CIGRE Study committe D2

PROPOSAL FOR THE CREATION OF A NEW WORKING GROUP

WG D2.68

NAME OF THE CONVENOR
Soares Alan (UNITED STATES OF AMERICA)

TITLE
Enhancing Access Management Cybersecurity in Power Utilities

THE WG APPLIES TO DISTRIBUTION NETWORKS: YES

ENERGY TRANSITION
3 / Digitalization
5 / Grids and Flexibility

POTENTIAL BENEFIT OF WG WORK
1 / commercial, business, social, economic benefits
2 / potential interest from a wide range of stakeholders
3 / likely to contribute to new or revised industry standards
4 / state-of-the-art or innovative solutions or directions
5 / Guide or survey on techniques, or updates on past work or brochures

STRATEGIC DIRECTION
1 / The electrical power system of the future reinforcing the End-to-End nature of CIGRE: respond to speed of changes in the industry by preparing and disseminating state-ofthe-art technological advances
2 / Making the best use of the existing systems

SUSTAINABLE DEVELOPMENT GOAL
9 / Industry, innovation and infrastructure

BACKGROUND :
Utility companies are becoming more vulnerable to cyberattacks as a result of the power industry's digital transformation and the convergence of IT and OT (Operational Technology). The increasing complexity and frequency of cyber threats, as well as the need for robust access control mechanisms to protect critical infrastructure, make this topic highly relevant. This WG leverages standards such as NIST Cybersecurity Framework (CSF) and IEC 62443, cloud integration, and evolving threats.

PURPOSE / OBJECTIVE / BENEFIT OF THIS WORK :
- To provide a technical reference guide for access management best practices and new developments in the power sector, with emphasis on AI-driven solutions and cloud security.

- To offer suggestions for access control framework implementation, design, and policy that are specific to OT/ICS contexts, including ethical and regulatory considerations.

- To encourage uniformity and harmonization in utilities' cybersecurity governance, fostering collaboration between industry and government.

- To aid in strengthening resilience and lowering risk for vital infrastructure, while addressing the shortage of skilled professionals.

- To investigate the effects of regulatory and compliance requirements on utilities' access control procedures, such as NIST CSF, IEC 62443, NERC CIP, and ISO/IEC 27001.

SCOPE :

The WG will cover:

1. **Identity and Access Management (IAM):**
- Policy-Based Access Controls (PBAC) and Risk Adaptive Access Controls (RAdAC):

Explore the latest trends in IAM, including PBAC and RAdAC, which offer finer-grained access control and can dynamically adjust access permissions based on risk levels.

- Verifiable Credentials and Self-Sovereign Identity (SSI): Discuss the implementation of verifiable credentials and SSI to enhance security and streamline access management.

- Current Challenges: Legacy systems and vendor lock-in; Role separation between IT and OT environments; Access to substations, control centers, cloud platforms, and remote workstations; Interoperability issues, data privacy concerns, and shortage of skilled cybersecurity professionals.

- Include access management practices for PAC devices such as protection relays, IEDs, SCADA-connected controllers, and disturbance recording units. This includes remote engineering access, configuration management, identity lifecycle, auditability, and secure maintenance workflows. Consider interoperability with B5 (Protection and Automation) and B3 (Substations) domains.

2. **Advanced Cybersecurity Measures: -**
- Cloud Security Solutions: Examine the integration of cloud security solutions to protect critical infrastructure and data. Cloud computing offers scalable and flexible security measures that can adapt to evolving threats.

- Modern Access Management Architectures: Zero Trust Architecture (ZTA); Identity and Access Management (IAM); Privileged Access Management (PAM); Identity Federation and Single Sign-On (SSO).

3. **Standards and Frameworks:**
- NIST Cybersecurity Framework (CSF): Utilize the NIST CSF to guide the implementation of cybersecurity practices, focusing on risk management, incident response, and workforce management.

- Standards or reports such as NIST SP 800 - 63, NIST SP 800 - 162, and NIST SP 800 – 207.

- IEC 62443: Apply the IEC 62443 standards to ensure the security of industrial automation and control systems (IACS). These standards provide a comprehensive approach to cybersecurity, addressing both technical and organizational aspects.

- Mapping to NERC CIP, ISO/IEC 27001, and national regulations.

4. **Challenges and Opportunities:**
- Challenges: Identify the challenges faced in implementing advanced IAM and cybersecurity measures, such as interoperability issues, data privacy concerns, the shortage of skilled cybersecurity professionals, managing identities in hybrid environments, balancing security and availability, and human factors/insider threats.

- Opportunities: Highlight the opportunities presented by these technologies, including improved operational efficiency, enhanced security, better regulatory compliance.

5. **Use Cases and Best Practices:**
- Secure remote access.

Segmentation and least privilege enforcement; Identity lifecycle management.

6. **Prospects and Recommendations:**
- Future trends in access management; Policy guidelines; Recommendations for standardization and technology adoption.

Remarks:

- This Working Group will address the growing cybersecurity challenges associated with **access management in the power sector**, a subject that is increasingly critical due to the convergence of IT and OT systems, remote connectivity, and regulatory pressures on critical infrastructure, as identified in Brazil's 2025 Country Report.

- The proposed WG complements and expands upon previous work related to cybersecurity frameworks, notably those focusing on general security architectures (e.g., WG D2.46, WG D2.53), by taking a deep dive into access control mechanisms, including their implementation, integration, and monitoring in power utility environments, with strong emphasis on and cloud solutions.

- The WG will invite liaison members from SC B3 (Substations) and SC B5 (Protection and Automation) to contribute perspectives related to PACS engineering access and substation-specific access management requirements.

- The WG will also engage National Committees, Women in Energy (WiE), and Next Generation Network (NGN) participants to promote diverse technical perspectives and global applicability of outcomes.

- The outputs of this WG aim to support standardization efforts, contribute to regulatory compliance, and provide a practical guideline for secure access implementation, aligning with global cybersecurity frameworks such as IEC 62443, NERC CIP, and ISO/IEC 27001, while addressing ethical considerations and collaboration for enhanced resilience.

DELIVERABLES AND EVENTS

Deliverables Types
Annual progress and activity report to Study Committee
Future connections
Meeting
Technical Brochure and Executive Summary in Electra
Tutorial
Webinar

Time schedule

Q1	2026	Recruit members:
Q1	2026	Develop work plan
Q2	2027	Draft TB for SC Review
Q4	2027	Final TB
Q4	2028	Tutorial / Webinar

APPROVAL BY TECHNICAL COUNCIL CHAIRMAN:
Rannveig S. J. Loken
November 28th, 2025