CIGRE Study committe D2

PROPOSAL FOR THE CREATION OF A NEW WORKING GROUP

WG D2.64

NAME OF THE CONVENOR
Chaoyang Chu (CHINA)

TITLE
Application of AI in Cybersecurity Defence of Power Systems

THE WG APPLIES TO DISTRIBUTION NETWORKS: YES

ENERGY TRANSITION
3 / Digitalization

POTENTIAL BENEFIT OF WG WORK
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
6 / work likely to contribute to improve safety

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

SUSTAINABLE DEVELOPMENT GOAL
9 / Industry, innovation and infrastructure

BACKGROUND :

In recent years, with the development of emerging technologies such as artificial intelligence, the Internet of Things, big data, and the continuous expansion of application scenarios, the digital transformation of the power industry has accelerated. By using emerging information technology, power enterprises can fully explore and utilize the data value throughout the entire life cycle of electricity, optimize their own decisions, and improve the operational efficiency of power generation, transmission, transformation, distribution, use, and dispatch, ultimately improving operating efficiency, resource utilization, and security.

At the same time, the current cyberspace security situation is becoming increasingly complex, and cyber warfare has become a new war situation. More and more cyber attacks are launched using AI technology, and the harm caused is becoming more serious. Intelligent network attacks have changed from passively using AI to bypass defences to actively using deep learning models as attack components, showing the features as large-scale, automated, and real-time. AI network attacks bring new security threats and challenges to the power industry.

Therefore, to follow the trend of technological development, in terms of cybersecurity defence, it is necessary to use AI technology and products to build a more three-dimensional, intelligent, and complete security defence system for the power information system, and to compete with AI network attack technology to provide an information security foundation for the construction of smart grids, and to achieve intelligent "security problem discovery, security status perception, and security policies execution".

This working group (WG) differs from the existing AI Applications and Technology in Power Industry Working Group (D2.52), which focused on the general AI topics in power industry. Instead, this WG targets a dedicated study on the AI applications in power cybersecurity, especially with vulnerability discovery, threat detection and automated response.

PURPOSE / OBJECTIVE / BENEFIT OF THIS WORK :

The purpose of the Working Group is to establish a reference document on the application of AI in power cybersecurity, achieving consensus on cutting-edge technologies among power enterprises (generation companies, power utilities, independent system operators, load aggregators, etc.), research institutions, academia as well as equipment and system vendors, promoting conceptual consistency and technology recognition and adoption, exploring and identifying practical application scenarios and key technologies, formulating recommended use cases, laying the foundation for large-scale implementation in power industry enterprises.

SCOPE :

The working group's job will cover the following aspects:

- **Development trend:** deep integration of AI technology and traditional power cybersecurity defence technology.
- **Application framework of AI in power cybersecurity defence:** collection and perception layer, data layer, analysis and decision layer, response and execution layer, visualization and monitoring layer, etc.
- **Key technologies:** intelligent cybersecurity defence technology at various levels such as access layer, system layer, network layer, application layer, and management layer.
- **Application scenarios and use cases:** vulnerability mining, network threat detection, cybersecurity situation awareness, cybersecurity operations & maintenance, personnel training and other scenarios.
- **Challenges:** Limitations of AI cybersecurity defence and the security of AI itself.
- **Prospect:** Future development trend of AI technology in the power cybersecurity defence.

DELIVERABLES AND EVENTS

Deliverables Types

Annual progress and activity report to Study Committee
Technical Brochure and Executive Summary in Electra
Tutorial

Deliverables schedule

Technical Brochure	Q2	2027	Final TB
Tutorial	Q4	2027	Tutorial

Time schedule

Q2	2025	Recruit members
Q4	2025	Develop final work plan
Q4	2026	Draft TB
Q2	2027	Final TB
Q4	2027	Tutorial

APPROVAL BY TECHNICAL COUNCIL CHAIRMAN:
Rannveig S. J. Loken
March 18th, 2025