CIGRE Study committe D2
PROPOSAL FOR THE CREATION OF A NEW WORKING GROUP

WG D2.69

NAME OF THE CONVENOR
MANYAPETSA Kgomotso (SOUTH AFRICA)

TITLE
Strategies for Secure Identity and Access Management in Power Operational Technology Environments

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 :
Identity and Access Management (IAM), centrally managed by Directory Services i.e. LDAP solutions, (Light-Weight Directory Access Protocol) is the critical perimeter for modern infrastructure security. Successful cyber-attacks often target privileged accounts and leverage compromised credentials, that make directory hardening against attacks such as Pass-the-Hash (PtH) mandatory.

Operational Technology (OT) environments impose unique constraints not addressed by standard IT deployment guidelines. These include demanding cyber-physical reliability, deterministic networks, low bandwidth/high latency links, harsh environmental conditions, and the pervasive presence of legacy devices. Vitally, core identity systems in these environments must maintain functionality without cloud dependency.

This Working Group is necessary to reconcile best practices for secure directory operation with OT requirements. The focus includes leveraging Read-Only Directory Replica to improve local authentication and manage security risk in physically less secure locations. Furthermore, the work will cover integration for devices such as IEDs/Controllers and RTUs using standardized authentication protocols (e.g., IEEE 802.1X/RADIUS/NPS).

This WG will focus on directory and identity infrastructure in OT environments. Broader access-management architectures, cloud identity, and policy frameworks (e.g. PBAC, RAdAC, SSI) will be addressed in WG D2.68

‘Enhancing Access Management and Cybersecurity in Power Utilities’.

PURPOSE / OBJECTIVE / BENEFIT OF THIS WORK :

The resulting Technical Brochure will provide utility engineers, administrators, technicians and security professionals with resilient architectural models and technical guidelines necessary to meet compliance mandates (e.g., IEC 62443, IEC 61850, IEC 62351) and embed Zero Trust security principles (Verify Explicitly, Least Privilege) within their core identity infrastructure.

SCOPE :

The WG addresses the following critical areas under stringent OT constraints (no cloud dependency, bandwidth limits, deterministic networks):

1. **Enterprise-level Directory Service Architecture Design and Security Boundaries**
Taking mainstream directory services (including but not limited to Microsoft AD, OpenLDAP, FreeIPA, Samba, etc.) as examples, the general design principles (such as security boundary division, management delegation, hierarchical management model) will be expounded, and the implementation differences and trade-offs of different solutions under OT constraints will be compared and analysed. This includes detailing design options and security patterns for trust relationships (e.g., one-way trusts, selective authentication) and identity integration between corporate IT and OT directory services. Strategies for separate forests and DMZ/‘shadow’ forests will be defined in alignment with IEC 62443 zones and conduits.

2. **Edge and Substation Deployments**
Guidance on deploying Read-Only Directory Replicas in remote or low-security sites to mitigate physical security risks. This includes configuring directory topology (sites, subnets, and replication links) to optimize authentication performance and control replication traffic over WAN links. Detailed procedures for configuring credential caching policies (such as restricting which user credentials are replicated to the edge) are included to manage the risks associated with compromised remote directories.

3. **Centralized Policy Management and System Hardening**
Best practices for utilizing centralized policies to enforce security across the OT environment. This covers expounding on general policy goals such as password policies, application control, session management, and peripheral device control. The WG will provide comparisons on how to achieve these goals on different platforms, such as Windows (via Group Policy Objects - GPOs) and Linux (via SSSD and custom policies). Specific attention will be given to deploying Fine-Grained Password Policies (FGPP), implementing whitelisting policies (e.g., WDAC/AppLocker), and aligning with IEC 62351-8 Role-Based Access Control (RBAC).

4. **Linux-based Directory Services and Integration**
Deployment architectures for open-source solutions such as OpenLDAP and FreeIPA, focusing on resilience (replication/caching) and integration with Linux-based servers and devices typically used in control systems. This includes strategies for bridging Linux clients with Windows-based directories (e.g., using Samba/Winbind) to ensure a unified identity strategy.

5. **Device Identity and Network Access Control (NAC)**
Defining identity provisioning for controllers, IEDs, RTUs, workstations, HMIs, relays and networking devices. Guidelines on achieving RBAC and centralized authentication using IEEE 802.1X integration with RADIUS/TACACS+/Network Policy Server (NPS) and Active Directory/openLDAP/LDAP, in alignment with IEC 62351-8 (Role-based access control for power system management). Illustrative identity and authentication flows for OT use cases (e.g. HMIs, IEDs, RTUs, remote access), including Kerberos/NTLM, LDAP/LDAPS, IEEE 802.1X/RADIUS/TACACS+ integration with directory services – with recommended secure patterns but without reproducing protocol specifications.

6. **Credential and Privileged Access Management (PAM)**
Strategies for mitigating shared account risks and securing privileged access across heterogeneous environments. This includes implementing automated local account password management to randomize and rotate privileged local credentials (e.g., Microsoft LAPS or scripted solutions for Linux). The scope covers enforcing hardened authentication policies for privileged identities to restrict credential caching and legacy protocols (e.g., Active Directory Protected Users group),. Furthermore, the WG will detail secure remote administration techniques designed to prevent credential exposure on target systems, such as Restricted Admin mode for RDP and SSH key management best practices including other remote access solutions.

7. **Resilience, Audit, and Compliance**
Ensuring high availability via redundant directory services (maintaining multiple directory servers or replicas per security zone is a best practice). Defining Disaster Recovery (DR) procedures (e.g., directory database restoration and replication convergence). Automating policy compliance checks using configuration management and auditing frameworks (such as OpenSCAP or scripting tools) and mapping architecture directly to standards: IEC 62443, IEC 61850, and Zero Trust principles.

The Working Group will produce a comprehensive technical guide and reference architectures for deploying secure, resilient, and non-cloud dependent Directory Services (Active Directory and Linux-based) tailored for OT environments (Power Plants, Substations, Control Centres). The work ensures robust Identity and Access Management (IAM) while meeting strict operational and compliance mandates.

DELIVERABLES AND EVENTS

Deliverables Types

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

Deliverables schedule

Meeting	Q2	2026	Detailed work plan development
Event	Q3	2026	Membership recruitment
Technical Brochure	Q1	2029	Draft TB for SC Review
Webinar	Q2	2029	Webinar
Tutorial	Q4	2029	Tutorial

Time schedule

Q1 2027
Publish an Electra article for non-specialists on this topic, to improve wider awareness in the CIGRE community on this topic

APPROVAL BY TECHNICAL COUNCIL CHAIRMAN:

Rannveig S. J. Loken
September 02nd, 2026