

## Jahresbericht 2025

# TK IoT, Internet der Dinge und verwandte Technologien

Vorsitz: Vakant

National sind 12 Mitglieder, International ist die Schweiz mit 9 Experten im IEC / MT, WG und JWG Gremien beteiligt.

Im Berichtsjahr fand keine Sitzung statt; die Stellungnahmen zu den verschiedenen Dokumenten wurden auf elektronischem Weg eingeholt.

Im Jahr 2025 wurden 123 Dokumenten verteilt, deren 57 abzustimmen, 3 Kommentaren wurde abgegeben. 34 Normen wurden publiziert.

Die wichtigsten IEC-IoT-Aktivitäten im Jahr 2025 waren:

- Einführung neuer Cybersecurity-Normen für IoT-Geräte und Industrie
- Erweiterung der IEC-62443-Standards für Industrial IoT
- Entwicklung von Frameworks für IoT-Anwendungen (z. B. Kulturerbe, Gesundheitsmonitoring)
- Zusammenarbeit mit ISO und ITU zur globalen Standardisierung
- Fokus auf Sicherheit, Interoperabilität und Vertrauenswürdigkeit von IoT-Systemen

Neue IEC- und ISO/IEC-Normen für IoT (2025):

Cybersecurity-Standards für IoT-Geräte, ISO/IEC 27404:2025 – Cybersecurity Labelling Framework für Consumer IoT

- Einführung eines Cybersecurity-Kennzeichnungsrahmens für IoT-Produkte wie Smart-Home-Geräte, Wearables und vernetzte Haushaltsgeräte.
- Ziel: Erhöhung der Transparenz, Sicherheit und Vertrauenswürdigkeit für Verbraucher und Hersteller.
- Definiert:
  - Risiken und Bedrohungen
  - Rollen und Verantwortlichkeiten
  - Anforderungen an Zertifizierung und Kennzeichnung

Bedeutung: Grundlage für zukünftige Sicherheitslabels (ähnlich Energieeffizienzlabels), insbesondere relevant für regulatorische Anforderungen wie den EU Cyber Resilience Act.

#### IEC 62443-Erweiterung für Industrial IoT (IIoT)

#### IEC PAS 62443-1-6:2025 – Anwendung der IEC-62443-Serie auf IIoT

- Erweiterung der IEC-Cybersecurity-Normen auf industrielle IoT-Umgebungen.
- Bietet Leitlinien für:
  - Integration von IIoT in industrielle Automationssysteme
  - neue Kommunikationsarchitekturen
  - neue Sicherheitsanforderungen durch vernetzte industrielle Systeme

#### Bedeutung: Besonders wichtig für Branchen wie:

- Industrie 4.0
- Energieversorgung
- kritische Infrastruktur
- Smart Manufacturing

#### IoT-Framework für Kulturerbe-Management, ISO/IEC TR 30189-1:2025

- Framework zur Nutzung von IoT für:
  - Monitoring von Kulturgütern
  - Asset-Tracking
  - Zustandsüberwachung
- Definiert funktionale Komponenten und Informationsflüsse.

#### Beispiel-Use-Cases:

- Museumsobjekt-Monitoring
- Smart preservation systems
- intelligente Archivsysteme

#### IoT-Standards für Gesundheits- und Monitoring-Anwendungen, ISO/IEC TS 30180:2025

- Funktionale Anforderungen für IoT-Systeme zur Überwachung von Personen, z. B.:
  - Quarantäne-Monitoring
  - Gesundheits-Tracking
  - IoT-basierte Monitoring-Tags und Managementsysteme
- Enthält auch Anforderungen zum Schutz der Privatsphäre.

#### IEC-Aktivitäten im Bereich Industrial IoT und Cybersecurity, konzentrierte sich 2025 stark auf:

- Erweiterung der IEC-62443-Serie
- Anpassung der Standards an neue Technologien wie:
  - Industrial IoT
  - Edge-Computing
- vernetzte Produktionssysteme
- Unterstützung kritischer Infrastruktur und Industrie

Ziel:

- Schutz von:
  - Energieanlagen
  - Fertigungssystemen
  - Smart grids
  - Industrieautomation

Diese Normen helfen Unternehmen bei:

- Risikobewertung
- Systemdesign
- Compliance mit regulatorischen Anforderungen

Internationale Zusammenarbeit (IEC, ISO, ITU)

Die IEC arbeitete 2025 eng mit anderen globalen Standardisierungsorganisationen zusammen, insbesondere:

- International Organization for Standardization (ISO)
- International Telecommunication Union (ITU)

Beispiel:

- Gemeinsame Initiativen zur Entwicklung globaler Standards für digitale Technologien wie IoT und AI.
- Organisation internationaler Standard-Summits zur Förderung interoperabler und vertrauenswürdiger Systeme.

Fokusbereiche der IEC IoT-Aktivitäten 2025, die wichtigsten strategischen Schwerpunkte waren:

Bereich	IEC-Aktivität
Cybersecurity	IEC 62443 Erweiterungen und IoT-Security-Frameworks
Consumer IoT	Sicherheits-Labeling-Standards
Industrial IoT	Integration und Schutz industrieller Automationssysteme
Healthcare IoT	Monitoring- und Tracking-Standards
Smart Infrastructure IoT	IoT für kritische Systeme und Asset-Management
Interoperabilität	Zusammenarbeit mit ISO und ITU
Digitalisierung	Frameworks und Referenzarchitekturen

Rolle der IEC-Technischen Komitees im IoT-Bereich, wichtige Komitees:

- IEC TC 65 – Industrial automation und IIoT
- ISO/IEC JTC 1/SC 41 – IoT und Digital Twin
- ISO/IEC JTC 1/SC 27 – Cybersecurity für IoT

Diese entwickeln kontinuierlich neue Normen und aktualisieren bestehende.

Bei Fragen oder Anregungen steht das CES-Sekretariat jederzeit zur Verfügung ([CES@electrosuisse.ch](mailto:CES@electrosuisse.ch)).

(C.C.)