DISCUSSION MEETING SUMMARY

Study Committee D2

Information systems telecommunications and cybersecurity

25th August 2026

Chair: Victor Tan

Secretary: Marcelo Araujo

Special Reporters:

PS1: Carolina Villasanti and Junho Hong

PS2: Joel Mataboge and Louise Watts

PS3: Pornpong Chiewcharat and Peter Ceferin

1. INTRODUCTION

The 2026 discussion meeting of Study Committee D2 was held on 25th August in room 352AB at the Palais des Congrès in a morning and afternoon session.

The three Preferential Subjects were:

> **PS1:** Extracting value from information and data through decision support tools and techniques in managing the increasing complexity of power grids
> **PS2:** Comprehensive approaches to managing cybersecurity in energy applications
> **PS3:** Next-generation telecommunications technologies to support grid decarbonisation and digitalisation

General statistics

Over 130 participants at the peak (during the morning session), averaged more than 100. All subjects stimulated very active discussions.
There were a total of 106 papers with 72 questions and 72 contributions.

PS1

33 papers, 25 questions, 22 contributions

PS2

28 papers, 24 questions, 18 contributions

PS3

45 papers, 23 questions, 32 contributions

2. RUNNING OF THE MEETING

The Discussion Group Meeting was chaired by the Study Committee Chairperson, Victor Tan (AU), with Carolina Villasanti (PY), Junho Hong (US), Joel Mataboge (ZA), Louise Watts (AU), Pornpong Chiewcharat (TH) and Peter Ceferin (SL) as Special Reporters and Marcelo Araujo (BR) and Marit Owren Valmot (NO) as GDM Secretary. Vitor Meneguim (FR) served as interactivity manager.

The morning session started with a brief summary by the chairperson of the scope of the work of SC D2. The chairperson also provided a quick summary of the procedure for running the GDM. The chairperson then introduced the special reporters and the preferential subjects, and indicated that the special reporters would provide a brief discussion of each preferential subject after the contributors' presentations with the assistance of Slido.

3. CONTRIBUTIONS TO PREFERENTIAL SUBJECT 1

PS1 – EXTRACTING VALUE FROM INFORMATION AND DATA THROUGH DECISION SUPPORT TOOLS AND TECHNIQUES IN MANAGING THE INCREASING COMPLEXITY OF POWER GRIDS

The contributions to PS1 show a clear transition toward more integrated cyber-physical power system environments, where operational technology, information systems, data platforms, analytics, artificial intelligence, and cybersecurity functions are increasingly interconnected to support more reliable and resilient grid operation.

Several contributions emphasized that future grid management depends not only on individual applications, but also on trusted and well-governed data foundations. Network models, grid-edge measurements, AMI data, SCADA information, asset data, and operational records must be structured, validated, and traceable before they can reliably support advanced analytics, automation, or operational decision-making.

Governed network models were presented as a way to improve trust in utility network data across GIS, SCADA, EMS, DMS, DERMS, digital twins, engineering applications, and AI. By introducing governance functions such as identity, semantics, topology validation, lineage, lifecycle management, evidence, and controlled publication, utilities can improve the reliability of network models used across enterprise and operational systems.

The use of AI and advanced analytics was another major theme. Contributions addressed LLM deployment in utility OT environments, AI-based predictive maintenance for EV charging infrastructure, edge AI and thermal analytics for substation monitoring, and machine-learning-based cyberattack detection. These papers show that AI can support monitoring, maintenance, forecasting, cybersecurity, and decision support, but also highlight the need for validation, auditability, and governance before AI outputs are used in real operational environments.

LLM deployment in OT environments requires special attention to cybersecurity, data handling, and regulatory constraints. A layered architecture with separated inference, orchestration, and audit/data-management functions can help reduce risk in air-gapped or restricted utility OT environments. However, practical implementation, testing, and comparison with existing approaches remain important for demonstrating operational value.

Predictive maintenance applications for EV charging infrastructure showed how AI and physics-based reasoning can be combined to identify abnormal conditions, estimate health indices, and reduce maintenance costs. These approaches can help utilities and charging service providers move from reactive or preventive maintenance toward predictive maintenance, but the methods require clear explanation of data handling, model validation, and health-score calculation.

Grid-edge and substation monitoring applications demonstrated the growing role of edge AI, thermal analytics, SCADA integration, and predictive monitoring in utility operations. Field-oriented examples showed that these technologies can support early detection of abnormal equipment conditions and improve situational awareness. At the same time, quantitative validation, alarm-quality metrics, and clearer separation between deployed functions and future concepts are needed to strengthen practical confidence.

Cybersecurity remained a central concern across PS1. Several contributions examined secure remote access, electronic security perimeters, internal network security monitoring, field-device vulnerabilities, IED management, and cyberattack detection in SCADA and microgrid environments. These papers highlight that modern utility cybersecurity is moving beyond perimeter protection toward continuous monitoring, secure access management, vulnerability evaluation, compensating controls, and operationally aware detection methods.

The evolution of NERC CIP requirements and internal network security monitoring indicates that utilities must increasingly integrate network visibility, anomaly detection, SIEM/SOC processes, and OT-specific monitoring architectures. Practical deployment challenges include legacy equipment, limited bandwidth, data volume, scalability, and resource constraints. These challenges show the importance of risk-based implementation strategies that can be adopted by utilities with different levels of cybersecurity maturity.

Field evaluations of distribution devices and IED management practices showed that cybersecurity programs must be connected to procurement, deployment, configuration management, credential management, monitoring, and compensating controls. These contributions are especially valuable because they focus on practical lessons from utility environments rather than only conceptual cybersecurity frameworks.

Several papers addressed cyber-physical detection and mitigation. DNP3-based microgrid testbeds, RTU-level cyberattack-versus-fault classification, and false-data-injection detection using transmission data showed the potential of machine learning and rule-based methods for

identifying abnormal grid behavior. However, these applications also require careful validation under realistic operating conditions, independent test cases, and consideration of the operational impact of false positives and false negatives.

The contributions also showed that digital validation platforms are becoming increasingly important. Hardware-in-the-loop testing for AMI 2.0 use cases, PSCAD-based cyber-physical testbeds, and real-time digital grid models can help utilities evaluate new technologies before large-scale deployment. These platforms support safer testing of grid-edge applications, communication interfaces, analytics, and control functions under more realistic conditions.

Some contributions focused on communication and timing infrastructures for resilient grid operation. Topics such as synergic power and communication networks, traveling-wave-based time distribution, and secure remote data collection show that communication systems are not merely supporting infrastructure; they are becoming essential components of modern power system reliability, observability, and cybersecurity.

Grid-forming resources, BESS, hybrid PV-diesel systems, and AI data-center load management appeared in several contributions as emerging operational challenges. Although some of these topics may fit more naturally within power-system planning, dynamics, or DER-focused study areas, they still demonstrate the growing importance of digital control, monitoring, and validation for future cyber-physical grid operation.

The papers also reflected the importance of interoperability and standardization. Common information models, governed data structures, utility architecture frameworks, and consistent device-management practices are needed to reduce fragmentation across utility systems. Without interoperability and consistent data governance, advanced analytics and AI tools cannot be easily scaled across planning, engineering, operation, maintenance, and cybersecurity functions.

Another important lesson from PS1 is that algorithmic performance alone is not sufficient. High detection accuracy or promising AI results must be accompanied by explainable assumptions, independent validation, realistic operating scenarios, and clear operational procedures. This is especially important when automated analytics may influence operator decisions, equipment control, or cybersecurity response.

Human oversight and accountability remain essential. Even when AI or automated analytics provide useful recommendations, utilities must understand how results are generated, how reliable they are, and what risks may arise if the system produces incorrect outputs. This is closely related to avoiding AI overreliance and automation bias in critical grid operations.

Overall, the PS1 contributions show that the future of IT/OT solutions in electric power systems will depend on the combined development of reliable data, trusted analytics, secure digital

infrastructure, interoperable platforms, and human-governed decision-making. The physical grid and the digital grid must evolve together to improve efficiency, resilience, cybersecurity, and operational value.

4. CONTRIBUTIONS TO PREFERENTIAL SUBJECT 2

PS2 - COMPREHENSIVE APPROACHES TO MANAGING CYBERSECURITY IN ENERGY APPLICATIONS

Preferential Subject 2 (PS2), titled *Comprehensive Approaches to Managing Cybersecurity*, explores how electric utilities can transition from isolated cybersecurity measures to integrated, defence-in-depth strategies that protect increasingly digitalised operational technology (OT) environments. The subject draws on eighteen contributions from international experts, covering areas such as digital substations, IT/OT segmentation, OT monitoring, distributed energy resources (DERs), artificial intelligence (AI), and quantum-safe cryptography. Together, these contributions demonstrate the growing need for holistic cybersecurity approaches that balance resilience, operational reliability, and technological innovation.

The contributions represent a broad international perspective, with participation from South Africa, the United States, Germany, Finland, France, Italy, the United Kingdom, China, and Brazil. Despite their varied focus areas, the papers converge around seven key themes: digital substation security, IT/OT segmentation, OT security operations centres (SOCs) and SIEM platforms, legacy SCADA protection, EV charging and DER security, AI-enabled threat detection, and quantum-safe security techniques. These themes highlight the industry's efforts to secure both existing critical infrastructure and emerging smart grid technologies.

A central message emerging from the contributions is that cybersecurity solutions for power systems must preserve deterministic performance, low latency, and high availability. Security is increasingly being embedded directly into engineering and operational processes through configuration-driven policies, automated enforcement mechanisms, industrial DMZs, and software-defined micro-segmentation. At the same time, utilities are seeking greater visibility and situational awareness through integrated IT-OT monitoring and coordinated security operations capabilities.

The papers further indicate that future cybersecurity strategies will increasingly depend on context-aware AI, explainable analytics, and quantum-safe protection mechanisms. However, these technologies are positioned as enhancements to, rather than replacements for, fundamental cybersecurity practices such as segmentation, hardening, and standards-based security architectures. Collectively, the contributions suggest that the future of utility

cybersecurity lies in combining proven engineering principles with intelligent, adaptive security controls that maintain the reliability and safety requirements of critical power system operations.

Cybersecurity is essential to enabling a safe, reliable and resilient digital energy transition and is now central to power systems engineering requirements. It is not enough to only apply traditional IT controls or meet compliance requirements, we need controls that protect connected operational technology while maintaining safety, availability, resilience and deterministic performance required by the electrical applications.

The main themes included the importance of secure-by-design architecture and lifecycle management. Standards like IEC 61850, IEC 62351 and IEC 62443 provide foundations for securing communications, implementing zones and conduits, managing access and validating controls throughout the lifecycle. There was also strong emphasis on defence in depth: segmentation, DMZs, secure remote access, OT-aware monitoring, testing and governance.

For digital substations, several contributions showed how Software-Defined Networking can support micro-segmentation, centralised policy control and deterministic whitelisting of IEC 61850 traffic. These approaches can strengthen security without compromising the low latency and high availability required for protection systems.

In relation to the modernisation of IT/OT segmentation, contributors recommended moving beyond static isolation towards controlled, policy-based connectivity, supported by hardened OT DMZs, Zero Trust principles, device profiling and compensating controls for legacy SCADA environments.

Monitoring and incident response was another key priority. Coordinated IT/OT SOC models and federated SIEM architectures can improve visibility and detection, but it was suggested that mitigation actions must remain aware of OT use cases and still be human-supervised.

Finally, the value of AI, digital twins, test traffic and quantum-safe communications was identified as useful applications, provided these technologies are deployed in a way that is practical for operational environments. AI was also discussed in regards to using it to better understand the operational context of an event prior to taking mitigative action and adaptive vulnerability assessments are required to revalidate controls as systems change.

The discussion highlighted emerging cyber risk from large-scale EV charging infrastructure. Secure-by-design principles, strong identity and access management, encrypted communications, continuous monitoring and simulation-based stress testing can help manage the potential impacts of coordinated attacks.

The contributions stressed that cybersecurity controls must be timing-aware. In particular, security for fast protection signalling should be selected based on the timing class and operational criticality of the communication. A layered approach to authentication and encryption is more suitable than a single universal solution.

We must remain vigilant with cyber controls where physical security may be lacking, to prevent unauthorised network access, particularly at the edge where remote substations may be unattended.

The overall conclusion from the General Discussion is that cyber resilience depends on a layered standards based and defence in depth approach taking into account practical operational context, continuous validation and strong collaboration between engineering, operations and cybersecurity teams.

5. CONTRIBUTIONS TO PREFERENTIAL SUBJECT 3

PS3 - NEXT-GENERATION TELECOMMUNICATIONS TECHNOLOGIES TO SUPPORT GRID DECARBONISATION AND DIGITALISATION

A hybrid SDH/MPLS-TP platform bridges the gap between legacy circuit-switched and modern packet-switched networks. This dual-layered strategy ensures guaranteed service continuity and ultra-low latency for critical teleprotection while avoiding the high capital expenditures and complexity of maintaining separate, redundant physical infrastructures during extended transition periods.

A structured six-step roadmap manages the migration of legacy TDM networks to packet environments by covering requirements gathering, technical studies, design reviews, verification, presentation, and lifecycle management. Transmission system operators (TSOs) prioritize equipment diversity and strict latency for differential protection, whereas distribution system operators (DSOs) focus on modular, cost-effective rollouts. Rigorous laboratory-based Proof of Concepts followed by extended field trials validate suitability before live grid deployment.

An MPLS-TP architecture utilizing Circuit Emulation Services (CES) successfully integrates legacy TDM equipment with packet networks during partial grid upgrades. Enhanced delay control mechanisms achieve sub-4ms latency and hitless switching, ensuring that current differential protection remains unaffected by background IP traffic and packet jitter.

A phased migration framework utilizes Layer 3 IP converters to packetize traditional TDM traffic. By deploying these converters from central hubs to remote access sites, the utility eliminates redundant hardware and maintains service continuity, proving that transmission delays remain well within acceptable limits for legacy analog telecontrol systems.

Line differential protection systems are highly sensitive to latency asymmetry and jitter introduced by TDM-to-packet migration. Standard circuit emulation can trigger unwanted protection tripping during network routing changes, highlighting the critical need for application-specific interworking functions and rigorous pre-deployment risk assessments.

Physical, reduced-scale network replicas provide a superior validation method compared to computer-based simulations for testing packet transport under live grid conditions. Physical

replicas capture real-time, high-resolution measurements of latency and jitter under extreme congestion, whereas software simulations struggle to model complex hardware behaviors and require excessive computing times.

An integrated two-stage test methodology validates packet network performance for current differential protection. The process begins with a laboratory-based Proof of Concept using physical power system simulators and multiple relay brands over a 10GE DWDM network carrying STM-over-MPLS-TP. This is followed by an extended field trial over a 1,400-kilometer fiber link to verify long-term packet network stability under real-world operating conditions.

IP/MPLS and SRv6 architectures meet strict operational technology (OT) requirements through a coordinated four-step adaptation framework. This framework combines TDM circuit emulation, network slicing, co-routed path policies to enforce symmetrical bidirectional paths, and dynamic buffering to eliminate packet jitter, successfully maintaining end-to-end latency below 10 milliseconds across a 16-hop network.

An enhanced fine-grain Optical Transport Network (fgOTN) platform serves as a modern successor to legacy SDH. By leveraging a native TDM hardware-scheduling mechanism, fgOTN provides rigid physical-layer isolation ('hard pipes') and ultra-low latency, enabling the secure, simultaneous transport of legacy teleprotection and modern packet services over a unified fiber backbone.

A comprehensive four-phase transition roadmap structures network migration around design, coexistence, shadow operations, and retirement phases. Testing the new packet infrastructure during the 'shadow operations' phase with active traffic allows the utility to identify hidden network vulnerabilities, validate synchronization performance, and train the workforce without risking live grid protection.

Asynchronous packet networks require precise synchronization tuning when replacing synchronous legacy TDM systems. Synchronous Ethernet (Sync-E) provides the stability needed for digital current differential teleprotection. A multi-phased risk-mitigation roadmap (deploying on small trial sites, isolating to single lines, replacing only backup paths, and enforcing long soak times) safely builds operational skills while avoiding network vulnerabilities.

Teleprotection services migrate to MPLS-TP networks utilizing Circuit Emulation Services (CES) to packetize legacy traffic over fiber networks. For regions where fiber is incomplete, hybrid microwave platforms facilitate a gradual transition, utilizing symmetrical virtual tunnels to actively manage latency and jitter for high-stakes protection applications.

Fine-grain Optical Transport Network (fgOTN) technology replaces legacy SDH by maintaining the deterministic latency and physical-layer isolation of traditional TDM while supporting modern Ethernet. A specialized path-symmetric protection switching mechanism

prevents false line differential tripping by ensuring transmit and receive paths remain perfectly symmetrical during fiber failures.

SDN-driven Segment Routing (SRv6) policies manage the massive traffic surges generated by unattended substation video surveillance. By utilizing Multi-SID Lists, the network automatically and dynamically distributes data loads across multiple paths based on real-time bandwidth weights, preventing network congestion and maximizing utilization without impacting critical OT traffic.

A machine learning-driven traffic shaping model dynamically prioritizes critical SCADA (IEC 60870-5-104) traffic over standard IT data on shared utility networks. This active traffic management serves as part of a four-stage roadmap designed to transition manual network configurations into a highly autonomous, secure, and self-healing OT network fabric.

No single wireless technology can fulfil all power utility communication requirements. Selection should consider application criticality, latency, coverage, resilience, capacity, cost and local conditions. A layered or hybrid architecture combining wireless and fixed technologies is therefore generally preferable.
Field experience confirms that coverage is often the first selection criterion, with terrain, propagation and existing infrastructure strongly influencing feasibility.

Microwave remains important for applications requiring high availability and predictable performance. Properly engineered systems can transport teleprotection, SCADA and legacy TDM/Ethernet services while meeting latency, jitter, synchronisation and resilience requirements.

The role of wireless as primary or backup transport should be determined service by service. Microwave may support protection and SCADA, while high-capacity applications generally remain better suited to fibre.

Private 5G and Wi-Fi provide complementary capabilities: Private 5G for wide outdoor coverage and Wi-Fi for flexible indoor connectivity. For non-critical applications, throughput and coverage may be the main priorities.

Long-term architectures should also exploit existing utility-owned infrastructure. Reusing cables and power-line communication assets, complemented by wireless where needed, can improve resilience and reduce investment.

For mission-critical WANs, deterministic communication requires coordinated design of transport, routing, redundancy and time synchronisation. All-photonic transport over OPGW was presented as one promising future option.

PTP-aware packet networks using Transparent and Boundary Clocks can provide accurate synchronisation. Independent PTP paths and additional local time references can enhance resilience.

Cross-border mission-critical networks additionally require operational autonomy and cybersecurity. MPLS-TP, controlled latency, common PTP synchronisation, and defined border gateways were proposed for interconnecting national networks.

Migration of inter-substation protection from TDM to packet networks should be phased. Hybrid IEC 61850 gateways allow legacy and digital systems to coexist while progressing toward native R-GOOSE and R-SV communication.

A practical migration path therefore combines continued use of TDM/hybrid gateways, the introduction of OT IP/MPLS, and an eventual transition to native IEC 61850 WAN services.

Complex multipoint protection requires system-level validation. Centralised engineering, offline simulation and pre-deployment testing can verify protection logic, communication behaviour and failure scenarios before commissioning.

Synchronisation resilience should combine geographically distributed grandmasters, redundant paths, appropriate oscillator holdover and application-specific accuracy. Protection should degrade gracefully by disabling only functions that require precise timing.

A utility pilot demonstrated PTP distribution for line differential protection over an MPLS WAN, with correct protection operation and almost five hours of Clock Class 7 holdover after loss of the external reference.

Redundant Grandmaster architectures should be complemented by continuous monitoring. BMCA failover, Boundary/Transparent Clocks and monitoring of ClockClass, Grandmaster identity and device availability provide both timing resilience and operational visibility.

6. CONCLUSION

The contributions to PS1 show that IT/OT solutions are becoming core infrastructure for efficient, resilient, secure, and data-driven power system operation. The papers highlighted AI-enabled monitoring, LLM deployment in OT environments, governed network models, AMI 2.0 validation, cybersecurity monitoring, secure remote access, IED management, and cyber-physical detection. A key message is that AI and advanced analytics can create significant operational value, but only when they are supported by reliable data, interoperability, validation, auditability, and appropriate governance.

Cybersecurity remains a cross-cutting priority as utilities adopt more connected field devices, remote access, cloud services, vendor platforms, and AI-based tools. The PS1 contributions also emphasized the need for real-world validation through field experience, hardware-in-the-loop testing, cyber-physical testbeds, and practical deployment studies. Overall, the physical grid and the digital grid must evolve together. Future IT/OT solutions should combine trusted data, validated analytics, strong cybersecurity, and responsible human oversight to create practical value for electric power utilities.

The contributions presented this year in telecommunications demonstrate that migrating mission-critical utility services from legacy TDM to packet-switched WAN backbones is both technologically mature and operationally viable when executed through highly structured, multi-phase roadmaps. Field validations and laboratory trials confirm that technologies such as MPLS-TP, fine-grain Optical Transport Networks (fgOTN) with rigid physical isolation, and Segment Routing (SRv6) can consistently meet the stringent sub-millisecond latency, symmetry, and failover constraints of line differential protection. De-risking these migrations requires a shift toward rigorous pre-deployment validation, leveraging physical reduced-scale network replicas and multi-vendor laboratory Proof of Concepts to address synchronization and jitter vulnerabilities before live cutover. Furthermore, as operational networks experience

greater IT/OT traffic convergence, the integration of software-defined networking (SDN) and machine-learning-based traffic shaping is proving essential to dynamically manage network congestion and guarantee absolute priority for critical SCADA and telecontrol traffic.

Future utility telecommunications will rely on complementary wired and wireless technologies rather than a single solution. Mission-critical services require deterministic transport, resilient architectures and accurate, redundant time synchronisation. Migration from TDM toward packet-based and native IEC 61850 communication should remain phased to preserve operational reliability and existing investments. Simulation, offline engineering and system-level validation will become increasingly important as protection and control applications depend more strongly on complex communication networks.