IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

Ongoing Legislation / Standardization - Security

Legal Requirements for Manufacturers

IFA - IVSS Webinar
Dr. Andreas Schmid

Legal Requirements

- NIS 2 Directive
  Directive (EU) 2022/2555 of the European Parliament and the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148
- Cyber Security Act
  Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013
- Machinery Directive
  Directive 2006/42/EC of the European Parliament and the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC
- Machinery Regulation
  Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC
- Cyber Resilience Act
  Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (as of 12/20/2023)

More information and DGUV statements on directives and regulations at https://cert.dguv.de

Security Built-In: Safety – Functional Safety

Risks, arising from hazards when a control system fails

- systematic failures including software failures
- random hardware failures
- “simple” manipulations by operators

These hazards affect either people or the environment.

Standards already available

- EN ISO 13849
- IEC 61508
- IEC 62061

Security Built-In: Security – IT Security

Risks that emanate from people/organisations

- initially affect the machine control system/data
- can also be “safety-relevant”

Vulnerabilities that allow for example

- data theft
- “simple” attack attempts
- complex manipulations by intelligent attackers

Standards landscape just emerging

- IEC 62443

Security Built-In: Misconceptions

- **Why should someone attack us?**

Year of discovery	name	SPS for SPS programmed	Safety SPS for safety SPS programmed	Intention: Production stop	Intention: Destruction
2010	Stuxnet	X		X	(X)
2010	Blackenergy2	X			
2014	Havex/Backdoor.Oldrea	X			
2015	Industroyer/Crashoverride	X		X	
2017	Trisis/Triton/Hatman		X	X	X

Security Built-In: Misconceptions

- Why should someone attack us?
- ***Intentional/malicious acts:***
  → no protection possible!

Security Built-In: Obligations of Manufacturers

- current Machinery Directive does not explicitly require security!
- BUT:

1.2.1. Safety and reliability of control systems
Control systems must be designed and constructed in such a way as to prevent hazardous situations from arising. Above all, they must be designed and constructed in such a way that:
— they can withstand the intended operating stresses and external influences,
— a fault in the hardware or the software of the control system does not lead to hazardous situations,
— errors in the control system logic do not lead to hazardous situations,
— reasonably foreseeable human error during operation does not lead to hazardous situations.

Machinery Directive [Directive 2006/42/EC of the European Parliament and the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC]

→ **Implicit requirement?**

Security Built-In: Obligations of Manufacturers

EN ISO 12100 / Machinery Regulation

- Intended use
- Foreseeable misuse

ISO/TR 22100-4

- Intentional misuse is a criminal offense
- outside the scope of current safety legislation
- No reasonable misuse in the case of
  - Attacks on IT security
  - Impact on machine security if control/electrical parts are vulnerable
- **Machine manufacturers should still consider IT security aspects if IT threats can have an impact on the safety of the machine!**

Security Built-In: Obligations of Manufacturers

EU Machinery Regulation

Chapter III

Annex III: Essential Health and Safety Requirements

Article 20 (9)

1.1.9. Protection against corruption

1.2.1 Safety and reliability of control systems

Requirements according to Annex III, 1.1.9 & 1.2.1 fulfilled if a certification or declaration of conformity according to a harmonized standard under the Cyber Security Act is available

No dangerous situation due to communication with remote access device

adequate protection against intentional or unintentional corruption of hardware components that transmit signals or data relevant for connecting or accessing the software

Designation for conformity of critical software and data

Identification of the installed software required for safe operation

Proof of unauthorized and authorized interventions or changes to the software or configuration

Resistance to (un)intended external influences, including reasonably foreseeable malicious attempts by third parties

Storage of log data after intervention and the version of the safety software after commissioning or placing on the market for 5 years

Control systems with fully/partially self-evolved behavior: "artificial intelligence"

Action does not go beyond the defined scope of duties

Recording of safety-relevant data to ensure the safety function and storage for 1 year after recording

Possibility of correction at any time to maintain inherent safety

NIS Directive

- National strategy for cyber security
- Requirements for operators in the sectors
  - Energy
  - Transportation
  - Banking and financial market infrastructure
  - Healthcare infrastructure
  - Digital infrastructure
  - Drinking water supply
  - Digital service providers
- Single Point of Contact (SPOC)
- National competent authority (NCA)
- Computer security incident response team (CSIRT)

NIS Directive : IT-Sicherheitsgesetze 2.0

- National implementation of the NIS Directive
  → Securing critical infrastructures (KRITIS)
- BSI Act: Powers of the Federal Office for Information Security (BSI)

BSI Act*

§ 7a (1)

Das Bundesamt kann zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14, 14a, 17 oder 18 auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte und Systeme untersuchen. Es kann sich hierbei der Unterstützung Dritter bedienen, soweit berechtigte Interessen des Herstellers der betroffenen Produkte und Systeme dem nicht entgegenstehen

§ 8a (3)

Betreiber Kritischer Infrastrukturen haben die Erfüllung der Anforderungen nach den Absätzen 1 und 1a spätestens zwei Jahre nach dem in Absatz 1 genannten Zeitpunkt und anschließend alle zwei Jahre dem Bundesamt nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt die Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Das Bundesamt kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen.

§ 8b (4)

Betreiber Kritischer Infrastrukturen haben die folgenden Störungen unverzüglich über die Kontaktstelle an das Bundesamt zu melden:

1.Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben,

2.erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können.

Die Meldung muss Angaben zu der Störung, zu möglichen grenzübergreifenden Auswirkungen sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zur erbrachten kritischen Dienstleistung und zu den Auswirkungen der Störung auf diese Dienstleistung enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat.

* Act on the Federal Office for Information Security

NIS-2 Directive

- replaces the previous NIS Directive
  - published on 27.12.2022
  - in force since 16.01.2023
- Transposition into national law by the member states
  - within 21 months after entry into force
  - still outstanding in Germany!

NIS-2 Directive

Scope of application

- **Essential facilities**
- > 50 employees &
- > 10 million € annual turnover
- in critical sector
  - energy
  - transportation
  - Banking
  - Financial market infrastructure
  - Healthcare
  - Drinking Water
  - Wastewater infrastructure
  - Digital infrastructure
  - Management of ICT services
  - Public administration
  - Space

- **Important facilities**
  - in critical sector or **other critical sector**
    - Postal and courier services
    - Waste management
    - Production/manufacture of chemical substances
    - Production, processing Distribution of food
    - Manufacturing industry
    - Provider of digital services
    - research
  - No essential facility

Reporting of incidents

- Report any incident that has a significant impact:
  - serious operational disruption
  - financial loss
  - Adverse impact on others due to (im)material damage
- Early warning within 24 hours
- Update of the early warning through comprehensive reporting within 72 hours
- Detailed final report within 1 month

Company management

- Approval and monitoring of the prescribed risk management measures
- Participation in cyber security training to acquire sufficient knowledge and skills to recognize risks
- Personal liability if obligations are not met

Risk management

- Equal requirements for essential and critical facilities
- Risk analysis and strategies for information systems security
- Protocols for dealing with incidents
- Business continuity plans
- Measures for supply chain security
- Cybersecurity testing
- Audit procedures
- Cybersecurity training
- Strategies for access control
- Use of multi-factor authentication and encryption

Control measures

- Essential facilities
  - Ex-ante & ex-post supervision
  - Documentation of measures taken
  - On-site audit
- Key facilities
  - Ex-post supervision
  - Investigations only in case of indications of violations
- Warnings & instructions
  - Fine:
    - Significant institution:
    - €10 million or 2% of annual turnover
    - important facilities:
    - €7 million or 1.4%of annual turnover
  - Personal liability of company management for compliance with cyber risk management

Cyber Security Act

Strengthening the European Union Agency for Cybersecurity **ENISA** to improve **coordination and cooperation** on cybersecurity between **EU Member States** and **EU institutions, agencies and bodies**

Creating an EU **cybersecurity certification framework** that will enable the development of tailored certification schemes for specific categories of **ICT products, processes and services**.

Companies can have their products, processes and services **certified only once** and receive certificates **valid throughout the EU**.

Cyber Security Act: ENISA

Improving the EU's response capability by:

- Organizing cyber security exercises
- Improving the exchange of information between EU member states via the Computer Security Incident Response Team (CSIRT) network

Supporting the Commission and Member States in the implementation of the NIS Directive

Supporting member states to improve expertise, e.g. in preventing and responding to incidents

Establishing and maintaining the EU cybersecurity certification framework

Cyber Security Act: Certification of Cyber Security

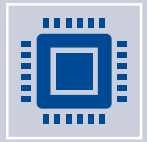
Certification strengthens confidence in the safety of products and services

ENISA & national experts develop certification framework

rules	standards	technical requirements

Certification is currently voluntary (unless future EU regulations require certification)

Cyber Resilience Act



Ensure that products with digital elements placed on the EU market have fewer vulnerabilities from the outset and that manufacturers remain responsible for cybersecurity throughout the lifecycle of their products;

greater transparency regarding the security of hardware and software products

greater protection for business users and consumers

Cyber Resilience Act: Obligations of Manufacturers § 10

- **(1)** The device shall comply with the essential requirements set out in Annex I, Section 1.
- **(2)** Carry out a cybersecurity risk assessment and take the results into account during planning, design, development, production, delivery and maintenance
- **(2a)** Document and update the cybersecurity assessment during the support period; Indication of the implementation of the requirements from Annex I, Part I (1) and (3) and Annex I Part II
- **(5)** All cybersecurity risks, including vulnerabilities, of which the manufacturer becomes aware must be documented systematically and appropriately for the risks.
- **(6)** During the support period, vulnerabilities in the product and components shall be effectively addressed in accordance with Section 2 of Annex I; Determination of the support period, based on time of use, intended use or comparison with similar products
- **(10)** Preparation of clear and comprehensible instructions for use for users and market surveillance authorities in ectropic form or on paper; Retention for at least 10 years or support period/product lifetime
- **(12)** The manufacturer must provide safety updates at least during the support period.

Cyber Resilience Act: Essential Requirements (Annex I, Section I)

(1) Appropriate level of cyber security

(2) Based on risk analysis according to §10 (2)

- Provision on the market without known vulnerabilities
- Delivery with standard configuration and possibility to reset to this configuration
- except for special agreements between manufacturer and business user for custom-made products
- Protection against unauthorized access and report on possible unauthorized access
- Confidentiality of stored, transmitted personal data
- Protection of stored, transmitted data, commands, programs against unauthorized manipulation
- The smallest possible attack surface, even with external interfaces
- Minimizing the negative impact of the product or connected devices on the availability of third-party services
- Reducing the impact of an incident
- Availability of essential functions including defense against overload attacks on servers (denial of service)
- Provision of security-related information (access to and changes to data, services, functions)
- Ability to securely and easily delete data and settings and ensure secure transfer to other devices if necessary

Cyber Resilience Act: Vulnerability Assessment (Annex I, Section II)

- **(1) Software Bill of Materials[1]**
  (SBOM)
  - machine-readable
  - frequently used format
  - Top-level dependencies

[1] BSI TR 03183-2:Software Bill of Materials

Cyber Resilience Act: Vulnerability Assessment (Annex I, Section II)

- **(1) Software Bill of Materials[1]** (SBOM)
  - machine-readable
  - frequently used format
  - Top-level dependencies

An SBOM must contain

- Creator of the SBOM
- timestamp
- Creator of the component
- Component name
- Version of the component
- Dependencies on other components
- License
- Hash value executable component

Uniform format:

- Software Package Data Exchange (SPDX),
- Software Identification (SWID) tagging and
- OWASP CycloneDX.

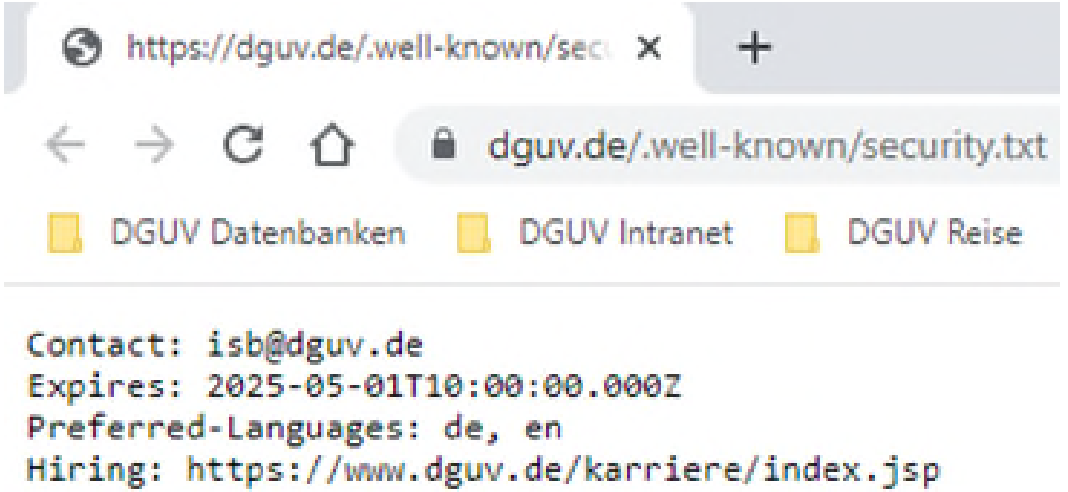
[1] BSI TR 03183-2:Software Bill of Materials

Cyber Resilience Act: Vulnerability Assessment (Annex I, Section II)

- (1) Software Bill of Materials (SBOM)
- **(6) Contact address**
  - Reporting vulnerabilities discovered in the product
    - Information to the right person(s)
      → sometimes very difficult!

Cyber Resilience Act: Vulnerability Assessment (Annex I, Section II)

- (1) Software Bill of Materials (SBOM)
- **(6) Contact address**
  - Reporting vulnerabilities discovered in the product
  - Solution: **security.txt**[1,2]
    - free of charge
    - RFC 9116
    - mandatory information:
      - Contact
      - expiration date



[1] https://securitytxt.org
[2] https://cert.dguv.de

Cyber Resilience Act: Vulnerability Assessment (Annex I, Section II)

- (1) Software Bill of Materials (SBOM)
- (6) Contact address
- **(4) Security advisories**
  - Information about fixed vulnerabilities **as soon as update available**
  - Description of the vulnerability
    - Impact and severity
    - Information for users on remediation
  - **in justified cases:**
    - Publish only after users had the opportunity to patch

Cyber Resilience Act: Vulnerability Assessment (Annex I, Section II)

- (1) Software Bill of Materials (SBOM)
- (6) Kontaktadresse
- **(4) Security advisories**
  - Information about fixed vulnerabilities **as soon as update available**
  - Description of the vulnerability
    - Impact and severity
    - Information for users on remediation
  - **in justified cases:**
    - Publish only after users had the opportunity to patch

Manual inspection of safety instructions:

- High expenditure of time and personnel
- Different information channels:
- e-mail, RSS feed, (possibly protected) website
- No automation possible due to different file formats and structure

Common Security Advisory Framework (CSAF)[1]

- machine-readable
- based on JSON format
- Retrieval from manufacturer and comparison with own inventory database
- Tool for creating from the BSI: https://secvisogram.github.io/

[1] https://oasis-open.github.io/csaf-documentation/

Cyber Resilience Act: Conformity Assessment Procedures § 24 (2)

- **Important Products (§ 6, Annex III)**
  - **Class I**
    - Standalone and embedded browsers
    - Microprocessors with security-related functionalities
    - Operating systems
    - Smart home general purpose virtual assistants
    - Smart home products with security functionalities (security camera, baby monitoring)
    - Personal wearable products with health monitoring
    - Password/boot managers

  ➢ **Procedures with presumption of conformity according to § 18**

  ➢ Harmonized standards

  ➢ Scheme of the Cyber Security Act with at least level "medium"

  ➢ **No or only partial application:**

  ➢ EU-type examination procedure (Annex VI, B) + internal production control (Annex VI, C)

  ➢ Full quality assurance (Annex VI, H)

Cyber Resilience Act: Conformity Assessment Procedures § 24 (3)

- **Important Products (§ 6, Annex III)**
  - Class I
  - **Class II**
    - Hypervisors and container runtime systems
    - Tamper-resistant microprocessors
    - Tamper-resistant microcontrollers
    - Firewalls, intrusion detection and/or prevention systems

➢ EU-type examination procedure (Annex VI, B) + internal production control (Annex VI, C)

➢ Full quality assurance (Annex VI, H)

➢ Scheme of the Cyber Security Act with at least level "medium“ according to § 18 (10)

Cyber Resilience Act: Conformity Assessment Procedures § 24 (3a)

- Important Products (§ 6, Annex III)
- **Critical Products (§ 6a, Annex IIIa)**
  - Hardware devices with security boxes
  - Smart meter gateways
  - Smart cards or similar devices, including secure elements

  ➢ Scheme of the Cyber Security Act according to § 6a (1)

  ➢ **if not available:**

  ➢ EU-type examination procedure (Annex VI, B) + internal production control (Annex VI, C)

  ➢ Full quality assurance (Annex VI, H)

Cyber Resilience Act: Conformity Assessment Procedures § 24 (1)

- wichtige Produkte (§ 6, Anhang III)
- kritische Produkte (§ 6a, Anhang IIIa)
- **Standard category: all other products with digital elements**
  - Photo/text editing software
  - games
  - Hard drives

➢ Internal control (Anhang VI, A)

➢ EU-type examination procedure (Annex VI, B) + internal production control (Annex VI, C)

➢ Full quality assurance (Annex VI, H)

➢ **if available and applicable:** Scheme of the Cyber Security Act according to § 18 (10)

IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

Thank you very much for your attention.

Dr. Andreas Schmid

Research Officer

Accident Prevention: Digitalisation – Technologies

Tel.: +49 (0)30/13001-3552

E-Mail: andreas.schmid@dguv.de

https://cert.dguv.de

Institute for Occupational Safety and Health of the German Social Accident Insurance

Alte Heerstr. 111

53757 Sankt Augustin

Germany