarised and further explanations on various target objects are given.

- Systems, such as e-mail servers, do exist several times – even within one business process – as there are usually several or many contributing companies within one business process. However, multiple systems in the information domain would not generate additional benefit, since no special features are to be expected opposite to a simplification.
- Generic services (including servers) are used to cover a wider spectrum. For example, the term “email server” is used instead of mentioning specific products such as Exchange, Postfix or Notes in the analysis (and modeling). When actually applying the IT-Grundschutz profile, the structure analysis must be expanded to include specific services or products.
- Test activities are apparent in several business processes, as they are carried out at different times with different means and goals.



- 
- For applications and IT systems that appear in different business processes, the same IDs are assigned. The reason for this is the assumption that there are no changes for the vast majority of systems across business processes.
  - Containers are not distinguished in terms of their use. If different fields of application with different protection requirements are identified during the analysis of the protection requirements and inheritance, an extension can be made.
  - With respect to the satellite components, the satellite is regarded as a room and space as a building (after launch). In this way, different phases (on the ground, transport, in space) can be distinguished and different threats/measures of the location can be mapped.
  - An Office as a communication medium remains part of the business process “operation”, because, for example, information about malfunctions must be exchanged between the operator and the manufacturer.
  - The implementation of process or program logic as software or hardware (e.g. FPGA) is not considered, but the generic case, the implementation as software, is considered.
  - In the structure analysis the supply chain security is not analysed in detail. In practice, it should be thoroughly considered, being aware of risks of manipulated components such as FPGAs, microcontrollers, other ICs, software, etc.
  - The outsourcing of parts or complete IT systems or processes is not explicitly considered but is conceivable and possible for all IT systems or processes. The same applies to the use of cloud services.
  - In the application “Mobile telephony”, the target objects IT systems, rooms and buildings are no longer listed or specified, since, on the one hand, the impact of the information owner on the mobile operator is low and, on the other hand, the effect on modelling is low.
  - IDE: The use of individual IDEs is rare nowadays. IDE has been enhanced with other components, e.g. source code management, build chain, unit testing, etc.
  - Telephony/TK: The TK system includes both, soft and hardphones based on VOIP, as well as TK servers or typical TK systems with extensions.
  - Transport containers for SAT and components are not considered as EGSE/MGSE, but as mobile rooms with air conditioning, alarm and building services. For this purpose, the containers may contain power generators or may be connected to those.
  - Transport container software: Software used in transport containers serves, for example, as air conditioning, transport localisation, alarm or ensuring of energy supply.
  - Ticket system: A ticket system usually consists of a central server and a client. Servers are usually operated on the basis of Linux or Windows and have an open (e.g. SQL) or a proprietary database. For web-based ticket systems, the client consists of a client system with a browser. There is no need for a dedicated client system. The term is used in a general sense and no specific products, e.g. Jira or OTRS, are listed.
  - DMS-KonfigMgmt (Document Management incl. Configuration Management System): A document management including configuration management system usually consists of a central server and a client. Servers are usually operated on the basis of Linux or Windows and have an open (e.g. SQL) or a proprietary database. For web-based DMS systems, the client consists of a client system with a browser. There is no need for a dedicated client system. The term is used in a general sense and no specific products, e.g. Eclipse or Sapienza, are listed.
  - Prototyping and software development: During prototyping and software development, development environments (IDE) are run on clients in conjunction with central source code management, build and unit testing systems. Typical server environments are based on Linux or Windows and have an open (e.g. SQL) or a proprietary database.

- Requirements-Eng/Mgt (Requirement Engineering and Management Systems): A requirement engineering and management system usually consists of a central server and a client. Servers are usually operated on the basis of Linux or Windows and have an open (e.g. SQL) or a proprietary database. For web-based requirements systems, the client consists of a client system with a browser. There is no need for a dedicated client system. The term is used in a general sense and no specific products, e.g. doors, are listed.
- ERP (Enterprise Resource Planning, in particular production planning and production-related applications): ERP systems usually consist of a central server and a client. Servers are usually operated on the basis of Linux or Windows and have an open (e.g. SQL) or a proprietary database. For web-based ERP systems, the client component consists of a client system with a browser. There is no need for a dedicated client system. The term is used in a general sense and no specific products, e.g. SAP, are listed.
- Sat ASW (application-specific satellite software platform and payload): Application software for payload can be integrated on the platform's on-board computer (OBC, specifically processor module) for small missions. For larger requirements or missions, a stand-alone OBC or processor module for the payload can be used.
- Sat Communication: The SAT communication (software) can be integrated into different units of a satellite: Telemetry Tracking & Command System (TT&C), Crypto Unit, On-Board Computer/Data Handling System. For specific payloads (e.g. Telekom-Sat), the payload has dedicated systems for SAT communication.
- Sat Control Unit/Controller: Microcontrollers can be used in subsystems (e.g. thermal, power) that process sensor data decentralised and trigger actions.
- Checkout system: The checkout system may also be used for launch, e.g. to charge the batteries. Examples of checkout systems: Terma CCS, SCOS-2000.
- EGSE: EGSE systems often consist of custom hardware with EGSE controller based on an industrial PC with Win/Linux. Examples of EGSE systems: S-Band SCOE, Ka-Band SCOE, EPS SCOE, AOCS SCOE, PL SCOE, Crypto SCOE.
- MGSE: In contrast to EGSE systems, MGSEs are mainly mechanical support devices, but feature electronic and in cases network controls. Examples: Trolley, cranes with network control.
- Soft/Hardware Test Tools: Examples of soft/hardware test tools are networkable oscilloscopes or digital multimeters.
- Simulators: Simulators are usually used in the development network. Simulators in the integration halls are represented by EGSE. Examples of simulators: Flight dynamics with MATLAB, Simulink, AGI's Systems ToolKit (STK), ESA's godot, GMAT, Orekit.
- Crypto Hardware/Software: This can be understood as dedicated devices, plug-ins into the OBC, integrated in TM/TC slots or other solutions.

## 8.7 Handling of Deviations

If the information domain to be protected deviates from the reference architecture shown here, the additional or non-existent objects should be documented and justified. The objects should be assigned to the appropriate components of the IT-Grundschutz Compendium. The derived requirements should be adapted to the respective protection needs.

---

# 9 Requirements to be Met and Measures to be Implemented

The BSI IT-Grundschutz Compendium provides modules that provide application-related recommendations for the implementation of IT-Grundschutz. First, the protection needs of the processes, applications, IT systems and communication connections are defined. Subsequently, the relevant modules are identified and an adaptation of the requirements to the corresponding target group is carried out. The result of the adaptation of the requirements may imply that all or only specific requirements of the module are relevant for information security in satellites or for their manufacturing and operation. Requirements may also be classified as completely irrelevant. The relevance of measures listed in the requirements should also be identified.

Furthermore, there are specific requirements for satellites that are not sufficiently modelled in the existing IT-Grundschutz modules. These additional requirements are listed at the end of this chapter. A supplementary security analysis may be required here.

## 9.1 Determination of the Protection Needs

### 9.1.1 General Conditions

The analysis of protection needs for a BSI IT-Grundschutz profile differs from a typical analysis of protection needs for the information domain of an institution or a project environment in the following points:

- There are no dedicated information owners available to identify the protection needs of the information concerned.
- The mission and therefore also function, size and criticality of the satellite, is not concretely known and cannot be used to determine the need for protection.

For this initial version of the IT Grundschutz profile, measures for a *minimum* protection are described, which should be applicable to all satellite missions. Therefore, mission examples are used to identify those with the lowest protection needs. This protection needs will be used to collect minimum requirements for satellite (-infrastructures).

### 9.1.2 Methodology

Due to the above-mentioned framework conditions, a top-down approach is used, considering different mission examples to allow for a general assessment of possible protection needs.

Relevant scenarios for space infrastructures and general regulatory requirements are combined with the mission examples to present the respective relevance.

For determining the minimum protection needs, it is sufficient to identify those combinations that require the lowest protection needs. All other relations represent higher protection needs and are not to be considered for this IT-Grundschutz profile.

The principles applied are listed in the following table:

Table 9: Application of the Principles

<i>Procedure</i>	<i>Principle</i>
Risk analysis, scenario derivation and filtering	Maximum principle
Filtering regulation to example missions	Minimum principle
Filtering scenarios for sample missions	Minimum principle
Evaluation within the final sample mission	Maximum principle

### 9.1.3 Selected Mission Examples

For the generic analysis of protection needs, example missions of different sizes and objectives are considered in order to determine the applicability of scenarios and the potential damage of these.

Table 10: Example Missions

<i>Name</i>	<i>Remark</i>
<b>M.01</b>	The mission includes a micro-satellite for scientific experiments brought into a near-earth orbit. It is put out of service at the end of the mission, ideally in a controlled way.
<b>M.02</b>	The mission includes one, several or many telecommunication satellites with a long mission duration. The orbits may be LEO, MEO and GEO.
<b>M.03</b>	Commercial <sup>6</sup> mission for Earth observation with long mission duration. The orbit is usually LEO.
<b>M.04</b>	Military mission for Earth observation with long mission duration. The orbit is usually LEO.
<b>M.05</b>	Mission for navigation satellites in a constellation, which have a long mission duration and are placed in a MEO.

### 9.1.4 Protection Needs, Regulatory and Scenarios

The consideration of the information security risks of relevant parties is clarified by using scenarios.

Due to the generalization of requirements derived from norms, standards and laws, the regulatory aspect is considered separately.

#### 9.1.4.1 Protection Needs Metric

For the classification of the protection needs, the BSI IT-Grundschutz methodology recommends to differentiate three categories:

- “Normal” – N
- “High” – H
- “Very high” – SH

Fundamental to determining the protection needs is the damage that would result from a breach of the basic objectives of information security, confidentiality, integrity or availability. The following table links the categories of protection needs with the possible damage effects:

Table 11: Related Protection Needs Category and Damage Impact

<i>Protection needs category</i>	<i>Damage impact</i>
<b>Normal</b>	The effects of damage to the satellite systems or the operators or manufacturers are limited and manageable.
<b>High</b>	The damage effects can significantly hamper the operation of the satellite system. For operators or manufacturers, the consequences can be considerable.

<sup>6</sup> For the M.03 and M.04 missions, earth observation missions for commercial and military purposes are analysed differently due to their different characteristics at mission level and concomitant differences in protection needs. Whereas, this distinction is not considered necessary for communication systems, M.02, for which there is no such stringent separation between military and civilian/commercial use.

<b>Protection needs category</b>	<b>Damage impact</b>
<b>Very high</b>	The damage effects may reach an existentially threatening, catastrophic scale for the operator or manufacturer. They may shut down the operation of the satellite system.

### 9.1.4.2 Regulatory Requirements

Requirements from norms, standards and laws have a general effect on the parties concerned. Below some selected, relevant regulatory text excerpts are shown as well as their relation to the sample missions:

Table 12: Regulation Requirements

	<b>M.01</b>	<b>M.02</b>	<b>M.03</b>	<b>M.04</b>	<b>M.05</b>
Satellite Data Security Act (SatDSiG)	—	—	x	—	—
Federal Data Protection Act (BDSG)/EU GDPR Other national data protection laws (CCPA, PDPB, DPA, etc.)	—	x/partial	—	—	special services
It Security Act 2.0	—	—	—	—	if necessary.
EU NIS2 Directive	x/partial	x/partial	x/partial	x/partial	x/partial
KRITIS-V	—	—	—	—	x/partial

### 9.1.4.3 Scenarios

Scenarios relevant for the Grundschutz profile were derived from the elementary threats and potential level of damage. The relations to the missions are shown in the table below. In addition to the scenarios, the persons affected by the scenarios are presented.

Table 13: Relevant Scenarios

<b>Affected persons</b>	<b>Scenarios</b>	<b>M.01</b>	<b>M.02</b>	<b>M.03</b>	<b>M.04</b>	<b>M.05</b>
Users/End customers	Availability of PL information	N	N	N	H/VH	H
Users/End customers	False/Falsified PL Information	N	N	N	H/VH	H
Users/End customers	Wrong S/C Reconfiguration by User	N	N	N/H	H/VH	
Affected persons	Scenarios	N	N	N	H/VH	
Users/End customers	User's operational restriction due to manipulation/false use by other users	N	N/H	N/H	H	N
Satellite owners	Loss of own satellites	N	N	N	H	H
Satellite owners	Unauthorised use	N		N	H	
Satellite owners	Operational constraints due to intended/unintended manipulation	N	N	N	N/H	H

<i>Affected persons</i>	<i>Scenarios</i>	<i>M.01</i>	<i>M.02</i>	<i>M.03</i>	<i>M.04</i>	<i>M.05</i>
Satellite owners	Operational restriction by Denial of Service	N	N	N	H/VH	H
Satellite owners	Interference/damage from other satellites	N	N/H	N/H	N/H	N/H

### 9.1.5 Result of the Generic Protection Needs Determination

In the previous chapters, the sample missions, scenarios and regulatory systems have been related with each other based on a top-down approach.

The sample mission M.01 is the mission with the least damage impact. Within this sample mission, no scenario has been identified which exceeds the protection needs category “Normal”.

For this IT-Grundschutz profile, the protection needs category “Normal” for the security objectives confidentiality, integrity and availability should therefore be assumed as the least protection needs.

### 9.1.6 Guidance for Developing an Individual Protection Needs Determination

This IT-Grundschutz profile is intended to provide minimum requirements for each satellite mission, so the minimum protection needs category was identified in Chapter 9.1.5. This profile does not provide requirements for further protection needs (these may be offered in a next version of the IT-Grundschutz profile or a technical guideline, respectively). Until such requirements, supporting enhanced information security requirements for missions and infrastructures with higher protection needs, are provided, it is recommended that the reader of the profile should analyse the additional protection needs himself. In case of increased protection needs (“high”, “very high”) for individual target objects, a standard or basic protection is not sufficient. The requirements should therefore be adapted accordingly, i.e., for example measures beyond standard protection should be identified and implemented. The German online course on IT-Grundschutz (Lektion “[Schutzbedarfsfeststellung](#)”) on the BSI website provides support in form of step-by-step instructions on how to perform a company- and mission-specific determination of protection needs.

## 9.2 Selection of the Relevant Modules

The IT-Grundschutz Compendium is updated annually. The BSI publishes the latest version on its homepage.<sup>7</sup>

In the Table 14 to Table 23, each component from the **2022 Compendium** is listed and checked for relevance in the present IT-Grundschutz profile. If a module is not relevant, this is justified. The minimum principle applies: Only those modules are considered that are significant to a majority of potential users of this profile. With this approach the IT-Grundschutz profile focuses on essential and reusable aspects. This simplifies the subsequent implementation for institutions. Regardless of this, users of the profile should examine to what extent their information domain differs from the profile. If necessary, further modules need to be classified as relevant in a subsequent implementation. For many mission one needs to consider protection needs of a higher category than the category “Normal”, used for this profile.

<sup>7</sup> [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-certification/IT-Grundschutz/IT-Grundschutz-Compendium/it-grundschutz-kompendium\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-certification/IT-Grundschutz/IT-Grundschutz-Compendium/it-grundschutz-kompendium_node.html) (accessed 18.05.2022)

## 9.2.1 Higher-Level Modules (entire Information Domain)

Table 14 to Table 19 list the modules that should be applied across the entire information domain. These comprise holistic requirements and are applicable to all parts of the information domain. On the other hand, Table 20 to Table 23 (Chapter 9.2.2) list system modules. System modules handle characteristics of certain components. Here it is crucial whether the module is relevant to a specific component specified in Chapter 7.

### ISMS: Security management

Table 14: Relevance of the Modules from the layer ISMS: Security Management

ID	Module	Relevant?	Justification (if not relevant)
ISMS.1	Security Management	Yes	

### ORP: Organisation and staff

Table 15: Relevance of the Modules from the Layer ORP: Organisation and Staff

ID	Module	Relevant?	Justification (if not relevant)
ORP.1	Organisation	Yes	
ORP.2	Personnel	Yes	
ORP.3	Information Security Awareness and Training	Yes	
ORP.4	Identity and Access Management	Yes	
ORP.5	Compliance Management	Yes	

### CON: Concept and approach

Table 16: Relevance of the modules from Layer CON: Concept and Approach

ID	Module	Relevant?	Justification (if not relevant) and guidance
CON.1	Crypto Concept	Yes	Depending on satellite mission, however, required to control the satellite.
CON.2	Data Protection	No	Usually, no processing of personal or related data takes place
CON.3	Backup Concept	Yes	
CON.6	Deleting and Destroying data and Devices	Yes	
CON.7	Information Security on Trips Abroad	Yes	
CON.8	Software Development	Yes	
CON.9	Information Exchange	Yes	
CON.10	Development of Web Applications	No	Usually, no web applications are developed.

Under the CON.1 crypto concept, adequate encryption of communication, in particular of satellite control, should be established in order to achieve the protection objectives of confidentiality, integrity and authenticity of communication. For this purpose, the communication links to be protected should be defined and the relevant protection objectives (if applicable, only a selection of the above mentioned

protection objectives) should be assigned. For the selection of suitable crypto methods, the technical guideline TR 02102 of BSI is recommended.

## OPS: Operation

Table 17: Relevance of the Modules from Layer OPS: Operation

<b>ID</b>	<b>Module</b>	<b>Relevant?</b>	<b>Justification (if not relevant) and guidance</b>
OPS.1.1.2	Proper IT Administration	Yes	
OPS.1.1.3	Patch and Change Management	Yes	Can be handled differently between ground segment and satellite
OPS.1.1.4	Protection Against Malware	Yes	
OPS.1.1.5	Logging	Yes	
OPS.1.1.6	Software Tests and Approvals	Yes	
OPS.1.1.7	System Management	Yes	
OPS.1.2.2	Archiving	Yes	Test data from simulations as well as AIV/AIT should be archived over the mission period in order to be able to analyse overlooked trends on errors that may occur in orbit.
OPS.1.2.4	Teleworking	Yes	
OPS.1.2.5	Remote Maintenance	Yes	
OPS.2.1	Outsourcing for Customers	No	
OPS.2.2	Cloud Usage	Yes	
OPS.3.1	Outsourcing for Service Providers	Yes	

## DER: Detection and reaction

Table 18: Relevance of the Modules from Layer DER: Detection and Reaction

<b>ID</b>	<b>Module</b>	<b>Relevant?</b>
DER.1	Detection of Security Relevant Events	Yes
DER.2.1	Security Incident Handling	Yes
DER.2.2	Provisions for IT Forensics	Yes
DER.2.3	Clean-up of Extensive Security Incidents	Yes
DER.3.1	Audits and Revision	Yes
DER.3.2	Audits Based on the BSI "Guideline for IS-Audits"	Yes
DER.4	Business Continuity Management	Yes

## APP: Applications

Table 19: Relevance of the Higher-Level Modules from Layer APP: Applications

<b>ID</b>	<b>Module</b>	<b>Relevant?</b>
APP.7	Development of Individual Software	Yes

The SYS.3.2.2 Mobile Device Management (MDM) and IND.1 Process Control and Automation Technology also apply to the entire information domain.



## 9.2.2 Modules per Target Object

The following tables list the system components. Here it is crucial whether the module is relevant to a specific target object specified in Section 7.

### APP: Applications

Table 20: Relevance of modules from layer APP: Applications

ID	Module	Target Object	Note
APP.1.1	Office Products	A115	
APP.1.2	Web Browser	A115	
APP.1.4	Mobile Applications (Apps)	S115, S211, S214, S218, S219	
APP.2.1	General Directory Service	A101	
APP.2.2	Active Directory	A101	
APP.2.3	Open LDAP	A101	
APP.3.1	Web Applications and Web Services	A105	
APP.3.2	Web Servers	A105	
APP.3.3	File Servers	A106	
APP.3.4	Samba	–	Not in use.
APP.3.6	DNS Servers	A103	
APP.4.2	SAP ERP System	A212	
APP.4.3	Relational Database Systems	A212, S109, S201, S217	
APP.4.4	Kubernetes	S108	
APP.4.6	SAP ABAP Programming	–	Not in use.
APP.5.2	Microsoft Exchange and Outlook	A114, A115	
APP.5.3	General E-Mail Clients and Servers	A114, A115	
APP.6	General Software	A101, A102, A103, A104, A105, A106, A107, A108, A109, A110, A111, A114, A115, A201, A202, A203, A204, A205, A206, A207, A208, A209, A210, A211, A212, A213, A214, A215, A216, A217, A218, A219, A301, A302, A303, A304, A220, A305, A221, A306	

### SYS: IT-Systems

Table 21: Relevance of the Modules from Layer SYS: IT Systems

ID	Module	Target Object	Note
SYS.1.1	General Server	S101, S102, S103, S104, S105, S106, S107, S108, S109, S111, S114, S115, S201, S202, S203, S204, S205, S206, S207, S208, S209, S210, S211, S212, S213, S214, S215, S216, S217, S218, S219, S301, S302, S303, S304, S220, S305, S221, S306	
SYS.1.2.2	Windows Server 2012	S101, S103, S104, S105, S106, S107, S108, S109, S111, S114, S201, S203, S205, S207, S209, S212, S217	

<i>ID</i>	<i>Module</i>	<i>Target Object</i>	<i>Note</i>
<b>SYS.1.3</b>	Linux and Unix Servers	S101, S103, S104, S105, S106, S107, S108, S109, S111, S114, S201, S203, S205, S207, S209, S212, S217	
<b>SYS.1.5</b>	Virtualisation	S107	
<b>SYS.1.6</b>	Containerisation	S108	
<b>SYS.1.7</b>	IBM Z	-	Not in use.
<b>SYS.1.8</b>	Storage Solutions	S102	
<b>SYS.2.1</b>	General Client	S115, S202, S204, S206, S208, S210, S211, S213, S214, S215, S216, S218, S219, S220	
<b>SYS.2.2.2</b>	Windows 8.1 Clients	S115, S202, S204, S206, S208, S210, S211, S213, S214, S215, S216, S218, S219, S220	
<b>SYS.2.2.3</b>	Windows 10 Clients	S115, S202, S204, S206, S208, S210, S211, S213, S214, S215, S216, S218, S219, S220	
<b>SYS.2.3</b>	Linux and Unix Clients	S115, S202, S204, S206, S208, S210, S211, S213, S214, S215, S216, S218, S219, S220	
<b>SYS.2.4</b>	macOS Clients	S115, S202, S204, S206, S208, S210, S211, S213, S214, S215, S216, S218, S219, S220	
<b>SYS.3.1</b>	Laptops	S115, S202, S204, S206, S208, S210, S211, S213, S214, S215, S216, S218, S219, S220	
<b>SYS.3.2.1</b>	General Smartphones and Tablets	S115, S202, S204, S206, S208, S210, S211, S213, S214, S215, S216, S218, S219, S220	
<b>SYS.3.2.3</b>	iOS (for Enterprise)	A113, S115, S211, S214, S218, S219	
<b>SYS.3.2.4</b>	Android	A113, S115, S211, S214, S218, S219	
<b>SYS.3.3</b>	Mobile Telephones	A113	
<b>SYS.4.1</b>	Printers, Copiers and All-in-One Devices	S112	
<b>SYS.4.3</b>	Embedded Systems	S301, S302, S304, S306, S221, S306	
<b>SYS.4.4</b>	General IoT Devices	-	Not in use
<b>SYS.4.5</b>	Removable Media	-	Not in use.

**IND: Industrial IT**

The modules from layer IND: Industrial IT are not in use.

**NET: Networks and Kommunikation**

Table 22: Relevance of the Modules from Layer NET: Networks and Communication

<i>ID</i>	<i>Module</i>	<i>Target Object</i>	<i>Note</i>
NET.1.1	Network Architecture and Design	NET	
NET.1.2	Network Management	NET	
NET.2.1	Wi-Fi Operation	NET	
NET.2.2	Wi-Fi Usage	NET	
NET.3.1	Routers and Switches	NET	
NET.3.2	Firewall	NET	
NET.3.3	VPN	NET	
NET.4.1	Telecommunications Systems	S110	
NET.4.2	VoIP	S110	

<i>ID</i>	<i>Module</i>	<i>Target Object</i>	<i>Note</i>
NET.4.3	Fax Machines and Fax Servers	—	Not in use.

## INF: Infrastructure

Table 23: Relevance of the modules from Layer INF: Infrastructure

<i>ID</i>	<i>Module</i>	<i>Target Object</i>	<i>Note</i>
INF.1	Generic Building	G01, G02, G03, G04, G05	
INF.2	Data Center and Server Room	R02	
INF.5	Room and Cabinet for Technical Infrastructure	—	Not in use.
INF.6	Storage Media Archives	—	Not in use.
INF.7	Office Workplace	R01	
INF.8	Working from Home	R01	
INF.10	Meeting, Event and Training Rooms	—	Not in use.
INF.11	Generic Vehicle	G06	
INF.12	Cabling	G01, G02, G03, G04, G05	
INF.13	Technical Facility Management (TFM)	—	Not in use.
INF.14	Building Automation and Control Systems (BACS)	—	Not in use.

Some targets specific to satellites cannot be sufficiently modelled with the existing modules of IT-Grundschutz. For such objects to which no module is assigned in the above table (e.g. the rooms “satellite” or “launch hall”), the user of the profile (usually using a risk analysis) should consider how or whether measures should be taken in addition to general modules (e.g. general building). For this purpose, requirements should be derived in accordance with the IT-Grundschutz methodology in order to achieve the desired level of protection.

## 9.3 Requirements for Satellites

This chapter presents some satellite-specific requirements that go beyond IT-Grundschutz. Their application can be evaluated mission-specific. These requirements relate to different aspects in the life cycle of the satellite, which is divided into the following categories:

- General Requirements
- Transport
- Launch facility
- In orbit phase
- Ground segment
- Decommissioning

### 9.3.1 General Requirements

General requirements are the requirements that are found in more than one sector.

### 9.3.1.1 Vulnerability scanning

Vulnerability scanning is used to detect and assess vulnerabilities. This should be done in all sectors. The type and extent of the scanning depends on the risk potential of the satellite and the mission.

Vulnerability scanning is the holistic consideration of possible security flaws, including infrastructure, personnel, supply chains and penetration testing.

### 9.3.1.2 Attack simulation

The simulation of (information security related) attacks (e.g. penetration testing & thread simulations) should be carried out during various segments, the integration, and the In Orbit phase taking into account the ground segment. In the case of particularly vulnerable missions, an attack simulation should also be considered on the check-out system, transport, launch setup, and the phase of the launch campaign.

### 9.3.1.3 Security Management

The satellite manufacturer/operator should request a security management or established security standards from its subcontractors and all participating companies and, if necessary, check compliance with the applicable rules and standards (via ISMS self-assessment or audit). In this context also the scope of the security standard should be examined in the relevant areas.

### 9.3.1.4 Conception and integration

During the design and integration phase, the satellite and the systems installed on the satellite should be protected to prohibit manipulation by external unauthorised access.

The EGSE and MGSE systems attached to the satellites for data exchange should be protected against external access according to the state of the art. This reduces the risk that the satellite could be damaged by external access.

Conceivable damage would be, among other things, the depth discharge of the batteries or the damage or destruction of the satellite by accessing the MGSE. For example, the satellite could be overturned by accessing the MGSE controllers, or existing explosive bolts could be triggered.

A secure network, high access controls and diligence during handover of work can significantly reduce the risk of damage.

## 9.3.2 Requirements for Transport

The transport from the integration hall to the test stations, between different facilities, to the start facility must be secured. The date, the route, the shipping company and the personnel involved should be kept as secret as possible. Staff should be instructed and obligated to maintain secrecy.

A separation of important elements of the satellite during transport should be examined, if this is still possible at this stage of integration. It should also be examined whether the selection of suitable tamper measures for individual components or for the transport container is necessary and useful.

## 9.3.3 Launch Facility

Compliance with security standards and requirements shall be ensured prior to awarding the contract of the satellite launch mission to the launch facility. Identified risks shall be presented in a transparent manner and shall be assessed in accordance with the applicable risk method.

---

## 9.3.4 Intersection in Orbit Phase and Ground Segment

The connection between ground segment and satellite should be particularly protected. For this purpose, measures should be taken to ensure the fulfilment of the protection objectives. Authentication and the use of secure cryptographic procedures are appropriate means to ensure the integrity of communication.

Contingency plans and security mechanisms to detect and fend off threats should be implemented in the system. Threats could include interference attempts, cyber attacks on satellites and/or ground segment, takeover, destruction, etc.

The use of intrusion detection, intrusion protection systems (IDS/IPS) as well as extensive recording and evaluation of log files increases the possibility of detecting attacks and anomalies. Extensive system monitoring and other security mechanisms should therefore be appropriately implemented in the systems.

If attacks or attempts to attack as well as other anomalies are detected, a change in communication encryption and other measures such as the change of crypto hardware and software, algorithms and keys must be examined. Depending on the severity and damage of the attack, additional emergency measures may become necessary, in addition to the reporting and information chains to be initiated.

The operating personnel should know about established procedures, and regular emergency exercises should continuously improve process security and the process itself.

### 9.3.4.1 In Orbit Phase

Modifications to hardware or even to software systems may be difficult to handle, so the implementation of important redundancy systems should be planned and the switch between the systems should be tested.

Where third-party information is processed directly for the satellite or in the satellite, appropriate integrity protection for that information should be implemented. External information is all information required and requested by external sources for processing, e.g. when using GPS time signals.

### 9.3.4.2 Ground Segment<sup>8</sup>

The ground segment as a direct connection to the satellite should be secured according to the state of the art. This includes infrastructure security and process knowledge by the personnel in the event of anomalies/emergency/attacks.

Therefore, contingency plans should exist in hard and soft copy. Regular training exercises to ensure process knowledge should be established. In case of system failures, if the satellite's construction allows, the "safe mode" should be applied, which must allow for appropriate responses to the failure or attack.

For example, in the event of loss of communication, secure and fast measures must be taken to ensure recovery. Once failures occurred extensive system tests must be carried out to ensure a trouble-free resumption of the operation.

## 9.3.5 Decommissioning

When the satellite has reached its end of mission and it can no longer be used due to exhausted resources or failed systems, it will be withdrawn. The size and altitude of the satellite usually decide on the type of decommissioning. The satellite can be placed in an orbit in order to burn up and be destroyed in the atmosphere. Alternatively, satellites are navigated into a graveyard orbit to remain there.

When the satellite burns up, all information is irretrievably destroyed. If this happens within a monitorable time window, the satellite should still be monitored until it burns up. If the satellite has burned up completely, no further action is required.

---

<sup>8</sup> The ground segment is not fully considered in this profile, but is limited to the interface with the satellite, see chapter 7.2. The requirements in this section also relate to this interface, accordingly.

If the satellite takes several years to burn up or if it is steered into the graveyard orbit, there is still information and possibly crypto material there. In order to exclude third-party access to the information, one should make sure that all information is irretrievably deleted prior to its disposal.

It is also possible to protect important devices using tamper measures, which are activated during the decommissioning process in order to destroy devices and information. If measures of this kind are planned, they must be executed without generating any space debris.

---

## 10 Residual Risk

Even when all requirements are implemented, no perfect security can be achieved. Both, the users of the IT-Grundschutz profile and the decision-makers must be aware of that fact. There remains always a residual risk. Cooperation with other organisations may potentially carry the risk of transferring confidential information to institutions without being able to apply appropriate security means. In spite of instructions and training, employees may also, intentionally or unconsciously, disclose such information to unauthorised persons. In addition, the purchase of third party services also poses a residual risk.

Targeted attacks on information technology of facilities of any kind are increasing. Known vulnerabilities in systems are being exploited faster. Timely fixes with adequate updates are not always possible. This applies in particular to systems where no special focus has been placed on information security during the development and operations process.

## 11 Application Notes

According to this IT-Grundschutz profile, the protection needs of each process should be evaluated mission-specific, as the protection needs of most satellite missions may exceed the category “Normal” and higher protection requirements should be applied. The profile only serves as a template and needs to be customised.



# 12 Checklist – Minimum requirements for IT security in space infrastructures

Table 24: Checklist – Minimum Requirements for IT Security in Space Infrastructures

	Element	Necessary action	Taken into account? Yes/No	Responsible	Measures to be initiated if necessary	Date
<b>1</b>	<b>Rooms/Buildings</b>					
1.1	Office	Security requirements determined?				
1.2	Server room	Security requirements determined?				
1.3	Satellite integration room/hall	Security requirements determined?				
1.4	Test room/hall	Security requirements determined?				
1.5	Transport containers	Security requirements determined?				
1.6	Launch hall	Security requirements determined?				
1.7	Satellite	Security requirements determined?				
1.8	Computing Center provider	Security requirements determined?				
1.9	Archive	Security requirements determined?				
<b>2</b>	<b>IT Infrastructure</b>					
2.1	General IT infrastructures	Security requirements determined?				
2.2	Special S/W (model, analytical instruments, etc.)	Security requirements determined?				
2.3	Hardware & Software Development	Security requirements determined?				
2.4	Test equipment	Security requirements determined?				
<b>3</b>	<b>Staff</b>					
3.1	Security instructions	Carried out?				
3.2	Security check (if necessary)	Carried out?				
3.3	Education/Training	Carried out?				
<b>4</b>	<b>Subcontractors (SC)</b>					

	Element	Necessary action	Taken into account? Yes/No	Responsible	Measures to be initiated if necessary	Date
4.1	Has the SC been checked whether it can meet the necessary security requirements?	Carried out?				
4.2	Do tenders and specifications include clear security instructions?	Carried out?				
4.3	Is compliance with security requirements checked regularly?	Carried out?				
4.4	Is the communication between the client and SC secured against third parties?					
4.5	external employees					
4.5.1	Security instructions	Carried out?				
4.5.2	Security check (if necessary)	Carried out?				
4.5.3	Education/Training	Carried out?				
4.5.4	Establishing an interface	Carried out?				
5.	<b>Integration and assembly of all system components including all necessary tests (AIT)</b>					
5.1	Access control	Security requirements determined?				
5.2	Inspection of personnel after completion of the work (daily if necessary)	Carried out?				
6	<b>Transport</b>					
6.1	Transport companies	Well known?				
6.2	Transport companies	Unknown?				
6.2.1	Security check performed?	Carried out?				
6.2.2	Security instructions	Carried out?				
6.2.3	Training if necessary	Carried out?				
6.3	Container	Sufficiently secured				
6.4	Accompanying staff	Necessary?				
6.5.1	If yes, security instructions	Carried out?				
6.5.2	If yes, training if necessary	Carried out?				
7	<b>Satellite operation</b>					

	Element	Necessary action	Taken into account? Yes/No	Responsible	Measures to be initiated if necessary	Date
7.1	Communication	Secured?				
7.2	Data transfer (payload)	Secured?				
7.3	Monitoring and Detection of hazards in Orbit	Available?				
7.3.1	Disruption of communication	Considered?				
7.3.2	Blinding	Considered?				
7.3.3	Deception	Considered?				
7.3.4	Hostile Takeover	Considered?				
7.3.5	Hostile approximation	Considered?				
7.3.6	System destruction (e.g. by kinetic, laser, RF weapons or Particle beam systems)	Considered?				
7.4	Emergency plans	Available?				
<b>8</b>	<b>Decommissioning</b>					
8.1	All components were destroyed during the crash	Status				
8.2	The satellite was sent to a safe cemetery orbit	Status				