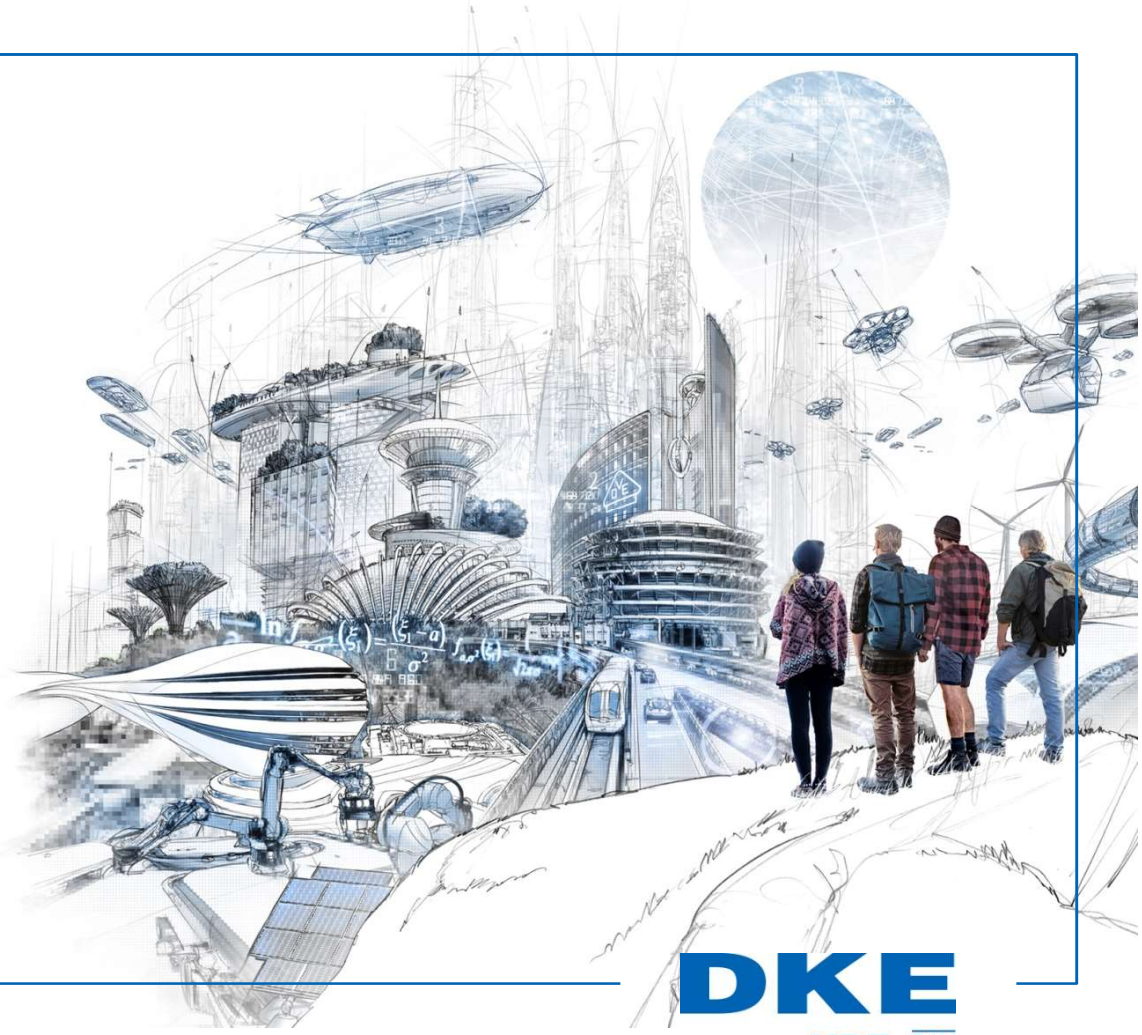
Verbindung zur Normung –
Stand der Arbeiten des
IEC TC 57 WG10 und WG15

Jochen Saßmannshausen

ABAC Workshop, 10.09.2020



DKE
VDE DIN

IEC TC 57 – Überblick

- **Entwicklung von Standards für die Steuerung und Automatisierung von Energiesystemen**
  - Automatisierung von Prozessen, Schutzfunktionen, Übertragung von Prozessdaten
  - Kommunikation mit Systemen wie SCADA und EMS
  - Security, System Management, Datenmodellierung, Konfiguration von Stationen, etc.

- **Standards, die von Arbeitsgruppen des IEC TC 57 entwickelt werden (Auswahl):**
  - IEC 60870 – Kommunikation zwischen SCADA-Systemen und Stationen
  - IEC 61850 – Automatisierung und Steuerung von Umspannwerken
  - IEC 61970 – API für EMS, spezifiziert das Common Information Model (CIM)
  - IEC 61850-7-410, -420 – Datenmodelle für Wasserkraftwerke und Distributed Energy Resources (DER)
  - IEC 62351 – Security, spezifiziert u.A. Profile für die Anwendung von TLS, eigene Protokolle für End-to-End-Security und Rollenbasierte Zugriffskontrolle (RBAC) für Smart Grid Anwendungen

IEC TC 57 WG 15 – Standards (Auswahl)

- **IEC 62351-3: Communication network and system security - Profiles including TCP/IP**
  - Veröffentlicht 2014, mit weiteren Amendments 2018 und 2020.
  - Spezifiziert die Anwendung von TLS für Protokolle, die auf TCP/IP basieren.
  - Sieht die Verwendung von TLS 1.2 vor.

- **IEC 62351-4: Profiles including MMS and derivatives**
  - Veröffentlicht 2018, mit einem Amendment 2020.
  - Spezifiziert ein eigenes Anwendungsprotokoll für End-to-End-Security.

- **Weitere Standards mit Fokus auf Kommunikationssicherheit:**
  - IEC 62351-6 (Security für IEC 61850), IEC 62351-5 (Security für IEC 60870-5-x)

IEC TC 57 WG 15 – Standards (Auswahl)

- **IEC 62351-8: Role-based access control for power system management**
  - Aktuelle Version wurde 2020 veröffentlicht
  - Fokus auf Rollenbasierter Zugriffskontrolle (RBAC) für verschiedene Anwendungen
  - Definiert ein Standardset von Rollen und assoziierten Berechtigungen
  - Definiert verschiedene Profile zur Darstellung von Access-Tokens (u.A. unter Verwendnung von X.509 Attributzertifikaten)
  - Definition eines XACML-basierten Formats zum Zwecke des Austauschs von Rollen und Berechtigungen.

- **IEC TR 62351-90-1: Guidelines for handling role-based access control in power systems**
  - Behandelt unter Anderem die Definition von eigenen Rollen.

IEC TC 57 WG 10

- **Innerhalb der IEC TG 57 WG 10 wurde die Task-Force „RBAC“ gebildet.**
  - Ziel: Entwicklung des Technischen Reports IEC TR 61850-90-19
  - Scope: Anwendung der rollenbasierten Zugriffskontrolle aus IEC 62351-8 auf IEC 61850.
  - Aktueller Stand: DC1 wurde an die nationalen Gremien verteilt und kommentiert.

- **Inhalt des DC1**
  - Sammlung von Use-Cases (u.A. RBAC Konfiguration, Operational States, RBAC für HMIs)
  - XACML-Profil um Permissions darzustellen (Kompatibel zu IEC 62351-8)
  - Schema, um Datenelemente zu referenzieren (unter Verwendung attributbasierter Konzepte)

RBAC für IEC 61850 – Use Cases

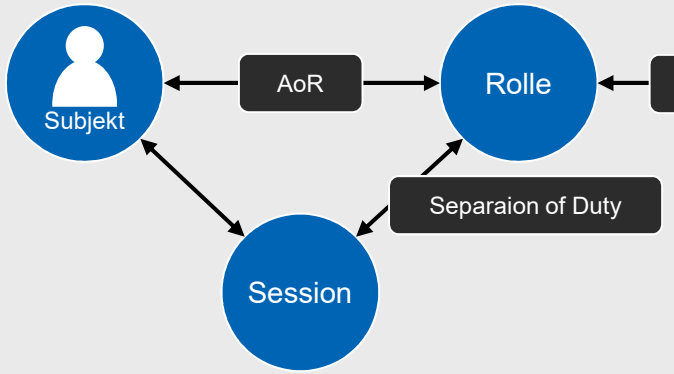
- **Area of Responsibility (AoR)**
  - Ist in IEC 62351-8 definiert und ist neben der Rolleninformation mit dem Subjekt assoziiert.
  - Bei dem Zugriff auf Datenobjekte muss geprüft werden, ob das Subjekt eine entsprechende *AoR* vorweisen kann.

- **Systemzustände**
  - Berechtigungen von Rollen können durch den Systemzustand beeinflusst werden.
  - Zustände einer Anlage – Local, Remote, Maintenance
  - Weitere Systemzustände: Green/Yellow/Red (Normal, Alert, Emergency)
  - Security Operational States

RBAC für IEC 61850 – Use Cases

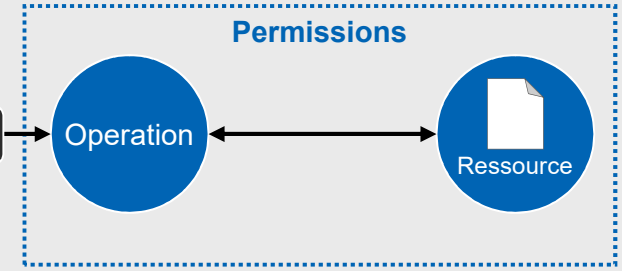
- **Zeitabhängige Zugriffsregeln**
  - Rechte, die nur zu bestimmten Zeiten gültig sind.
  - Subjekte haben bestimmte Zeitfenster, in denen sie ihre Rechte ausüben können.
- **Konfiguration der Security-Systeme**
  - Definition von Policies durch ein Security Configuration Tool.
  - Verteilen von Policies an die Systeme.
- **Dynamische Systemzustände**
  - Der Operational State (z.B. Green/Yellow/Red) muss ggf. von außen bereitgestellt werden.
  - In bestimmten Systemzuständen kann die Anlage von durch DSO/TSO kontrolliert werden.

RBAC mit ABAC-Ansätzen für IEC 61850



IEC 62351-8:

- Definition von Standardrollen und -Berechtigungen
- Definition einer *Area of Responsibility (AoR)*
- Verschiedene Profile, um die Rolleninformation an Subjekte zu binden (z.B. durch Attributzertifikate)



IEC TR 61850-90-19:

- Beschreibung der Operationen in Bezug auf das Abstract Communication Service Interface (ACSI) aus IEC 61850-7-2
- Beschreibung von Ressourcen durch Sets von Attributen
- Definition von zustandsabhängigen Role-Permission-Assignments

Vielen Dank für Ihre Aufmerksamkeit!