CIGRE Study committe D2

PROPOSAL FOR THE CREATION OF A NEW WORKING GROUP

WG D2.63

NAME OF THE CONVENOR
Junho Hong Junho (UNITED STATES OF AMERICA)

TITLE
Inter-Control Center Communications Protocol (ICCP) Security and Resilience for Grid Reliability

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
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 :
The ICCP (Inter-Control Center Communications Protocol) (also referred to as Telecontrol Application Service Element 2 (TASE.2), as defined in IEC 60870-6-503:2014, IEC 60870-6-702:2014 and IEC 60870-6-802:2014) is fundamental for real-time telemetry and data exchange among utilities and Balancing Authorities (BAs) worldwide.

In increasingly interconnected power grids, ICCP enables utilities and operators to monitor and control the generation and transmission facilities essential for reliable grid operation. As power systems integrate a growing mix of distributed energy resources, safeguarding the resilience and security of ICCP systems is of paramount importance on a global scale.

Recent assessments highlight potential vulnerabilities within the ICCP infrastructure that could lead to single-point failures or common-mode disruptions, affecting critical grid telemetry. While ICCP is often supported by redundant systems and robust cybersecurity measures, evolving energy landscapes worldwide necessitate the exploration of alternative technologies and resilient data exchange pathways. Strengthening these systems is essential to maintaining global grid reliability and ensuring the capacity to address extreme operating conditions.

This proposed working group will address these challenges by evaluating the current ICCP infrastructure, exploring enhanced technologies and processes to increase resilience/security, and identifying alternative data exchange methods to sustain basic grid operations during ICCP disruptions. Additionally, the working group will develop approaches to maintaining core operations under minimal data availability and manual control, supporting grid operators in preserving reliable operations amid external threats and infrastructure vulnerabilities.

PURPOSE / OBJECTIVE / BENEFIT OF THIS WORK :

Purpose

The purpose of this working group is to develop methodologies to strengthen the resilience and security of the ICCP systems, which are critical for the reliable exchange of real-time telemetry and operational data across interconnected power grids internationally. This working group's objective is to ensure that ICCP infrastructure is robust against emerging cyber and operational threats, enabling uninterrupted grid monitoring and control in a dynamically evolving energy landscape.

Objective

1. Assess ICCP Infrastructure Resilience: Conduct a high-level assessment of existing ICCP systems under select failure scenarios, such as single-point failures and common-mode vulnerabilities, to identify primary resilience gaps.
2. Explore Alternative Technologies: Review and recommend a limited set of alternative data exchange methods that offer redundancy to ICCP, focusing on maintaining essential grid functions in case of partial ICCP outages.
3. Outline Minimal Operation Conditions: Develop necessary strategies for sustaining critical grid operations using minimal data and manual interventions, targeting a few key scenarios to maintain essential functions during ICCP disruptions.
4. Promote Core International Best Practices: Establish a concise set of best practices for securing ICCP systems to foster adaptable international standards and collaboration on shared resilience risks.

Benefit

1. Enhanced Grid Reliability and Resilience: Strengthening ICCP infrastructure will enhance reliable and resilient grid operations and ensure that utilities and grid operators can respond effectively to operational challenges without jeopardizing system stability.
2. Reduced Risk from Cyber and Operational Threats: By enhancing cybersecurity and integrating alternative technologies, the working group aims to mitigate the risk of catastrophic failures, safeguarding the grid from cyberattacks and infrastructure vulnerabilities.
3. International Standardization and Knowledge Sharing: Developing and promoting international best practices will facilitate cooperation, allow nations to share knowledge, and bolster ICCP resilience.
4. Improved Preparedness for Future Energy Challenges: Ensuring the adaptability of ICCP systems prepares the international power sector for evolving demands, including increasing penetration of renewable energy resources and the need for robust inter-utility data sharing in diverse operational scenarios.

SCOPE :

1. **State of the Art**

- Overview of ICCP Infrastructure: Survey and analyze current ICCP practices and infrastructure resilience standards across power systems in different countries.
- Coverage of ICCP cybersecurity, as specified in IEC 62351-4:2018+AMD1:2020 CSV.
- International ICCP Security Practices: Investigate and document the ICCP security frameworks and protocols implemented in various countries, highlighting differences in resilience approaches, compliance requirements, and security standards. This includes studying national adaptations of ICCP to address local cybersecurity threats and operational challenges.
- Resilience and Redundancy Best Practices: Survey and document best practices in ICCP resilience, focusing on technological and procedural solutions.

2. **Technology and Processes for Resilience**

- Evaluation of Redundancy Measures: Assess current redundancy protocols within ICCP, focusing on multi-circuit and alternate communication channels for enhanced resilience.
- Alternative Technology Integration: Explore viable alternative technologies and data exchange protocols that support or replace ICCP in certain scenarios.
- Impact of Emerging Technologies: Study the compatibility and impact of integrating emerging technologies, such as cloud-based data exchanges or blockchain, with existing ICCP systems for secure data handling.

3. **ICCP Failure Scenarios and Impact Mitigation**

- Single-Point-Failures and Common-Mode Vulnerabilities: Identify potential vulnerabilities that lead to widespread ICCP failures and propose strategies to mitigate these risks.
- Grid Operation with Limited Data: Develop methods for maintaining minimal operational functionality with reduced ICCP data availability, including manual intervention protocols.
- Resilience Strategies for Critical Control Centers: Recommend resilient infrastructure strategies for control centers reliant on ICCP, ensuring continuous operations under compromised conditions.

4. **Cybersecurity Considerations**

- Cyber Threat Overview: Provide an overview of cybersecurity risks relevant to ICCP, focusing on key cyberattack scenarios that could impact data exchange and grid reliability.
- ICCP Security Practices Review: Summarize existing ICCP security practices, identifying practical enhancements to strengthen data integrity, authenticity, and confidentiality.
- Guidelines for Incident Response: Outline general guidelines for incident detection and recovery to support a quick response to ICCP-related cyber incidents, focusing on key strategies to minimize data loss and downtime.
- Metric and KPI: Discuss metrics and KPIs to measure the effectiveness of implemented cybersecurity measures.

5. **Operator Preparedness and Response Scenarios**

- Impact of ICCP Failures on Grid Operations: Identify key scenarios that illustrate the effects of ICCP outages, including shifts to manual control and limited use of alternative data sources, to help operators understand primary challenges.
- Scenario-Based Insights: Provide example scenarios of ICCP failures and cybersecurity threats, offering insights into resilient response strategies. This approach will help operators gain an understanding without creating detailed exercises or extensive training modules.
- Best Practices Overview: Compile a concise overview of selected international best practices in operator preparedness for ICCP-related disruptions, encouraging knowledge exchange and regional adaptation.

6. **Data and Tools for Resilience Assessment**

- Essential Data Requirements: Outline core types of data necessary to assess and maintain ICCP resilience, particularly during high-stress scenarios.
- Modeling and Simulation Tools: Recommend a few widely available modeling and simulation tools for assessing ICCP performance under select failure modes, aiming to inform resilience practices.
- Preliminary Resilience Standards: Propose a set of high-level guidelines for ICCP resilience assessment to assist utilities in identifying areas for improvement in system robustness. This initial guidance can serve as a foundation for future, more detailed standards.

Remarks:

The ICCP Security and Resilience Working Group addresses an essential area for power grid reliability, given the increasing interconnectivity and cybersecurity risks facing modern power systems. By examining international best practices and developing standardized resilience strategies, this group aims to contribute significantly to enhancing ICCP infrastructure.

This working group will collaborate closely with North American Electric Reliability Corporation (NERC) in the U.S. On-going discussions have established the ICCP security and resilience as areas of common interest. Further activities will be determined by the working group in consultation with SC D2 and NERC.

DELIVERABLES AND EVENTS

Deliverables Types
Electra report
Meeting
Technical Brochure and Executive Summary in Electra
Webinar
Work Schedule

Deliverables schedule

Meeting	Q2	2025	Membership recruitment
Work Schedule	Q4	2025	Develop work plan
Technical Brochure	Q4	2026	Draft TB for SC Review
Technical Brochure	Q1	2027	Final TB
Webinar	Q2	2027	Webinar
Electra report	Q2	2027	Electra

APPROVAL BY TECHNICAL COUNCIL CHAIRMAN:
Rannveig S. J. Løken
January 13th, 2025