German American Chambers of Commerce
Deutsch-Amerikanische Handelskammern

TeleTrusT Pioneers in IT security.
IT Security Association Germany

German-American IT Security Forum

IT Security Association Germany (TeleTrusT) in cooperation with GACC – German American Chamber of Commerce

San Francisco, 06.05.2024

Cybersecurity for Space

Jacques Kruse Brandao

TÜVIT & ALTER Technologies

TÜVIT

On the Mission to IT Security

Resilience for critical use cases in space

Jacques Kruse Brandao | TÜVIT | Cybersecurity for Space | 06.05.2024

Agenda

1. **Cybersecurity challenges related to Space – Threats to the Space Ecosystem**
2. **Expected requirements**
3. **Standards and Certification Schemes**
4. **The role of Assurance Levels**

Landscape of European Union Space Programmes

Essential use cases

Observation

Copernicus
Satellite Earth Observation and in-situ (non-space) data

Navigation

Galileo
Global satellite navigation and positioning system (GNSS)

EGNOS
Enhances GNSS for civil safety-critical applications, especially in aviation

Communication

GOVSATCOM
Secure communications for critical missions by the EU members

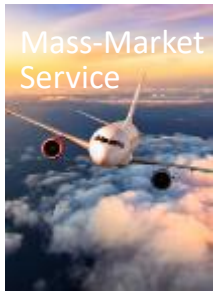
IRIS²
Enhanced high speed communication capacities to governmental users & businesses

SSA
Space situation detection and monitoring to protect space assets

3 Missions

5+1 Programmes

IRIS² missions & use cases:
Guarantee provision of secure SATCOM services



- Mobile/Fixed Broadband
- Satellite Trunking for B2B
- Satellite access for transportation
- …

- Government & institutions
- Satellite & terrestrial networks
- Banking & data centers
- …

ALTER | TÜVIT

In the context of the EU Space Strategy for Security and Defence

A lot of the things we do in space are crucial for the functioning of our society and economy. It keeps essential services running for public administrations, private companies and citizens.

Margrethe Vestager
Executive Vice-President for A Europe Fit for the Digital Age

TÜVIT

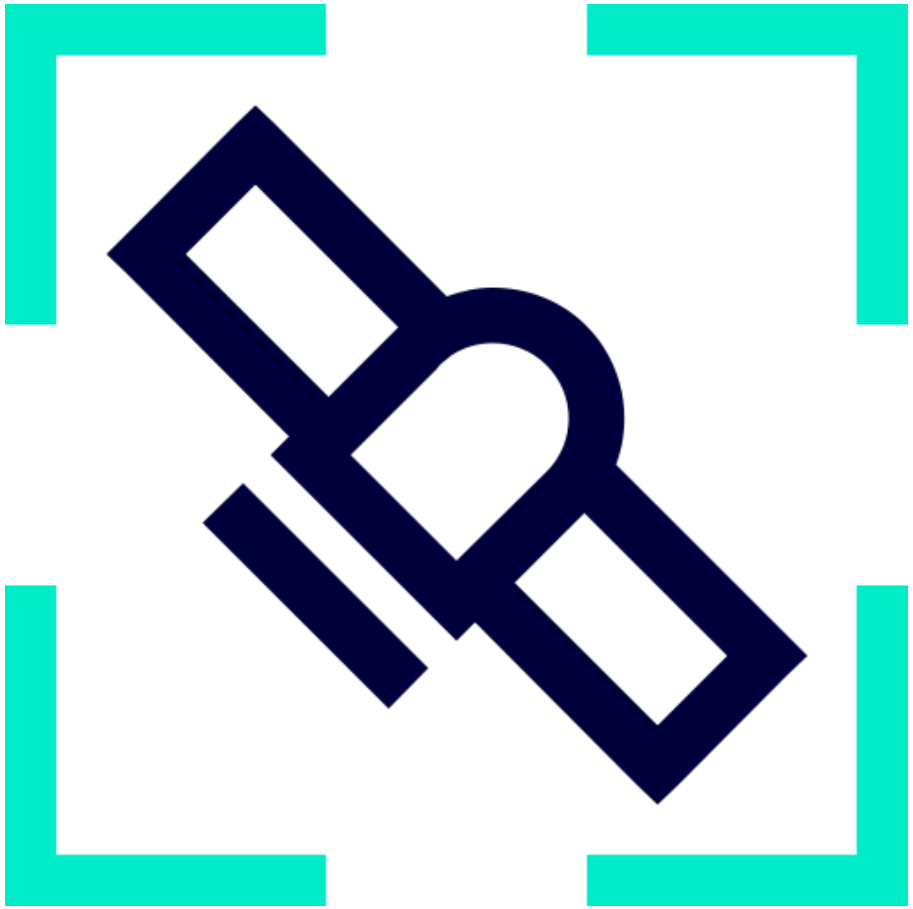
Landscape of main threats in space

Robotic arms

Kinetic non-kinetic SIGNIT

Electronic warfare

Kinetic anti-satellite (ASAT) weapons



Radiation

Space Debris

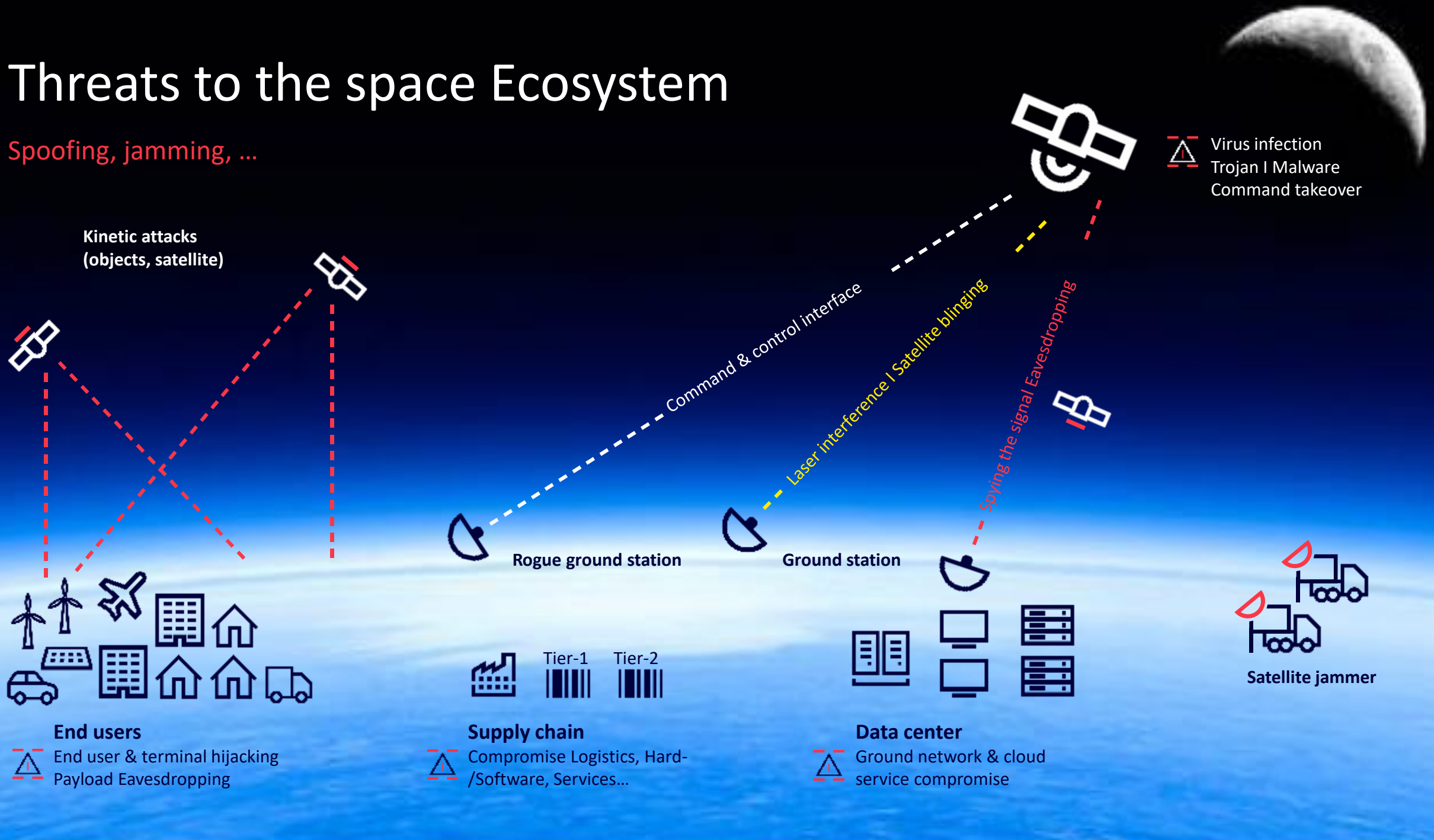
Cyber Attack sabotage

NON-kinetic laser or directed energy weapons

ALTER | TÜVIT

Threats to the space Ecosystem

Spoofing, jamming, …



Who is affected by cybersecurity threats?

3 Space ecosystem player:

Defense

Governments

Business

- Affecting our daily life on earth in various segments
- High-scale effects, therefore becoming critical infrastructure
- Dual-use nature of many space systems
- Military/Governments also use commercial products

Need for European harmonized cybersecurity requirements

Alignment between member states on risk classification and associated assurance levels

Who to take action:

- Ground stations
- Ground network operation center
- Data center
- Mission control center
- Components/sub-systems/device manufacturer
- Satellites manufacturer
- Terrestrial/non-terrestrial communication provider
- Managed security services provider
- Public key infrastructure/key management provider

+ Supply chain partner (tier 1-x, SBOM, HWBOM)

+ Secure SW development life cycle until end-of-fife

TÜVIT

Cyber attacks are old news down on earth

Awarness is increasing and regulation is also gaining momentum

ALTER | TÜVIT

One strategy for all

The European Cybersecurity Strategy

Authoritative bodies

ENISA
European Union Agency for Cybersecurity

National bodies of the EU Member States

European acts, directives & regulations

CSA
Cybersecurity Act
(EU) 2019/881

NIS 2
Network & Information Security Directive
(EU) 2022/2555

RCE
Resilience of Critical Entities Directive
(EU) 2022/2557

CRA
Cyber Resilience Act

GDPR
General Data Protection Regulation

eIDAS
Regulation on electronic identification and trust services
(EU) 910/2014

AI Act
Cybersecurity of Artificial Intelligence in the AI Act

National implementation of the directives

DE: > IT Sig. | BSI Law | TKG | EnWG | ...

European Cybersecurity Certification Framework

European certification schemes

EUCC
EUCS
EU5G

Harmonized Standards for all

TÜVIT

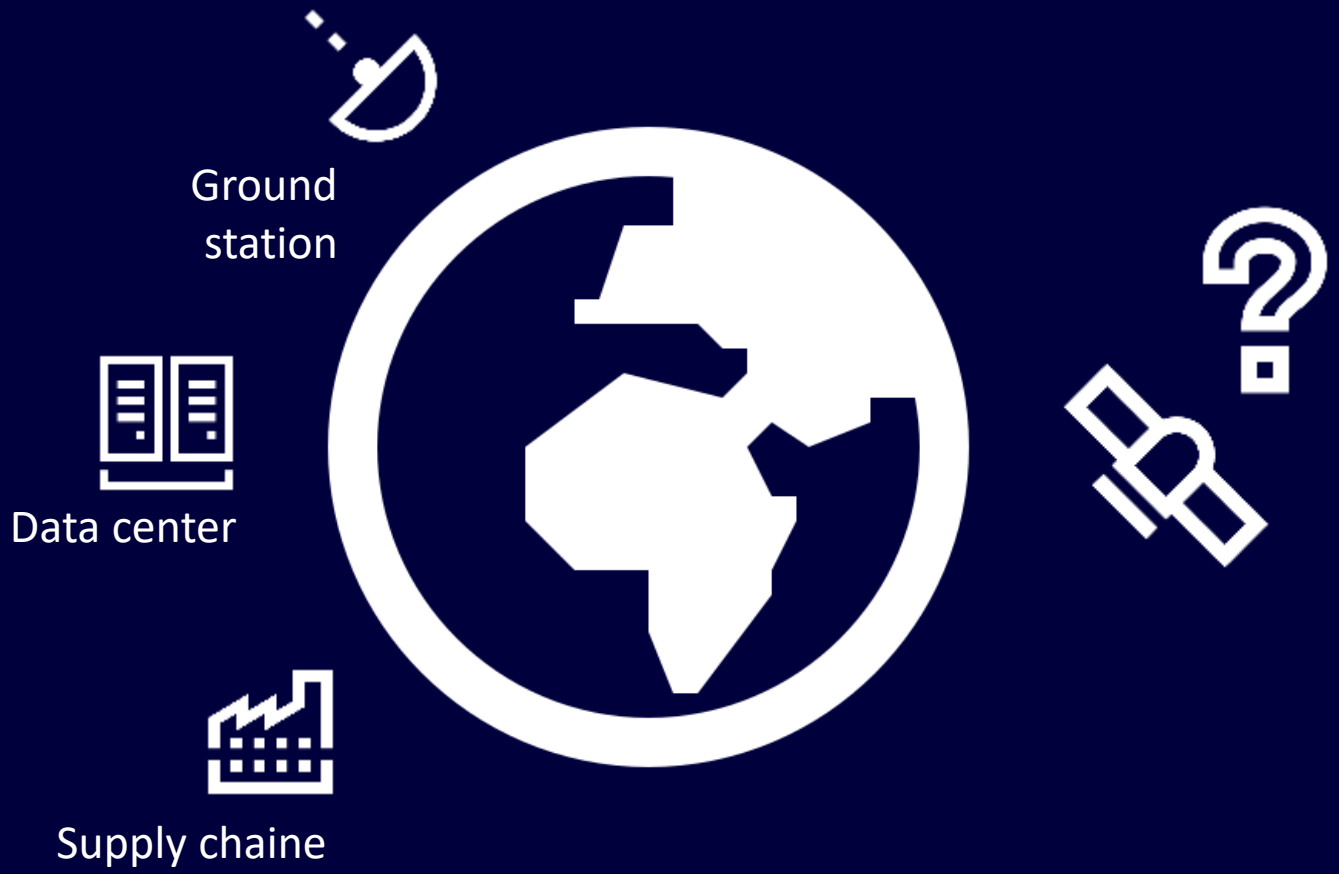
Space is not on the other side of the moon

EU regulation on earth is affecting space infrastructure operators and their suppliers

NIS 2
Network & Information Security Directive
(EU) 2022/2555

RCE
Resilience of Critical Entities Directive
(EU) 2022/2557

CRA
Cyber Resilience Act



TÜVIT

EU NIS 2 Directive

The Network and Information Security Directive

Purpose

EU NIS 2 is the European framework for operators of critical infrastructures and defines minimum cyber security standards in the EU.

Implementation Timeline

- NIS 1 Directive (in force since 06/2016)
- NIS 2 Directive (effective from 27.10.2024, replaces NIS 1)
- EU member states must transpose NIS 2 into national law by 17.10.2024.

Cybersecurity Requirements & Obligations

Risk management ++ Management accountability ++ Policies ++ Incident prevention, detection and response ++ Business continuity ++ Supply chain ++ Procurement ++ Effectiveness ++ Training ++ Cryptography ++ Personnel, access & asset management ++ Authentication & Communication

Impact to the space ecosystem > Cybersecurity

Essential Entities (x Sectors)	**Important Entities** (x Sectors)
Energy, transport, banking, healthcare, ... SPACE	Postal & courier services, chemicals, food, ... MANUFACTURING INDUSTRY

In addition - regardless of their size - there are other critical infrastructures and additional facilitiesfacilities that are categorised as "essential" by the state.

NIS2 AFFECTED!

Operators of ground-based infrastructure
owned, managed and operated by Member States or by private parties, that support the provision of space-based services

Manufacturing Industry for Space
of computer, electronic and optical products, electrical equipment, machinery and equipment

ALTER | TÜVIT

EU RCE Directive

Resilience of Critical Entities Directive

Purpose

The CER Directive requires Member States to identify critical facilities and strengthen their physical resilience to threats such as natural hazards, terrorist attacks or sabotage.

Implementation Timeline

- ECI Directive/2008/114/EC (in force since 2008)
- RCE Directive (EU 2022/2557) (in force since 01/2023; replaces ECI)
- According to the RCE Directive, Identification of affected operators based on national risk analyses by 17 Oct 2024.

!

Requirements & Obligations for physical resilience

Disaster preparedness ++ Physical access protection ++ Risk and crisis management procedures ++ Emergency response plans ++ Business continuity measures ++ Identification of alternative supply chains ++ Personnel security management ++ Awareness measures

Impact to the space ecosystem > Cyberresilience

Critical Entities (11 sectors)

Energy, transport, banking, healthcare, ... SPACE

In addition - regardless of their size - there are other critical infrastructures and additional facilitiesfacilities that are categorised as "essential" by the state.

NIS2 AFFECTED!

Operators of ground-based infrastructure
owned, managed and operated by Member States or by private parties, that support the pro-vision of space-based services

Manufacturing Industry for Space
of computer, electronic and optical products, electrical equipment, machinery and equipment

ALTER | TÜVIT

EU CRA

Cyber Resilience Act

COMING SOON!!

Purpose

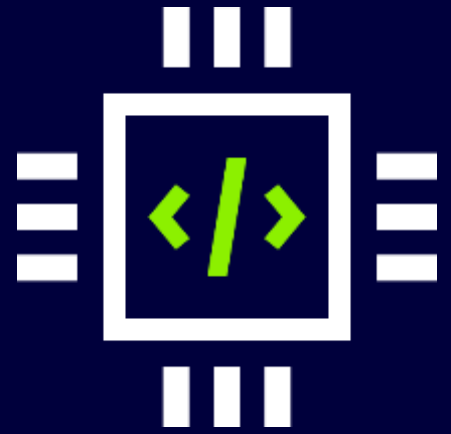
The CRA aims to safeguard consumers and businesses buying or using products or software with a digital component. The new EU cybersecurity rules ensure safer hardware and software.

Implementation Timeline

- Final adoption of the text is expected soon during Q-2024
- Majority of the obligations are subject to a 36-month transition period
- CRA requirements last for 5/10 years or until end-of-life

Requirements & Obligations

- 3rd party evaluation for high-risk products
- Secure software development life cycle (SDLC)
- Reporting about exploited vulnerabilities/incidents towards authorities and users
- Assurance that the product is free from exploitable vulnerabilities
- Management of Supply Chain risks, and many more ….



Product related essential requirements

- Security by default
- Protection from unauthorized access
- Confidentiality and integral data, command and programs
- Minimalization of data
- Availability of essential functions
- Minimize own negative impact on other devices
- Limit attack surface
- Reduce impact of an incident
- Record and monitor security televant events
- Enable adequate security updates

TÜVIT

Regulations for space

Existing legislation & standards and what‘s coming up?

TÜVIT

EUSL

EU Space Law

COMING SOON!!

Scope

- SAFETY
- RESILIENCE & CYBERSECURITY
- SUSTAINABILITY

Implementation Timeline

- Publication of the first draft version expected in June 2024
- Negotiation and trilogue with the new European Parliament only
- Final voting not before 2025

Requirements & Obligations

- DRAFT version not published yet
- Expected references to CRA, NIS2, CSA for assurance levels, GSPR, EU AI Act with associated requirements and obligations

ECSS Standards

European Cooperation for Space Standardization

Scope

- Safety related standards used by ESA for all tenders as a pre-requisite (https://ecss.nl/standards/active-standards/)
- "Cybersecurity" not mentioned so far

Standards related to e.g.

++ TM Synchronization and Channel Coding ++ TM Space Data Link protocol ++ AOS Space Data Link protocol ++ TC Synchronization and Channel Coding ++ TC Space Data Link Protocol ++ Criteria of assessments ++

Remember: 5 "Cybersecurity" related standards currently in work at ECSS, e.g. ECSS-Q-ST-80-10C DIR1 "Space product assurance - Security in space systems lifecycles"

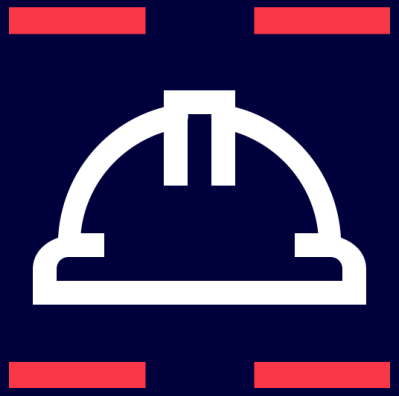
Additional Space Standards

- BSI TR-03184 Information Security for Space Systems
- NIST IR 8441_Hybrid Satellite Networks_Cybersecurity Framework (in prep)

Safety vs. Security

What is the difference?

Domain TÜV



SAFETY

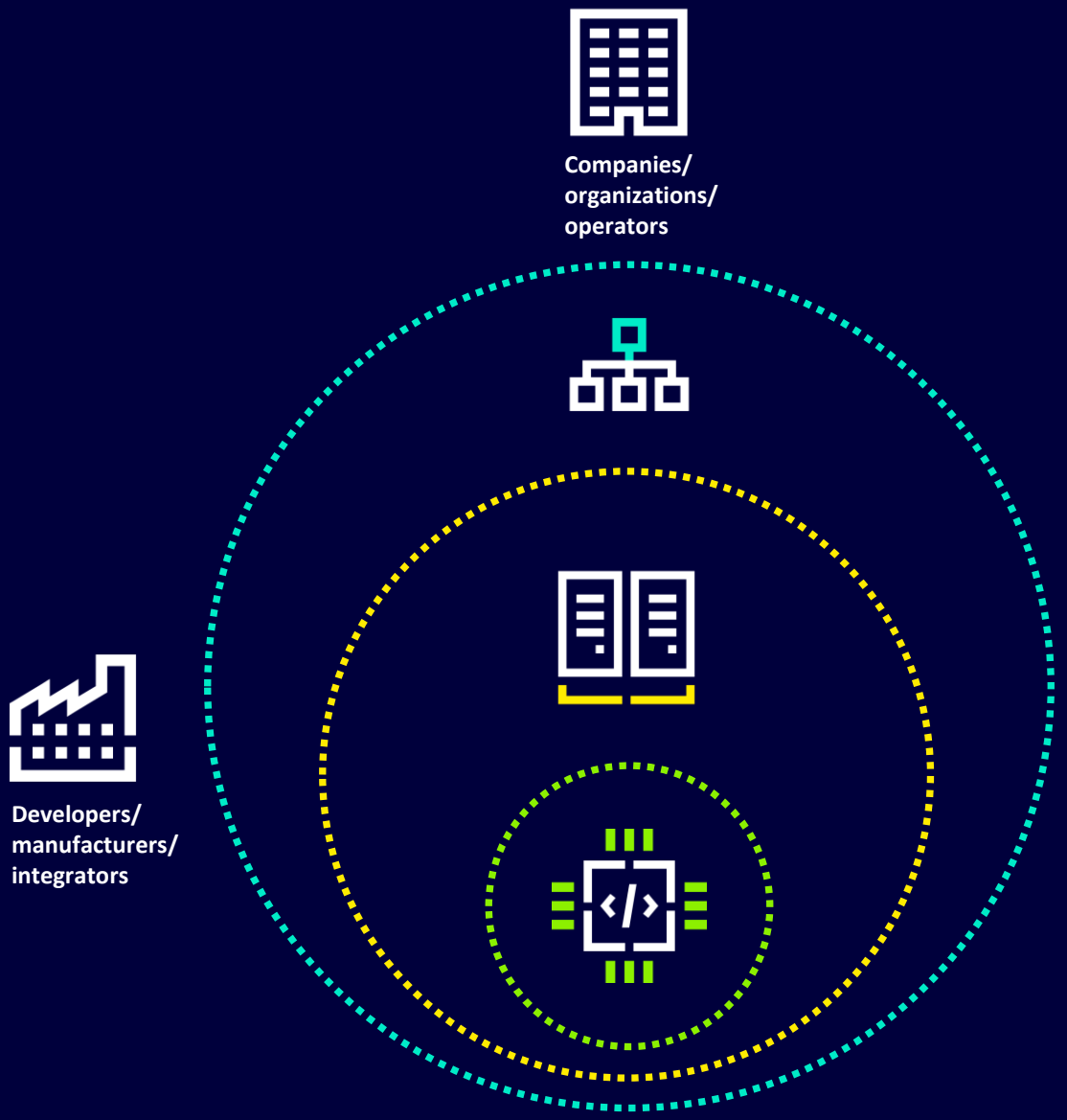
Prevention of danger to life and limb in the professional and private environment
„Intended Use“

Domain TÜVIT

SECURITY

Measures to protect IT systems, IT products and IT infrastructures to increase IT security
„Non-Intended Use“
+ sector specific requirements
related to space environment

ALTER | TÜVIT



We are a knowledge company

Resilience & Defence for companies and organizations

Strengthening the company's resilience by increasing the organization's adaptability and resistance as well as recovery measures in the event of an attack.

Information Security Management (ISO/ITGS) ++ Data Privacy (GDPR) ++
ICT-Project and Quality Management++ Process Optimization ++

Secure digital ICT system infrastructures & applications

Networked, highly available ICT infrastructures are the basis for a successful, digital company. We ensure security in design, implementation and operation.

Industrial Security (IEC) ++ System & Network Security (NIST) ++ Web App. & Mobile Security (OWASP) ++ Data Center (TSI) ++

Security at component level

IT security scaled millions of times over - we check the IT security of hardware and software components and ensure trust throughout the entire life cycle.

Product Evaluation (CC) ++ Validation Tests (FIPS140-2) ++ Security Tests/Assessments ++ Source Code Analysis (SW/Embedded) ++

ALTER | TÜVIT

Testing & certification approaches

CubeSat
→ EN 303645/BSZ/LINCE/CSPN/EN17640(FITCEM) oder EUCC
(Secure Access Control, Secure Key Storage, Secure Communication, Encrypted Data, Secure Onboarding Process, Secure FW Update, Secure SW Update, Secure SW Development Life Cycle, SBOM, HWBOM, Vulnerability Management, etc.)

Communication
→ EU5G

Secure Key Management / Certificate Management in PKI Infrastructure
-> Analog BSI TR-03129

Collision Avoidance System
→ EUCS

TÜVIT

Testing & certification approaches

for ground stations

Secure SW Development Lifecycle (SDLC) → EUCC, IEC 62443-4-1

Mission Control System → EUCS

Secure Onboarding Process

Collision Avoidance Services Tool → CRA/EUCC; SaaS → EUCS)

Secure Key Management / Certificate Management in PKI Infrastructure
-> Analog BSI TR-03129

Managed Security Services Tool → CRA/EUCC; SaaS → EUCS)

Physical Data Center Security → EN 50600 / TSI Standard

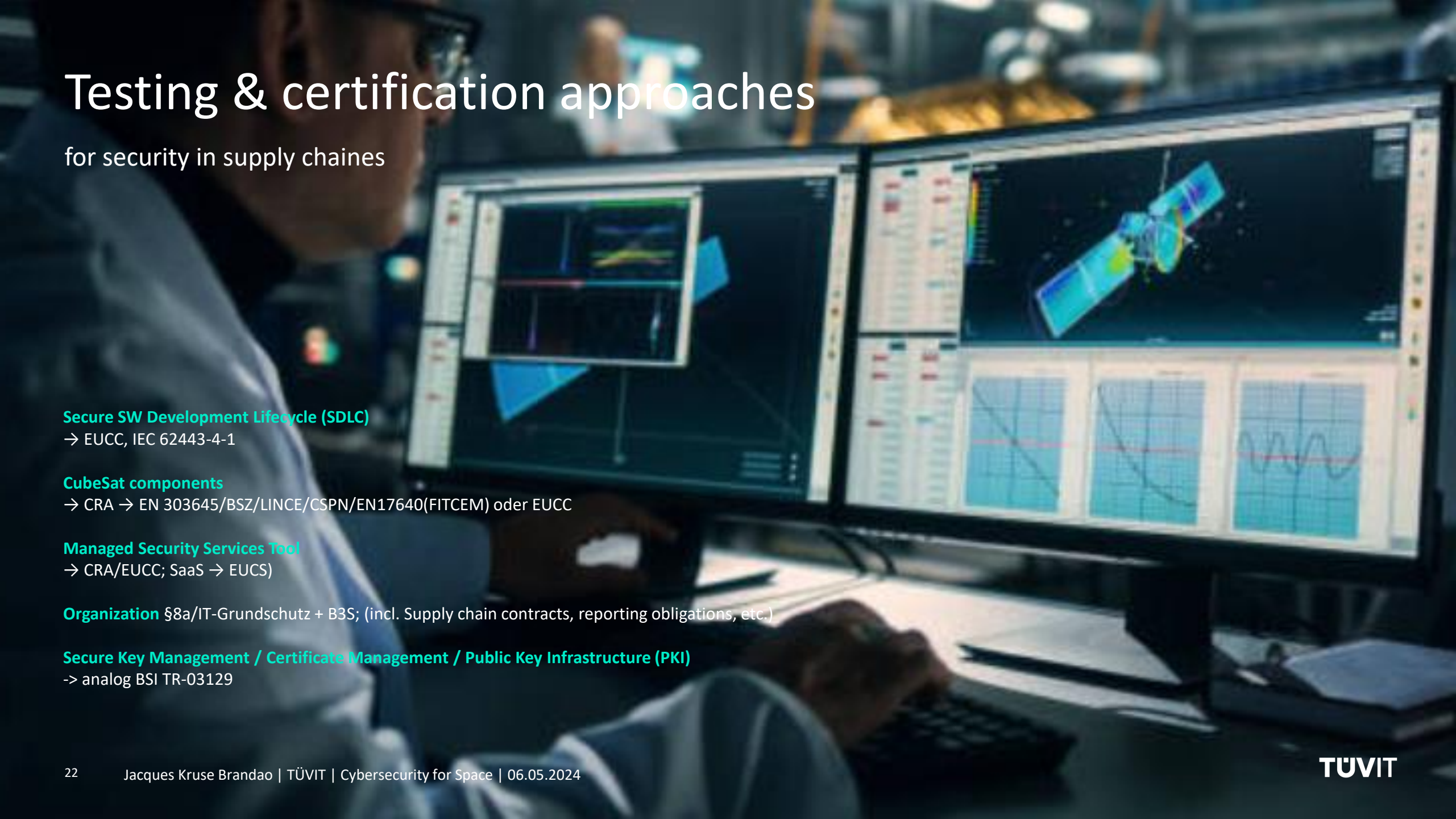
Organization → §8a/IT-Grundschutz+ (Supply chain contracts, reporting obligations, etc.)

Data Privacy → (External) Data Protection Officer

TÜVIT

Testing & certification approaches

for security in supply chaines



Secure SW Development Lifecycle (SDLC)
→ EUCC, IEC 62443-4-1

CubeSat components
→ CRA → EN 303645/BSZ/LINCE/CSPN/EN17640(FITCEM) oder EUCC

Managed Security Services Tool
→ CRA/EUCC; SaaS → EUCS)

Organization §8a/IT-Grundschutz + B3S; (incl. Supply chain contracts, reporting obligations, etc.)

Secure Key Management / Certificate Management / Public Key Infrastructure (PKI)
-> analog BSI TR-03129

TÜVIT

Space.
Secure space?

ALTER

- 38 years of experience in space and aeronautics
- leading engineering company which provides reliable and agile solutions
- …

IT SECURITY FOR SPACE

TÜVIT

- 25 years of proven track record in cybersecurity
- Worldwide recognized security lab with national/international accreditations
- …

About ALTER & TÜVIT

2 World Leading Experts

ALTER is a leading engineering company which provides reliable and agile solutions for many of the world‘s most innovative technologies, such as semiconductors, photonics, and electronic equipment.

TÜVIT helps companies to protect most valuable assets of the space ecosystem through independent security inspection and evaluation of products and services.

ALTER | TÜVIT

TÜVIT Competence Fields

Also offered for Space

ALTER | TÜVIT

TÜVIT

Let‘s stay in contact

Jacques Kruse Brandao

T.: +49 170 9209055

M.: j.krusebrandao@tuvit.de