KI-FACHKONFERENZ

Artificial Intelligence Act

Dr.-Ing. Eric MSP Veith, OFFIS – Institut für Informatik

Dr.-Ing. Mathias Uslar, OFFIS – Institut für Informatik

22.11.2021

Agenda „Workshop 6: Energietechnologie, intelligente Stromnetze“

	Was
15:15 – 15:35	Input: Einordnung & Bestehende Normen
15:35 – 15:55	Interaktive Arbeit an Leitfragen
15:55 – 16:00	Zusammenfassung durch WS Leitung

https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_de

Schlaglichter zur Einordnung von AI Act und KI-Normung

EU Level:
High Level Expert Group on AI: Ethikleitlinien für eine vertrauenswürdige KI (2018, 2019)

Weißbuch KI (2/2020)

Vorschlag für eine Verordnung zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz - AI Act - (4/2021)

Datenethik-Kommission der Bundesregierung (BMJV, BMI)
2019, Kritikalitätspyramide

Enquete-Kommission KI & Gesellschaftliche Verantwortung
2018-2020, Bundestag + Experten

KI Strategie der Bundesregierung (BMBF u.a.)
- Erste Version 2018, Zwischenbericht 2020 + Fortschreibung
- 12 Handlungsziele:
  Nr. 10 „Standards setzen“

Normungsroadmap KI (BMWi)
Version 1: 11/2020
Fortschreibung 2022 ff
Energie offen bisher

Innovationspolitische Initiativen
- SINTEG (BMWi)
- Realllabore
- SMGW und IMSys – Gesetz zur Digitalisierung der Energiewende

AI Act: Zusammenfassung

1. Alles was dem Prinzip einer menschenzentrierten KI widerspricht (***human-in-command approach)*** ist verboten (**Artikel 5**). Ausnahme: zur Strafverfolgung und Gefahrenabwehr
2. Alles was schon heute Harmonisierungsrechtsvorschriften der Union unterliegt **und** einer Konformitätsbewertung unterzogen werden muss (CE), ist eine Hochrisiko-Anwendung (**Artikel 6**).
3. Alle in **Anhang III** aufgeführten Anwendungsbereiche, gelten zusätzlich als Hochrisiko-Anwendungen.
    a. Wenn Hochrisiko-Anwendung, dann Pflichten entsprechend Anforderungen aus **Titel 2, Kap.2** erfüllen (etwa Datenqualität, Transparenz, menschliche Aufsicht, **Kap. 3**), technische Dokumentation (**Anhang IV**) , automatisch erzeugten Protokolle, Konformitätsbewertungsverfahren (**Anhang V**), Registrierungspflichten, CE-Kennzeichnung.
    b. Registrierung in EU-Datenbank (**Art. 51**) und Kooperation mit nationalen Aufsichtsbehörden.
    c. Strafzahlungen bei Verstoß gegen Verbot, Anforderungen und Pflichten, Falschangaben (**Art. 71**).
4. Besondere Transparenzpflichten (**Art. 52**) für die Interaktion von KI-Systemen mit natürlichen Personen.
5. Verhaltenskodizes (**Art. 69**), mit denen erreicht werden soll, dass die in **Titel III Kapitel 2** genannten Anforderungen auf KI-Systeme Anwendung finden, die kein hohes Risiko bergen **und** mit denen erreicht werden soll, dass KI-Systeme freiwillig weitere Anforderungen erfüllen.
6. Einrichtung eines Europäischen Ausschusses für Künstliche Intelligenz (**Titel VI, Kap. 1**)
7. Umsetzung durch nationale Aufsichtsbehörden und notifizierende Behörden (**Titel VI, Kap 2**).

New rules for providers of high-risk AI systems

Step 1

A high-risk AI system is developed

Step 2

It needs to undergo the conformity assessment and comply with AI requirements
For some systems a notified body is involved

Step 3

Registration of stand-alone AI systems in an EU database

Step 4

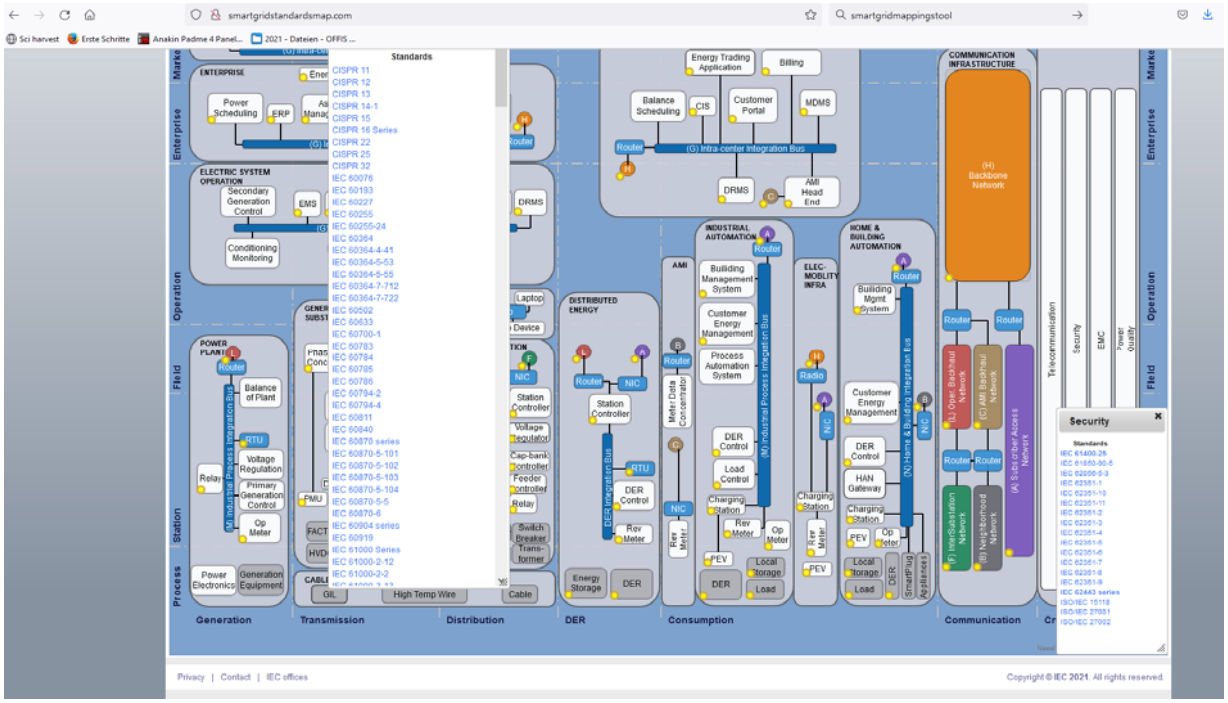
A declaration of conformity needs to be signed and the AI system should bear the CE marking. The system can be placed on the market

If substantial changes happen in the AI system's lifecycle, go back to Step 2

KRITIS – Kritische Infrastrukturen

- Kritische Infrastrukturen sind Anlagen, Systeme oder ein Teil davon, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind und deren Störung oder Zerstörung erhebliche Auswirkungen hätte, da ihre Funktionen nicht aufrechterhalten werden könnten

IEC Sicht auf das Problem

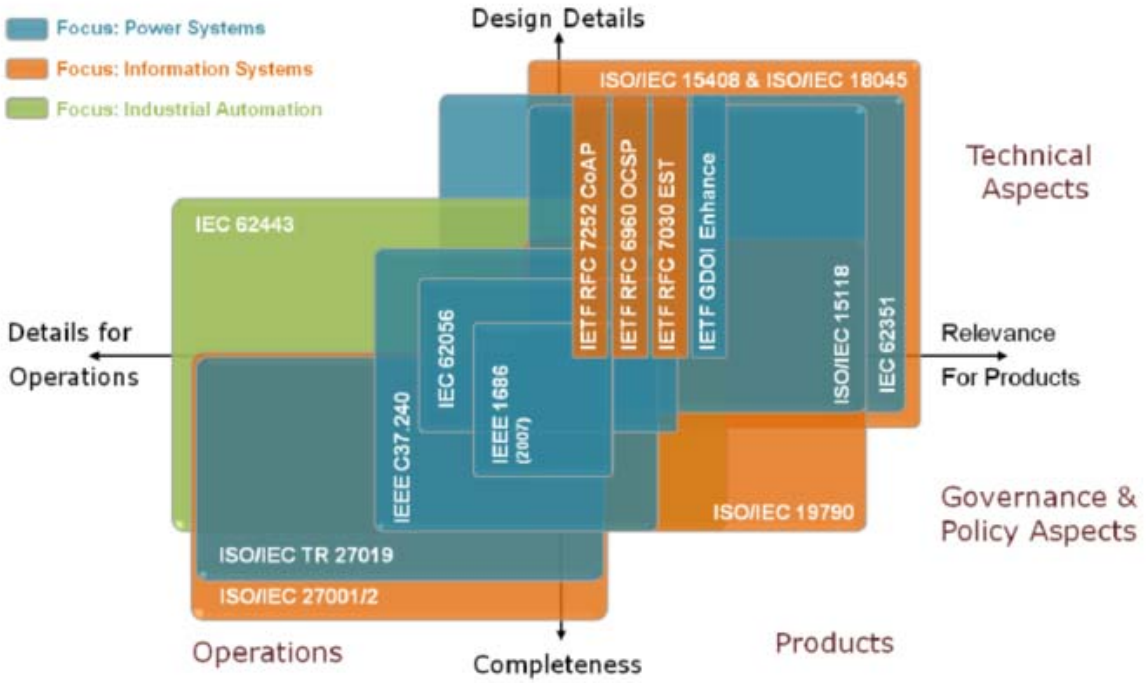


Security

Standards

IEC 61400-25
IEC 61850-90-5
IEC 62056-5-3
IEC 62351-1
IEC 62351-10
IEC 62351-11
IEC 62351-2
IEC 62351-3
IEC 62351-4
IEC 62351-5
IEC 62351-6
IEC 62351-7
IEC 62351-8
IEC 62351-9
IEC 62443 series
ISO/IEC 15118
ISO/IEC 27001
ISO/IEC 27002

IT Sicherheit Normungsroadmap

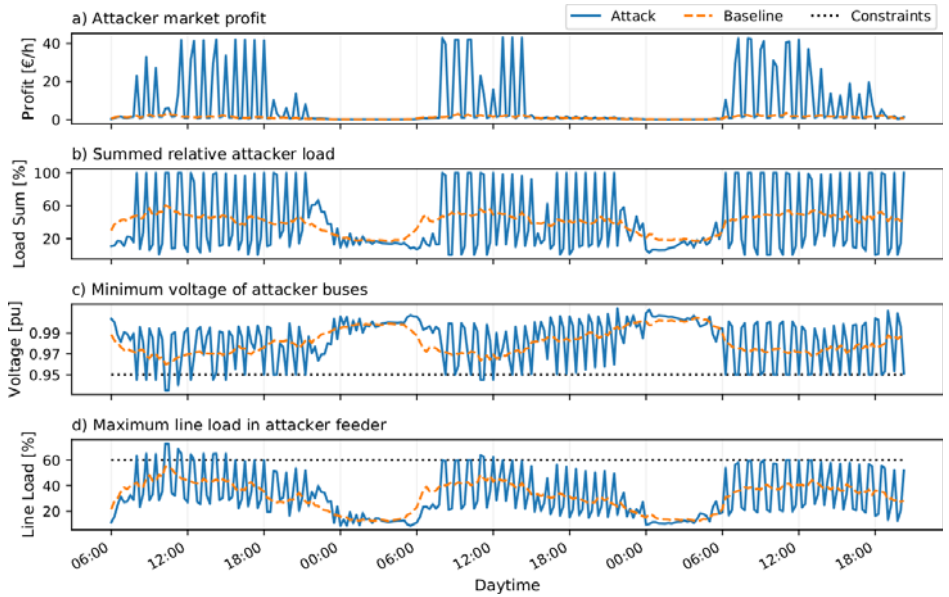


IT-Sicherheit Normungsroadmap II

Requirement standards (beschreiben "Was" gesichert werden muss):

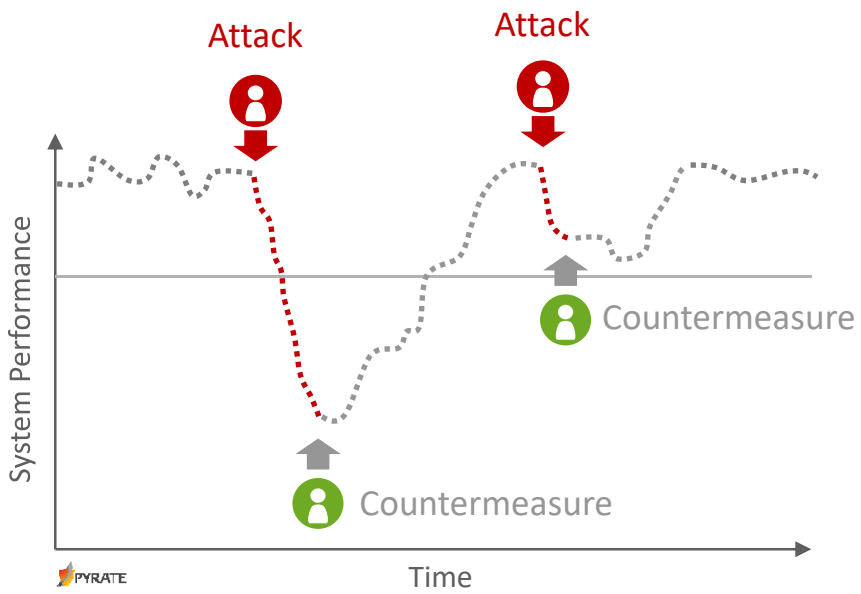
- ISO/IEC 15408 Information technology — Security techniques — Evaluation Criteria for IT 361 security
- ISO/IEC 18045 Information technology — Security techniques — Methodology for IT Security 363 Evaluation
- ISO/IEC 19790 Information technology — Security techniques — Security requirements for cryptographic modules
- ISO/IEC TR 27019 Information technology - Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
- IEC 62443-2-4 Security for industrial automation and control systems - Network and system security - Part 2-4: Requirements for Industrial Automation Control Systems (IACS) solution suppliers
- IEC 62443-3-3 Security for industrial automation and control systems, Part 3-3: System security requirements and security levels
- IEC 62443-4-2 Security for industrial automation and control systems, Part 4-2: Technical Security Requirements for IACS Components
- IEC 62443-2-1 Security for industrial automation and control systems - Network and system security - Part 2-1: Industrial automation and control system security management system
- IEEE 1686 Substation Intelligent Electronic Devices (IED) Cyber Security Capabilities
- IEEE C37.240 Cyber Security Requirements for Substation Automation, Protection and Control Systems

Moderne Energiemärkte ohne KI? Undenkbar.



- Die Weiterentwicklung des Energiesystems benötigt innovative Akteure
- Schwarmintelligenz, lernende Systeme: Notwendig für Multi-Purpose-Bewirtschaftung
- Lernende Systeme als autonome „Black Boxes“?
- Normierung als sicheres Rahmenwerk für autonome Systeme in KRITIS
- „Den neuronalen Netzen auf die Finger schauen“: eXplainable AI erlaubt erst Zertifizierung und die Anwendung von Normen

Hochautomatisierter Netzbetrieb



- Spannungshaltung, Netzzustandsschätzung, SCADA-Autopilot: Zukünftige Netze benötigen wegen ihrer Komplexität autonome lernende Systeme
- Verteidigungsstrategien gegen Cyber-Angriffe: „Immunsystem“ für KRITIS
- Autonome, lernende Systeme müssen kontrollier- und zertifizierbar sein
- Teststrategien basierend auf „Black Box Modelling“ zu unsicher (Adversarial Samples!)
- Aufbrechen der Black Box durch XAI

Zielstellung

- Ziel der Workshops ist die Erstellung einer Übersicht für die Themenkomplexe:
  - Welche Normen gibt es bereits in dem Bereich, die als mögliche harmonisierte Norm vorgeschlagen werden könnten?
  - Welche Normen befinden sich in dem Bereich derzeit im Entwicklungsprozess, die als mögliche harmonisierte Norm vorgeschlagen werden könnten?
  - Welche harmonisierten Normen müssen in diesem Bereich entwickelt werden, um die Anforderungen zukünftig erfüllbar zu machen?

Leitfragen (von Teilnehmenden auf Concept Board zu beantworten)

- Haben wir relevante Normen vergessen?
- Was sind die Haupt-Herausforderungen bei der Einführung von IT / KI im Energietechnik und KRITIS
- Wo würde Normung helfen?
- Welche Vorbehalte gibt es aktuell gegen die Normung?

➢ ***Link zum Concept Board wird gleich im Chat geteilt.***

Vielen Dank für Ihre Aufmerksamkeit!

Ihr Ansprechpartner:

Mathias USLAR
OFFIS – Institut für Informatik
Escherweg 2
26121 Oldenburg
uslar@offis.de

Ihr Ansprechpartner:

Eric MSP Veith
OFFIS – Institut für Informatik
Escherweg 2
26121 Oldenburg
veith@offis.de