SPECIAL REPORT FOR SC D2 -

CHAIR: Victor Tan
SECRETARY Marcelo Araujo

SPECIAL REPORTERS

Carolina Villasanti & Junho Hong (PS1)
Joel Mataboge & Louise Watts (PS 2)
Pornpong Chiewcharat & Davy Haegdorens (PS3)

A few words about Session Papers

Session Papers focussed on a number of Subjects – referred to as 'Preferential Subjects' – selected in advance by the 16 Study Committees of CIGRE and available in the Call for Papers .
Session Papers are selected through a two-phase review process – abstracts and full Papers.
Have a look at the Technical Programme - the list of selected Papers for the Session, and so have an overview of subjects that will be discussed. It is updated as Full Papers review proceeds.

And specificity of CIGRE Sessions

At CIGRE Sessions authors are given the opportunity to present their Paper during half-day specific meetings – the Poster Sessions.
Four days are also dedicated to 'Group Discussion Meetings' organised by Study Committees. Four meetings run simultaneously each day from Tuesday to Friday, under the presidency of the Study Committee Chairs. The purpose of these meetings is the discussion of the Session Papers on the basis of "Special Reports" which incorporate the gist of the Session Papers and raise a number of questions for discussion.
The Special Reports are available to all on free access – at the end of May - on the CIGRE website, on the Session page.
For fruitful discussions delegates are strongly encouraged to read the Papers before the Session.
The set of Session Papers is made available for downloading to all duly registered delegates before the Session through their private account on the registrations portal.
Papers are also readable on the Session smartphones application on site in Paris.
Follow our Session latest news and General Programme - by regularly visiting our website !

PARTICIPATING IN THE 2026 PARIS SESSION

You are invited to participate in discussing this Special Report at the SC D2 session held on **August 25 starting at 08:45 in room 352AB** at the Palais de Congress de Paris.
The reporters have compiled up to 68 questions, these are not specifically aimed at the papers' authors, but are synthesised from common issues and trends identified in across the papers. This provides the opportunity for a broader response and participation in the discussion session.
We encourage you to share your views or experiences in response to the specific questions in this report. During the Group Discussion Meeting, each prepared contribution will be allocated a time slot of three to four minutes for a presentation.

Procedure for contributions.

1. Contributors should upload contributions on the registrations portal – "Contributions to Group Discussion Meetings" section - using your existing account and own credentials **before 7th August 2026**, for a prior screening and a good organization of the Group Discussion Meeting. Important points:
2. Access to contribution uploading is given only to duly registered delegates.
   - As a consequence, registration to CIGRE Session should be finalized before uploading contribution(s) online.
   - Register now for the Session registrations
   - Contributions uploading will be open at start of June.
3. Special Reporters will review the prepared contributions (Power point presentation with max **3** slides and a written word file with max 1000 words pr contribution). A guide for contributors as well as templates and sample pages will be available on the Paris Session webpage. Important notice: No commercial names are to be included in presentation or the written summary (even TSO/DSO names).
4. Any recommendations or changes to the contributions will be provided to the contributors by the Special reporters directly on the Registration platform between 7th of August and 14th of August 2026. Contributors are encouraged to visit their account on the registrations portal to see the result of this review.
5. All contributors with accepted/finalised contributions will be contacted by the Special reporters between 7th of August and 14th of August 2026, to finalize the presentation and receive the instructions regarding the session.
6. Important note:
   - All contributions must be uploaded prior to the Conference in Paris.
   - Last minute changes to the contributions will not be granted.

7. During the GDM the Study Committee Chair may call for spontaneous contributions, which will only be verbal with no slides. All attendees are eligible to make such a contribution. Attendees who provide a spontaneous contribution are allowed to deliver a written contribution which will be included in the Session Proceedings. This text is required to be forwarded within a maximum delay of two weeks after the Study Committee GDM Session (i.e. by date) to the SC Secretary (email address).
8. It is expected that the questions relevant to the Preferential Subjects will attract many prepared contributions. The number of contributions for each Preferential Subject (PS1, PS2 and PS3) may need to be limited. The selection will be based on relevance, quality and time of submission of the contribution.

9. Please note that there will be no pre-session meeting with the Special Reporters, SC Chair and SC Secretary. SC D2 asks you to provide to the Special Reporters a single sentence that summarizes your prepared contribution. The Special Reporters will share with contributors the GDM schedule, so they can be aware of the time of your presentation.

A summary of SC D2 Activities during the Paris Session, including the GDM and the Poster Session is available in the table below:

Date	Event	Start Time	End Time	Room
25/08/2026	D2 GDM - Group Discussion Meeting	08:45	18:00	352AB
26/08/2026	SC D2 Poster Session	08:30	10:30	Hall Ternes (Level 1)
	SC D2 Tutorial - Application of AI for Power Utilities	14:00	15:30	342AB
	SC D2 Workshop - Challenges and Recommendations for DER integration to the grid from the perspective of information exchange, cybersecurity and telecommunications	16:00	17:30	REGENCY 15

Table 1 - SC D2 Activities

SC D2 POSTER SESSION

Authors of SC D2 Session papers are required to present their papers during the **SC D2 Poster Session scheduled on August 26th, from 08:30 to 10:30** in **Hall Ternes on level 1**. Template and instructions on poster preparation are available on the CIGRE 2026 Session website. Posters will be displayed on digital screens. **Poster presentations must be uploaded on the ConfTool platform from 18th May by 29th June at the latest** for review by the poster session convener. Poster conveners may ask for a final version, incorporating any requested changes, must be uploaded **by August 14th**. It should be noted that authors will **not** have the possibility to upload their own file on the day of the Poster Session. If the author(s) cannot attend the Poster Session he/she or the relevant National Committee is requested to send a substitute.

SCOPE OF STUDY COMMITTEE D2 - INFORMATION SYSTEMS, TELECOMMUNICATIONS AND CYBERSECURITY

The scope of CIGRE Study Committee D2 is focused on the fields of information systems, telecommunications and cybersecurity for power systems. SC D2 contributes to the international exchange of information and knowledge, adding value by means of synthesizing state of the art practices and drafting recommendations.

SC D2‘s principal areas of interest:

- Studying and considering the evolution of information and telecommunication technologies to cope with traditional and new requirements driven by the digital transformation in the power industry including extension of Distributed Energy Resources.
- Assessment of Technologies and architecture to assure business continuity and disaster recovery.

- Overcoming security threats in the deployment of the networks of the future and especially in Smart Grids.

The Preferential subjects for the 2026 Paris Session are:

Preferential Subject 1 (PS 1): Extracting value from information and data through decision support tools and techniques in managing the increasing complexity of power grids

- Predictive analytics techniques to forecast generation from renewable sources/distributed energy resources
- Case studies and guidelines for AI application in power system operation and planning
- Development of AI and machine learning models for real-time and predictive grid optimisation

Preferential Subject 2 (PS 2) - Comprehensive approaches to managing cybersecurity in energy applications

- Cybersecurity compliance, obligations, regulations and legislations in the energy sector, including cybersecurity organisational processes, technical measures, standards, and certifications
- Integrated solutions for physical and cyber threat detection platforms to support asset and incident management, including artificial intelligence techniques
- New strategies and approaches for protecting energy infrastructures and sensitive data against cyber threats

Preferential Subject 3 (PS 3) - Next-generation telecommunications technologies to support grid decarbonisation and digitalisation

- Optimised migration approach from legacy to packet networks to support mission-critical power systems services
- Next-generation technologies in enhancing coverage and resilience of wireless communication networks for power systems
- Telecommunications technologies and techniques for a highly resilient and mission-critical system

In the next paragraphs, a summary for each approved paper and the questions produced by the Special Reporters are presented.

Preferential Subject 1 (PS 1): Extracting value from information and data through decision support tools and techniques in managing the increasing complexity of power grids

Introduction

Modern power systems are becoming increasingly complex due to the large-scale integration of renewable generation, distributed energy resources, advanced communication infrastructures, and intelligent field devices. As a result, utilities are required to manage larger volumes of heterogeneous data across planning, operation, asset management, and market-related processes. Within this context, the ability to extract actionable value from information and data is becoming essential for improving the efficiency, reliability, resilience, and flexibility of electric power systems.

This Preferential Subject addresses the growing role of decision support tools and techniques in managing this increasing complexity. It covers contributions related to data-driven and AI-enabled applications for forecasting, monitoring, anomaly detection, asset management, system planning, and operational decision-making. It also includes the development of digital twins, standardized data environments, data historians, interoperability frameworks, and advanced analytics platforms that enable utilities to transform raw data, legacy documents, and real-time measurements into structured and useful knowledge.

This year's papers show a clear transition from isolated analytical tools toward integrated, data-centric, and AI-assisted grid management approaches. Many contributions emphasize the importance of data quality, observability, interoperability, explainability, and governance as prerequisites for the practical deployment of advanced analytics in real utility environments. The papers also demonstrate increasing maturity in the application of machine learning, deep learning, multimodal AI models, knowledge-based methods, and optimization techniques to support both short-term operational decisions and long-term planning studies.

A common theme across the contributions is that future power system performance will depend not only on physical grid infrastructure, but also on the robustness and intelligence of its digital counterpart. Integrated digital platforms, standardized information models, and scalable data architectures are becoming critical foundations for reliable decision-making across the asset lifecycle. Together, the papers under this Preferential Subject highlight the continuing shift toward holistic cyber-physical ecosystems in which data, models, and intelligent decision-support tools play a central role in enabling the secure, efficient, and resilient operation of modern power grids.

A total of 33 papers were accepted within the SC D2 PS1:

Paper Reference	Title	Country
10112	NWPsolarNet: A Scalable Deep Learning Framework for Medium-Term Solar Forecasting across Europe	Slovenia
10137	Machine Learning Model for Real-time Prediction of Influx of Critical Corrective Maintenance Work on the Grid	United States of America
10156	Collaborative Forecasting Platform: Results after one year of operation for wind and solar forecasting in Belgium	Belgium
10168	Leveraging RAG for Reasoning and Analyses of Electricity Distribution Codes	Egypt
10524	ANN Based Day Ahead Forecasting Model for All India Demand	India
10525	ISTS Communication System for cross border links in Indian Power Sector	India
10526	Real-Time Time Synchronisation Monitoring System for IEDs in Power System	India
11227	Deployment of an Intelligent Robotic Diagnostic System for Outdoor Switchgear Equipment Based on Multispectral Analysis and AI	Russia
11230	Application of AI (ML) Tools for Model Validation and Anomaly Detection	Russia

11231	Synchrophasor Data Reliability Monitoring in Power System Operational Mode Analysis	Russia
11232	AI-Based System for Automated Digitalization of Relay Protection Settings Forms	Russia
11235	The Accuracy of Renewable Energy Generation Forecasting in Energy Systems: Quality Improvement Practices	Russia
11239	Leveraging AI to Identify the Root Causes of PMU Data Latency and Loss for Control Room	Russia
11240	Use Cases of Digital Models and Digital Twins in Power Supply Systems of Large Consumers	Russia
11402	AI Applications in Power Systems: The Role of Structured Data and the Acceleration of Legacy Data Structuring through Artificial Intelligence	Brazil
11573	Recommendation Algorithms for Smart Distribution Network Standards	China
11578	PowerPlan-GPT: A Framework for Generating Intelligent Power Supply Solutions Based on Multimodal Models and Its Empirical Application Research	China
11642	Renewable energy forecasting with Deep Learning tools	Spain
11682	Performance Comparison of Various Regression Models in Geothermal Power Plant Net Power Generation Prediction	Turkiye
11774	AI-enhanced generation- and load forecasts in isolated power systems	Denmark
11888	Application of Deep Neural Networks for Fault Detection in Modern Power Systems	Norway
11944	A Comprehensive Framework for the Deployment of AI-Based and Data-Driven Supporting Tools in Generation Expansion Planning	Jordan
11964	Leveraging Meter Load Data to Build a Bottom-up Spatial Load Forecasting	Canada
11988	PowerCIM: A Standardized Data Environment for Decision-making in Complex Power Grids	Croatia
12098	Unlocking the full potential of data historians across the modern power grid: from generation	South Africa
12146	Transforming Information Management: Data Governance in the Operator and Administrator of the Wholesale Energy Market in Colombia	Colombia
12200	Real-Time Flexibility Analysis and Visualization of Power Systems Using IoT and Augmented Reality	Colombia
12402	Analysis and Modelling of Powerline Communication Data for Low Voltage Cable Asset and Condition Management	Germany
12403	Evolution of Interacting Digital Twins for High Voltage Switchgear Monitoring	Germany
12461	Towards Trustworthy Artificial Intelligence in Grid Control	Germany
12529	Intelligent Computing Resource Management and Optimization Support for AI Applications in the Power Industry	China

12546	Proving the concept of supervised machine learning to predict largest infeed and outfeed volumes and prevent over procurement of reserves – a study of Ireland's three systems	Ireland
12614	From documents to knowledge graphs: Intelligent requirements management using CIM-based ontology	Serbia

Table 2 - Papers for PS1

Paper 10112 showcases NWPsolarNet, a scalable deep-learning framework for medium-term solar forecasting across Europe that supports grid operators in managing renewable-generation variability. It focuses on physics-informed quality control and data-driven normalization to overcome unreliable PV metadata, and on fusing ICON-EU weather forecasts with clear-sky irradiance to produce robust 120-hour solar forecasts that outperform operational and benchmark models.

Paper 10137 presents a machine-learning approach for predicting peaks in emergency corrective maintenance work on transmission and substation assets. It focuses on using weather forecasts and PJM load-demand data to compare regression and classification models, thereby supporting proactive resource planning and faster responses to grid-stress events.

Paper 10156 describes a collaborative forecasting platform for wind and solar forecasting in Belgium. It focuses on creating an open forecasting market where multiple forecasters compete and are rewarded based on performance, with ensemble forecasts improving point and probabilistic forecast accuracy relative to existing operational forecasts.

Paper 10168 discusses the use of Retrieval-Augmented Generation for analyzing electricity distribution codes. It focuses on semantic retrieval and comparison of regulatory documents across countries, helping planners and policymakers identify differences in forecasting, renewable integration, planning rules, and regulatory complexity.

Paper 10524 presents an ANN-based day-ahead forecasting model for All-India electricity demand. It focuses on 5-minute block demand forecasting using historical SCADA demand data, weather variables from multiple locations, and event indicators to support high-resolution operational decision-making.

Paper 10525 examines communication systems for Indian cross-border transmission links. It focuses on OPGW and SDH-based infrastructure for SCADA, VoIP, PMU and operational data exchange, while addressing interoperability, bandwidth, cybersecurity, centralized monitoring, and regulatory requirements for cross-border power trade.

Paper 10526 describes a real-time time-synchronization monitoring system for IEDs in power systems. It focuses on a custom hardware-and-software solution that monitors SNTP packets, compares device time with a GPS-based global reference, and highlights time deviations via a centralized dashboard.

Paper 11227 presents an intelligent robotic diagnostic system for outdoor high-voltage switchgear. It focuses on coordinated UAV and UGV inspections using RGB, infrared, and ultraviolet data; AI-based defect localization; asset-to-data consistency; and defect-development forecasting to support maintenance decision-making.

Paper 11230 discusses AI and machine learning tools for power system model validation and anomaly detection. It focuses on improving data preparation for decision-support systems by

combining traditional validation methods with AI/ML approaches, showing that a hybrid approach is most effective.

Paper 11231 investigates the reliability monitoring of synchrophasor data for operational mode analysis. It focuses on using recurrent neural network forecasting to detect hidden anomalous fragments in PMU signals that may distort low-frequency oscillation analysis yet are difficult to identify with classical statistical methods.

Paper 11232 describes an AI-based system for automated digitalization of relay protection setting forms. It focuses on the MaLena system, which uses machine learning, OCR, and related techniques to extract setting attributes and values from scanned or paper-based forms, reducing the manual effort required to populate digital relay-protection databases.

Paper 11235 presents quality-improvement practices for renewable-energy generation forecasting in the Russian power system. It focuses on the influence of telemetry and equipment-status data quality on wind and solar forecasts, including error classification, data-processing methods, and coordination between plant personnel and forecast users.

Paper 11239 describes AI-assisted root cause identification of PMU data latency and loss in control room applications. It focuses on combining PMU data-quality metrics with LSTM-based time-series analysis, clustering, topology-aware root-cause analysis, dynamic thresholds, and human-in-the-loop learning.

Paper 11240 presents use cases for digital models and digital twins in the power-supply systems of large industrial consumers. It focuses on consumer-side digital-twin architecture for internal grid modeling, condition-based maintenance, remaining useful life estimation, predictive load management, and participation in flexibility or tariff mechanisms.

Paper 11402 examines the role of structured engineering data in enabling scalable AI applications in power systems. It focuses on using AI to extract metadata from legacy documents into a centralized engineering database, improving access to technical information, fault analysis, maintenance support, and future AI-assisted advisory tools.

Paper 11573 proposes a recommendation algorithm for smart distribution-network standards. It focuses on modularizing 186 power standards and combining structural, semantic, and keyword-based retrieval methods — Word2Vec/GAT, SBERT, and BM25 — to recommend scenario-specific standards more accurately.

Paper 11578 introduces PowerPlan-GPT, a framework for generating intelligent power-supply solutions. It focuses on combining multimodal large language models, RAG, graph spatio-temporal neural networks, and adaptive evolutionary algorithms to optimize source-grid-load-storage planning across cost, safety, and timeliness criteria.

Paper 11642 presents deep learning tools for renewable energy forecasting in the Spanish power system. It focuses on Red Electrica's wind and PV forecasting developments, including cloud-based multi-model ensembles, 3D CNN-based architectures, plant-level forecasts, and the use of NWP and historical production data to support operational decision-making.

Paper 11682 compares regression models for predicting the net power generation of a geothermal power plant. It focuses on the influence of geothermal fluid temperature, mass flow rate, and ambient temperature, showing that Gradient Boosting Regression provides the best accuracy and helps reduce imbalance-penalty risk.

Paper 11774 discusses AI-enhanced load and renewable-generation forecasting in the isolated power system of the Faroe Islands. It focuses on using automated machine learning with SCADA and weather data to improve short-term forecasts, support dispatch and storage operations, and enable future dynamic-pricing strategies.

Paper 11888 presents a deep neural network methodology for fault detection and classification in modern power systems. It focuses on co-simulation-based generation of fault scenarios and training data, showing that DNNs can provide very fast fault-location estimates and serve as a useful redundancy tool alongside classical impedance-based methods.

Paper 11944 presents a structured framework for assessing the deployment readiness of AI and data-driven tools in generation expansion planning. It focuses on functional capability mapping, requirements profiling, adapted TRL and ARL* assessment, scoring, and deployment prioritization, with the Jordan case study identifying quick-win capabilities such as dimensionality reduction and explainable diagnostics.

Paper 11964 describes a bottom-up spatial load-forecasting approach built on meter-level data. It focuses on predicting future demand at the lowest measurement level and aggregating it by geography and electrical connectivity, while using load-transfer detection and EV-charger penetration inference to guide infrastructure investment and outage-mitigation planning.

Paper 11988 introduces a standardized CIM-based data environment for decision-making in complex power grids. It focuses on harmonizing SCADA/EMS, GIS, and asset-management data through a central repository with branching, merging, REST access, and bitemporal versioning, enabling traceable reconstruction of historical, current, and planned network states.

Paper 12098 discusses the role of data historians and time-series databases as critical infrastructure for modern power grid operations. It focuses on Eskom's Remote Monitoring and Diagnostics Center, showing how centralized historian architecture, semantic standards, and integrated operational data support fleet-wide monitoring, predictive fault detection, and future digital twin and AI analytics capabilities.

Paper 12146 presents the transformation of information management at Colombia's power-system operator and wholesale energy market administrator. It focuses on an information governance and data quality program that defines roles, catalogs, data flows, quality rules, and master data processes, positioning data as a strategic asset for reliable and agile decision-making.

Paper 12200 describes a real-time flexibility analysis and visualization platform for power systems using IoT and augmented reality. It focuses on combining the geometric method for secure operating-region assessment under N-k contingencies with live simulation data, web dashboards, and a HoloLens-based digital twin of Colombia's transmission system.

Paper 12402 examines the use of power-line communication data for the management of low-voltage cable assets and conditions. It focuses on distributed vector network analyzer measurements, attenuation time-series analysis, waterfall plots, and HDBSCAN clustering to detect anomalies, degradation, and overloads in cable sections before failures occur.

Paper 12403 presents the evolution of high-voltage switchgear monitoring toward interacting digital twins. It focuses on linking digital twins of the switchgear and the monitoring system itself to support virtual configuration, automated commissioning tests, improved interpretation of monitoring data, asset-health prediction, and optimized maintenance decisions.

Paper 12461 discusses how trustworthy AI can be introduced into grid-control applications. It focuses on regulatory and technical barriers and proposes a process-driven approach that covers requirements specification, offline development, and supervised online operation, illustrated through a case study on the AI-based selection of optimal protection settings.

Paper 12529 proposes intelligent computing-resource management for large-scale AI applications in the power industry. It focuses on unified orchestration of heterogeneous edge, regional, and cloud resources, deep learning-based load prediction, elastic scaling, and model-hardware co-design to improve latency, energy efficiency, and utilization in applications such as UAV line inspection and construction safety monitoring.

Paper 12546 presents a supervised machine-learning proof of concept for predicting the largest single infeed in Ireland's All-Island power system. It focuses on a logistic regression classifier that uses demand and wind generation time series to predict whether the largest infeed will remain below a defined ceiling, thereby supporting more accurate reserve procurement and reducing unnecessary reserve costs.

Paper 12614 describes an intelligent requirements-management framework based on a CIM ontology and knowledge graphs. It focuses on transforming static engineering requirement documents into RDF/OWL/SPARQL-based semantic models, enabling automated requirement retrieval, compliance checking, constraint inheritance, consistency validation, and improved traceability for DSO projects.

Discussion and Questions

Q1.01. What are the key challenges in deploying your solution from an experimental stage to real-world operation, and how do you evaluate its scalability in electrical systems?

Q1.02. What level and type of data do you need to achieve reliable results with your methodology?

Q1.03 How does your solution integrate with existing systems in industrial plants, such as SCADA, data historians, or analytics platforms?

Q1.04 How do you build operator confidence in your model's results, and what methods do you use to explain or validate them?

Q1.05 What are the main lessons learned from your project, and what recommendations would you give to industrial plants interested in implementing a similar solution?

Q1.06 How did class imbalance—like having more normal than abnormal events—impact your results, and what approaches did you use to overcome it?

Q1.07. How can the adoption of AI use cases be strategically prioritized in industries with intermediate digital maturity?

Q1.08. What specific types of predictive maintenance or operation problems may benefit most from the quantum approach versus classical methods? What is the current level of technological maturity and what infrastructure would be necessary for a pilot implementation in industries?

Q1.09. Do you believe that feedback from AI model predictions is essential for identifying deviations? How can this be done in production?

Q1.10. What would be the limits of AI use in control centers and predictive maintenance processes? what should be the governance direction in industrial scenarios?

Q1.11. How can an AI-based document digitization system be validated and governed in real operational environments to ensure that extracted technical parameters are not only accurate but also trustworthy enough for safety-critical engineering workflows?

Q1.12. How can forecasting systems be made robust in real operational environments where model performance depends not only on algorithm selection but also on telemetry quality, equipment conditions, and coordination among different operational stakeholders?

Q1.13. How can AI-based monitoring tools be validated and maintained in real control-room environments where data quality problems may evolve over time, share similar symptoms, and require both automated root-cause analysis and human expert feedback?

Q1.14. How can digital twins be practically implemented and maintained across different industrial use cases when each application requires different model fidelity, synchronization frequency, data quality, and integration with existing operational workflows?

Q1.15. How can utilities ensure that AI-ready structured data environments remain accurate, scalable, and governable over time, especially when legacy documents, object-oriented engineering databases, and AI-assisted advisors must coexist within real operational workflows?

Q1.16. How can standards recommendation systems be designed to remain accurate and useful in real engineering workflows where users may search with incomplete terminology, documents are highly unstructured, and both exact keyword matching and deeper semantic understanding are needed?

Q1.17. How can AI-generated planning solutions be trusted and governed in real utility workflows where customer requirements, grid constraints, regulatory rules, and multi-objective optimization results must all be explainable, verifiable, and acceptable to human decision-makers?

Q1.18. How can deep learning forecasting models be reliably integrated into real-time system operation when their performance depends on weather uncertainty, spatial resolution, model selection, and continuous validation across different renewable technologies and geographic regions?

Q1.19. How can forecasting models be selected and validated for real power plant operation when prediction accuracy, overfitting risk, limited data availability, and economic consequences such as imbalance penalties must all be considered together?

Q1.20. How can AutoML-based forecasting tools be reliably deployed in isolated or high-renewable power systems when model rankings, weather-data resolution, local operating conditions, and real-world validation may significantly affect operational performance?

Q1.21. How can AI-based fault detection methods be validated for real control-center use when they must balance speed, accuracy, realistic fault scenario coverage, and redundancy with conventional protection and impedance-based methods?

Q1.22. How can utilities determine which AI-based tools are ready for practical deployment when technical maturity alone is not enough and data readiness, workflow integration, governance, and regulatory acceptance must also be considered?

Q1.23. How can utilities ensure that bottom-up spatial load forecasting models remain accurate, explainable, and operationally useful when they depend on meter-level data quality, inferred customer behavior, network connectivity models, and GIS-based planning workflows?

Q1.24. How can standardized data environments be designed to support reliable decision-making when power system data must be integrated across heterogeneous sources, historical and planned versions, and operational workflows while maintaining traceability, interoperability, and cybersecurity compliance?

Q1.25. How can utilities turn high-volume time-series operational data into reliable AI-ready information when historian architecture, semantic interoperability, edge-to-enterprise integration, cybersecurity, and data readiness must all be addressed together?

Preferential Subject 2 (PS 2) - Comprehensive approaches to managing cybersecurity in energy applications

This preferential subject explores the approaches to managing cyber security in energy applications. Across papers accepted, the strongest theme is the need to secure increasingly digital and interconnected power systems without undermining the core OT requirements of safety, availability and deterministic behaviour. Cyber security in power systems is no longer limited to defence in depth or compliance to standards but is an operational challenge spanning digital substations, dynamic energy resources and multi-organisational protection and control schemes and should be designed to work within the technical and operational constraints of utility environments.

Another strong theme is the role of standards, governance and security architectures in delivering effective cyber security programs. Standards including IEC 62351, IEC 62443 and IEC 61850 are referenced often in discussions proposing approaches to architecture, OT/IT convergence, zero trust, automated testing and governance across complex infrastructures.

Resilient cyber security depends on sound technical controls, clear accountability, lifecycle process and good coordination between engineering, operations and security teams.

Finally there is a growing interest in advanced analytics and emerging technologies for securing critical infrastructure. Several papers explore AI for anomaly detection and intrusion analysis, traffic generations for model training, and advanced technologies for situational awareness, vulnerability management and quantum safe communications, showing how we are preparing for the next generation of cyber threats to critical infrastructure.

A total of 28 papers were accepted within the SC D2 PS 2:

Paper Reference	Title	Country
10116	Cyber Sentinels: Harnessing Deep Packet Inspection for Real-Time Defense of Substation	France
10223	System-Level Factors Influencing AGC Cyber-Attack Success and RAS Vulnerability in Multi-Area Grids	United States of America
10309	Cyber Security of Digital Substations: Cyber Threats Identification and Mitigation Evaluation	Netherlands
10665	Study of Cybersecurity in Power Automation: Implementation Challenges of IEC 62351 for IEC 61850 Systems	India
10667	DigiTEL CyberTwin: Integrating Digital Twin and Cybersecurity for Enhanced Situational Awareness in Critical Electrical Substations	Romania
10677	Cybersecurity Design Considerations for Offshore Wind Energy Facilities Based on IEC 62443	United States of America
10883	AI-Enabled Fault Detection and Cyberattack Differentiation Using ICS Kill Chain	United States of America
11145	Cybersecurity and EV Charging: Protecting the Future of e-Mobility	Italy
11176	Modified Purdue Model: Introducing the security zone concept for enhanced IT/OT convergence	South Africa
11252	Securing the Energy Transition: Cybersecurity Challenges and Solutions for Modern Digital Grids	Australia
11276	Dedicated operational technology security operations centre (OT SOC) “A specialized approach to monitoring, threat detection, and incident response tailored to OT environments”	South Africa
11403	Cybersecurity Governance and Performance Evaluation in the Largest Special Protection Scheme in Brazil: A Real-World IEC 61850-Based Multi-Company Architecture	Brazil
11405	Application of Artificial Intelligence for Real-Time Intrusion and Anomaly Detection in Industrial Control Systems	Brazil
11435	SASMaker: A Framework for Generating Synthetic IEC 61850 Traffic from Diverse Substation Setups	Sweden

11575	An Adaptive Cybersecurity Vulnerability Assessment Method for Power Systems Using Knowledge Graphs and Fuzzy Logic	China
11643	Automating IEC62443-4-2 Conformity Assessment for Substation control systems: raising Cybersecurity to the Next Level	Spain
11779	A Standards-Based Cybersecurity Framework for Substation Automation Design: Applying IEC 61850, 62351, 62443, and Lessons Learned from Real-World Events	Paraguay
11801	Designing SCADA Architectures for Scalability, Cybersecurity and Digital Resilience	Croatia
11957	Operational Integration and Customization of a SIEM System in ANDE's OT Network	Paraguay
11958	Modernizing the ANDE SCADA Control Center Infrastructure with HCI and SDN: A Strategy for Resilience and Cybersecurity in OT Environments	Paraguay
11969	Securing Grid Connectivity with Quantum-Safe IPsec	Canada
12100	Securing IEC 60870-5-104 and DNP3 over IP with IEC 62351: Application and Transport Layer Security	South Africa
12133	Protecting Critical Power Infrastructure: A Cybersecurity Architecture for Electric Grid Protection Systems	Colombia
12215	Mitigating Cyberattack Risks in Digital Substations Using a Cybersecurity Model	Colombia
12386	Stress testing power systems' systemic resilience against cyber-attacks	Germany
12394	VERISBERT: Exploring darkBERT’s Capabilities for Cyber Threat Intelligence in Critical Infrastructure	Paraguay
12533	Experience implementing IEC 62443 cybersecurity requirements in hybrid Battery/Solar power plant	Ireland
12642	A Room-Temperature Quantum Secure ROCOF for Power Grid Reliability	Serbia

Table 3 - Papers for PS2

Paper 10116 presents a hardware-based Substation Real-time Intrusion Prevention Module (SRIM) for protecting IEC 61850 process bus communications. Implemented as an FPGA-accelerated SFP module, it performs protocol-aware deep packet inspection at line rate. It demonstrates that inline intrusion prevention can meet microsecond-level latency requirements without disrupting protection and control traffic.

Paper 10223 examines how system-level parameters influence the success of cyber-attacks on automatic generation control in multi-area grids. It uses a feedback-based attack policy and a large parametric sweep to identify vulnerable combinations of inertia, AGC capacity, tie-line loading, update rate, and load damping, with the results validated in a three-area phasor-domain simulation that includes remedial action schemes.

Paper 10309 evaluates cybersecurity threats and mitigation options for IEC 61850-based digital substations. It compares standardized and emerging approaches for GOOSE, Sampled Values, MMS, and PTP communications. It proposes a crypto-agile blueprint that combines segmentation, PRP-based reliability, TLS for MMS, and AAA proxy functions.

Paper 10665 reviews implementation challenges of IEC 62351 cybersecurity for IEC 61850 systems. Using a realistic laboratory testbed and bump-in-the-wire solutions, the paper quantifies effects such as latency, recovery time, message loss, and operator diagnostic effort, showing that operational manageability is often as important as cryptographic performance.

Paper 10667 introduces DigiTEL CyberTwin, a cyber-physical digital twin for high-voltage substations. It links passive OT cybersecurity monitoring to a spatial digital twin, enabling vulnerabilities, communication dependencies, and alerts to be interpreted in relation to physical assets and operational roles.

Paper 10677 addresses cybersecurity design for offshore wind facilities using IEC 62443. It focuses on zones and conduits, target security levels, defense-in-depth, secure remote access, DMZs, redundancy, and hardening adapted to offshore wind's distributed topology, wide-area communications, and limited physical access.

Paper 10883 proposes AI-enabled detection of physical faults and cyberattacks in smart grids using the ICS Kill Chain. By combining deep learning applied to electrical measurements and IEC 61850 GOOSE data with LLM-based reasoning, the framework supports classification of physical, cyber, and hybrid events, attack-stage mapping, and human-supervised incident response planning.

Paper 11145 describes a monitoring and anomaly-detection platform for electric vehicle charging infrastructure. It combines real-time traffic monitoring, AI-based detection, support for OCPP and IEC 61850, and synthetic OCPP traffic generated using a W-GAN/LSTM approach, validated on a multi-vendor EV charging testbed against anomalies and DDoS attacks.

Paper 11176 discusses a modified Purdue Model for managing IT/OT convergence in large OT environments. It introduces a Security Zone concept that separates OT and IT DMZ functions, using controlled session-based links, Zero Trust principles, policy enforcement points, OT-specific IAM, jump servers, and monitoring tools to reduce lateral movement and clarify accountability.

Paper 11252 reviews cybersecurity challenges in modern digital grids and substations. It focuses on legacy protocols, IBR-related access points, constrained field equipment, IT/OT organizational gaps, and practical mitigation measures validated in a digital substation testbed, including segmentation, relay hardening, firewalls and role-based access control.

Paper 11276 makes the case for a dedicated OT Security Operations Center for power utilities. It describes a distributed model with local OT SOC nodes coordinated by a global OT SOC, emphasizing OT-aware analysts, specialized monitoring, managed OT/IT data sharing and incident-response playbooks aligned with safety, availability and regulatory requirements.

Paper 11403 presents cybersecurity governance and performance evaluation for Brazil's large SEP N-NE-SE special protection scheme. It focuses on a multi-utility IEC 61850 Layer-2 wide-area architecture using segregated protection, monitoring and supervision networks, dedicated MPLS-TP tunnels, whitelist-based GOOSE security, rate limiting and end-to-end validation of approximately 40 ms corrective actions.

Paper 11405 examines the use of AI for real-time intrusion and anomaly detection in industrial control systems. It integrates AI into the iCPS cybersecurity methodology, combining continuous observation, contextual analysis, response and validation to reduce false positives and improve detection and response times in OT environments.

Paper 11435 introduces SASMaker, an open-source framework for generating synthetic IEC 61850 GOOSE traffic datasets. Linking power-system simulation with IEC 61850

communication behavior produces standard-compliant PCAP traces that preserve protection-event behavior and can support machine-learning intrusion detection where real substation datasets are scarce.

Paper 11575 proposes an adaptive vulnerability assessment method for power systems using knowledge graphs and cascaded fuzzy logic. It improves on CVSS by extracting features from vulnerability texts, producing continuous severity scores, and adapting risk evaluation to changing power-system operational scenarios.

Paper 11643 presents Cyber Test Box, a portable platform for automating IEC 62443-4-2 conformity assessment of substation IEDs and station control units. It can operate in laboratory or autonomous mode, virtualizing required services such as PKI, LDAP, syslog, and NTP to reduce manual testing effort and support consistent cybersecurity evaluation across manufacturers.

Paper 11779 proposes a standards-based methodology for initial cybersecurity assessment of IEC 61850 substations. It combines IEC 61850, IEC 62351, and IEC 62443 with lessons from real incidents to support segmentation, risk-based control prioritization, and validation against recurring human, organizational, and architectural weaknesses.

Paper 11801 discusses lessons from designing scalable, cybersecure, and resilient SCADA/EMS/DMS architectures. It emphasizes modernization under NIS2 and NCCS expectations, careful treatment of legacy assets, OT-specific security controls, FAT/SAT cybersecurity testing, lifecycle patching, disaster recovery, monitoring and periodic vulnerability assessments.

Paper 11957 presents the operational integration and customization of a SIEM system in ANDE's OT network. The work focuses on the progressive integration of SCADA, WAMPAC, firewall, and network device logs using secure protocols, with tailored dashboards, queries, alerting, Active Directory integration, and contextual asset organization to improve security visibility and incident analysis.

Paper 11958 describes the modernization of ANDE's SCADA control center using hyperconverged infrastructure and software-defined networking. The solution improves resilience through live migration and rapid recovery. At the same time, SDN microsegmentation applies IEC 62443 zones and conduits to limit lateral movement and support defense-in-depth and Zero Trust principles.

Paper 11969 discusses how to prepare utility communication networks for quantum-era threats by applying quantum-safe IPsec at the network layer. It highlights how network-layer encryption can protect legacy IEDs, SCADA systems, and inter-entity communications without requiring replacement of field devices, while maintaining operational continuity and performance. The paper positions IPsec, together with MACsec and other layered protections, as a practical path for securing grid connectivity against both classical and future quantum attacks.

Paper 12100 examines the cybersecurity of IEC 60870-5-104 SCADA communications and the role of IEC 62351 in addressing protocol weaknesses. It combines application- and transport-layer security measures with an AI-based intrusion detection model for threats such as spoofing, replay, message modification, and eavesdropping, providing practical guidance for utilities operating IP-based SCADA systems.

Paper 12133 presents a cybersecurity architecture for electric grid protection systems in Colombia. The paper uses ICS Cyber Kill Chain, MITRE ATT&CK for ICS, and national tools for high-impact scenario analysis to identify weaknesses in protection architectures and propose layered mitigations such as IEC 62443 zones and conduits, RBAC, encrypted channels, secure remote access, OT SOC monitoring, and dedicated attention to IEC 61850 traffic and timing synchronization.

Paper 12215 describes a standards-based model for mitigating cyberattack risks in IEC 61850 digital substations. It validates preventive, detective, and segmentation controls in a laboratory environment, showing a significant reduction in high-risk scenarios such as GOOSE false data injection, PTP denial-of-service, unauthorized SCADA access, and sampled-value manipulation.

Paper 12386 proposes simulation-based stress testing to evaluate the systemic resilience of power systems against cyber-attacks. It adapts a concept familiar in the banking sector to power grids, with examples involving internet-connected DERs and analyses of impacts such as inter-area oscillations and voltage-band violations, thereby supporting regulators and utilities in comparing cyber and physical defense measures.

Paper 12394 introduces VERISBERT, a transformer-based approach for extracting structured cyber threat intelligence from incident narratives. By fine-tuning a cyber-domain language model to identify VERIS-aligned ACTOR, ACTION and ASSET entities, the paper shows how critical-infrastructure incident reports can be converted into more consistent, machine-readable information for analyst review and future SOC workflows.

Paper 12533 shares practical experience from implementing IEC 62443 cybersecurity requirements in hybrid battery/solar and other renewable generation sites. It focuses on project delivery challenges, including IEC 61850 interoperability, SCADA security, supplier coordination, remote operation requirements, risk assessment, zones and conduits, DMZ design, and the need to address cybersecurity early in procurement and engineering.

Paper 12642 presents a quantum-secured ROCOF protection concept for low-inertia power grids with high penetration of inverter-based resources. It combines room-temperature quantum key distribution with lightweight HMAC authentication of IEC 61850 GOOSE-based trip signals, demonstrating in hardware-in-the-loop tests that fast protection messaging can be protected against manipulation and quantum-channel eavesdropping without compromising the timing requirements of ROCOF schemes.

Discussion and Questions

PS2 papers may be grouped into the following sub-topics:

A) Securing digital substations and industrial control systems for power utility applications
B) Cyber Security standards, compliance, governance and security architecture for critical power utility environments
C) Advanced detection, analytics and next generation technologies for resilient utility Cyber Security

A) Securing digital substations and industrial control systems for power utility applications

Relevant papers: 10116, 10223, 10309, 11145, 11252, 11276, 11957, 11958, 12215, 12386

Q2.01 As utilities adopt IEC 61850 and move towards highly interconnected digital substations, cybersecurity is a requirement that can impact reliability, safety and operations. How can power utilities secure IEC 61850 based digital substations in real time without compromising the latency, availability and deterministic requirements of protection critical operations?

Q2.02 As power systems become more interconnected and digital, it is important to understand how the operating conditions of control systems and protection schemes respond to cyber-attack. What are the key risks that require attention and what should be the main focus area for the industry?

Q2.03 Traditional cyber security controls such as firewalls, segmentation and passive monitoring are important but may not be sufficient in digital substation environments. How can utilities overcome the limitations of conventional cyber security controls in digital substations without increasing the complexity?

Q2.04 EV charging infrastructure is becoming more widely connected, data-driven and integrated with wider energy systems. What approaches are likely to be most effective in addressing the cyber security threats facing these systems?

Q2.05 The growing use of digital communications and intelligent electronic devices in substations is expanding the cyber-attack surface of protection and control systems. How are organisations testing and validating cybersecurity controls in these environments to ensure operation performance is preserved?

Q2.06 OT environments prioritise safety, reliability and availability, which means cyber monitoring and incident response must be designed differently from standard IT security operations. How should a SOC be coordinated across IT and OT systems to improve visibility, response and resilience?

Q2.07 Security Information and Event Management (SIEM) systems are being adopted to improve the visibility, monitoring and incident response to cyber security threats. How are organisations approaching the deployment of SIEM platforms to meet the specific operational, technical and security requirements OT environments?

Q2.08 Many utility SCADA environments contain a mix of legacy and modern technologies making security upgrades technically difficult, slow and expensive. What are ways to improve cyber security in SCADA systems that are unable to be fully replaced or redesigned in the short term?

Q2.09 Digital substations are becoming more reliant on IEC 61850 based communications and interconnected systems and applying practical and standards aligned cybersecurity controls is important. Discuss approaches to the assessment, validation and implementation of

cybersecurity measures for these environments.

B) Cyber Security standards, compliance, governance and security architecture for critical power utility environments

Relevant papers: 10665, 10667, 11176, 11403, 11643, 11779, 11801, 12100, 12133, 12533

Q2.10 As power systems become more connected, utilities can no longer rely on the assumption that OT networks are isolated and therefore secure. How should utilities decide which cyber security controls are proportionate, practical and worth prioritising?

Q2.11 The classic Purdue model was designed for a time where OT and IT were more isolated. Modern utilities now require data sharing, remote access and integrated cyber security functions. How can utilities modernise OT/IT segmentation to improve cyber security without introducing unacceptable risk?

Q2.12 Multi-operator energy systems require multiple organisations to share data, trust boundaries, and operational responsibilities. How can cyber security governance be structured effectively across multiple organisations?

Q2.13 Zero Trust concepts are increasingly being adapted for OT, but their assumptions do not always align neatly with availability and latency requirements of OT systems. How can zero trust principles be realistically applied to OT systems?

Q2.14 Cyber security requirements for IEDs and substation automation systems continue to expand. How can utilities use automated cyber security testing to improve assurance, consistency and deployment readiness?

Q2.15 The CTB demonstrates a strong focus on IEC 62443-4-2 component-level security testing, particularly across authentication, communication, and logging functions. Given that many of these controls are implemented within power system communication protocols (e.g., IEC 61850, IEC 60870-5), how do you envision integrating or validating IEC 62351-specific security mechanisms within the CTB, such as secure profiles, message authentication, and encrypted communications, to ensure protocol-level cybersecurity assurance alongside component-level compliance?

Q2.16 The proposed methodology highlights the importance of risk-based segmentation and validation against real-world cyber incidents, particularly emphasizing human-mediated attack vectors and architectural weaknesses.
In practical substation projects, where design constraints, legacy systems, and vendor-specific architectures often limit ideal segmentation and control implementation, how do you foresee adapting this methodology to ensure that the derived cybersecurity criteria and target security levels remain both achievable and effective in real-world deployments?

Q2.17 The paper emphasises a lifecycle-based approach combining architecture design, rigorous testing, and continuous operational security management in SCADA environments. Given the inherent constraints of legacy systems, long asset lifecycles, and strict availability requirements, how do you prioritise and phase the implementation of cybersecurity controls in

a way that achieves measurable risk reduction without introducing unacceptable operational or system stability risks?

Q2.18 The paper demonstrates that combining IEC 62351 security mechanisms with AI-based intrusion detection can significantly enhance the security of IEC 60870-5-104 communications. From a practical deployment perspective, how do you foresee balancing the computational and operational overhead of real-time AI-based intrusion detection with the strict latency and availability requirements of SCADA systems in live utility environments?

Q2.19 Given the stringent timing and reliability requirements of protection systems, what trade-offs or design strategies are necessary to ensure that multi-layered cybersecurity controls can be realistically implemented without introducing unacceptable operational risks?

Q2.20 The paper highlights that many implementation challenges arise from late integration of cybersecurity requirements and misalignment with the EPC project lifecycle. In practice, what governance or project management approaches can be used to ensure that cybersecurity—particularly risk assessment and architecture decisions—is effectively embedded from the early design stages?

C) Advanced detection, analytics and next generation technologies for resilient utility cyber security

Relevant papers: 10677, 10883, 11405, 11435, 11575, 11969, 12394, 12642

Q2.21 Considering both the need for quantum-safe network encryption and the requirement for ultra-fast, secure protection signalling, what practical implementation strategies can utilities adopt to integrate these solutions across communication and protection layers while preserving interoperability, scalability, and strict real-time performance constraints?

Q2.22 Given the need to accurately distinguish between physical faults, cyber incidents, and hybrid events in increasingly complex digital substations, what practical approaches can be used to integrate AI-driven detection with operational context and ICS Kill Chain analysis in a way that improves decision-making while maintaining trust, explainability, and operational reliability?

Q2.23 Considering the growing reliance on data-driven cybersecurity in IEC 61850 environments, how can utilities ensure that synthetic data generation and AI-based threat intelligence extraction are effectively integrated into a cohesive workflow that supports reliable

intrusion detection, accurate situational awareness, and practical decision-making in real-world operations?

Q2.24 In increasingly complex and distributed power system environments, how can utilities effectively align secure-by-design architectural approaches with adaptive, context-aware vulnerability assessment methods to ensure that cybersecurity controls remain both operationally practical and responsive to dynamic risk conditions?

Preferential Subject 3 (PS 3) - Next-generation telecommunications technologies to support grid decarbonisation and digitalisation

The decarbonization and digitalization of power generation, transmission and distribution are driving significant changes in EPU telecommunication networks. The increasing integration of new substations to interconnect distributed energy resources like renewables poses several challenges when it comes to scalability, especially with legacy network deployments. Modern operational telecom backbone networks must offer the flexibility to expand efficiently and rapidly without impacting the reliability of it.

The transition from legacy to packet-based networks must be achieved without compromising the stringent requirements of protection, automation, control and operational communications while offering coexistence of old and new systems during phased implementation, alongside robust strategies for maintaining wide-area precision time synchronization.

Wireless and hybrid communication solutions, including private LTE, 5G, microwave, industrial wireless and other technologies that can complement fiber-based networks, extend communications to remote assets, and improve flexibility and resilience.

Finally, as EPC telecommunications become more complex, there is a critical need for improved network management, monitoring and automation. Bridging the gap between agile IT networks and deterministic OT environments demands advanced, multi-vendor operational support to ensure highly resilient, mission-critical power grids.

A total of 45 papers were accepted within the SC D2 PS 2:

Paper Reference	Title	Country
10333	Segment Routing for Differential Protection: Transport Network Evolution and Field Validation for C37.94 Applications in High Power Substations	France
10349	A proven & optimised approach to Network transformation of legacy networks to next generation technologies	Australia
10401	Field Deployment of Hybrid Microwave Technology for DSO in Queensland for Transporting Mission Critical Tele-protection and SCADA services through lab testing	Australia

10486	The Importance of Automation Systems in the Electrical Interconnection between Brazil, Paraguay, and Argentina: Challenges and Perspectives	Argentina
10543	Transition to Packet Networks	India
10544	Implementation of OSTP Amplifier Solution with ROPA Technology and its operational experience	India
10545	Unified Network Management System (UNMS) for Power SyStem Communication Network: A Roadmap for Future Grid Communication Management	India
10547	Migration Strategy from TDM to IP/MPLS in Utilities : A Roadmap and Lessons Learnt	India
10549	Packet-Based Power: Enabling Grid Decarbonisation through Next Generation Telecommunications	India
10550	Automation and Artificial Intelligence by OT Network Operations Center in Power utility	India
10885	Supporting Routed GOOSE (R-GOOSE) Traffic over IP/MPLS Using Multicast VPNs	United States of America
10933	Private LTE 450 MHz wireless network for MV Teleprotection	France
10934	Enhancing Resilience in Critical Applications through hybrid Optical and PLTE Networks	France
10935	Use of co-simulation for zonal congestion management systems to assess the resiliency of the associated ICT infrastructure and validate their performances under communications hazards	France
11003	Evaluating transmission performance for migration from SDH/PDH networks to MPLS-TP and IP networks	Japan
11004	Field Evaluation of diverse Communication Methods for supporting smart Maintenance in remote hydroelectric Power Facilities	Japan
11005	Application of All-Photonics Network (APN) for Power Communication	Japan
11006	Migration To The Next-Gen Packet-Based Transport Network: Enabling IP-Based Power Control Applications of Tomorrow	Japan
11007	Realisation of a resilient Packet-based Network over Wireless Microwave Technology	Japan
11008	Case Study of Legacy Communication Migration to IP Networks in Japan	Japan
11009	Measurement of PTP Synchronization Accuracy and Study of its Application to IP Networks of Japanese TSOs	Japan
11010	An Example of Building and Using a Smart Safety Network Using Private 5G/Wi-Fi	Japan
11047	Deployment of multipoint grid control applications over mixed communication networks using protection signaling devices	France
11168	A hybrid OSS framework for utility telecommunications: Bridging operational technology and information technology service management	South Africa

11177	Optimizing IP based SCADA IEC 60870-5-104 protocol performance through adaptive machine learning driven traffic shaping in classical computing environments	South Africa
11234	Transition to SCADA/EMS Cloud Architecture in Big Power Systems in the Light of Present-Day Challenges and Cybersecurity Requirements	Russia
11238	Adaptive OFDM PLC Technology as a Tool for Automation of Distribution Electrical Networks and Monitoring the State of Power Cable Systems and Overhead Lines	Russia
11275	Line differential protection over packet-switched network: performance and considerations in South Africa	South Africa
11343	5G-Enabled Smart Grid IoT: Architecture, Use Cases, Challenges & Solutions	Sweden
11378	Benchmarking Line Differential Protection under emerging Communication Infrastructures	Finland
11379	Pilot project: Line differential protection over Ethernet	Sweden
11394	Upgrading Argentina's 500 kV Transmission Network: From Legacy SDH Microwave to Hybrid TDM/Packet Systems for Enhanced Reliability	Argentina
11406	IEC61850 based PACS network automation enabled via Intent-Based Networking	Brazil
11436	Protection automation and control using private 5G: Use-case evaluations for fully digital substations	Sweden
11576	Research on passive and semi-passive P-IoT sensing for UHV equipment monitoring based on energy harvesting and low-power wireless communication	China
11577	Research and Deployment of IPv6+ and SDN Technologies for Smart Grid Data Networks	China
11644	Implementation and Deployment of Multiprotocol Services into a MPLS Critical Infrastructure Network	Spain
11645	Real-Time IDS for Digital Substations: From Lab to Field Deployment	Spain
11852	A Universal Gateway for IoT-Driven Power Infrastructure for SCADA Integration	United Kingdom
12026	Protection relays using 5G for inter-substation communication to enhance selectivity	Sweden
12109	Digital Transformation in Substations Using Mesh Networks: Telecommunications Infrastructure for the Advanced Monitoring Era	Colombia
12208	Real-life case of Routable-GOOSE over MPLS-TP: Implementation, Testing and Validation at Tele-protection Santa Rosa-Carapongo 220 kV line in Perú	Peru
12340	Field Experience Report of using Process Bus over Substation Boundaries with multi-vendor line differential Protection	Switzerland
12341	Field Experience Report of hybrid Distance Protection Solution using IEC 61850 GOOSE Gateway	Switzerland

12344	Segment Routing for Differential Protection: Transport Network Evolution and Field Validation for C37.94 Applications in High Power Substations	Switzerland

Table 4 - Papers for PS3

PS3 papers may be grouped into the following sub-topics:

1) Optimized migration approach from legacy to packet networks to support mission-critical power systems services
2) Next-generation technologies in enhancing coverage and resilience of wireless communication networks for power systems
3) Telecommunications technologies and techniques for a highly resilient and mission critical power system

1) Optimized migration approach from legacy to packet networks to support mission-critical power systems services

Paper 10333 shows how utility transport networks can shift from IP/MPLS to Segment Routing for current differential protection using C37.94 interfaces. Field validation of ELFEC's 115 kV backbone in Bolivia confirms that Segment Routing can deliver resilient, protection-grade wide-area communications, with testing covering latency, failover, active multipath, quality of service, and MPLS encryption.

Paper 10349 outlines a practical roadmap for moving legacy operational telecom networks to next-generation packet technologies. Drawing on TSO and DSO experience in Australia and the United Kingdom, this approach highlights a phased approach—requirements gathering, technical study, laboratory validation, and acceptance testing—to migrate mission-critical services with minimal disruption.

Paper 10543 captures an Indian transmission utility's shift from SDH/SONET and TDM to packet transport networks. Experience across roughly 250 substations shows that IP/MPLS and MPLS-TP can improve bandwidth, centralize monitoring, and sustain network availability above 99.9% while continuing to support protection and SCADA services.

Paper 10547 shares field lessons from migrating utility communication rings from SDH-based TDM to IP/MPLS. It focuses on maintaining service continuity during partial ring migration, using protected Ethernet paths, clear SDH/IP/MPLS boundary definitions and bidirectional optical transceivers to allow legacy and packet rings to coexist over the same fiber infrastructure.

Paper 10549 provides a framework for packet-based telecommunications that support grid decarbonization and digitalization. It contrasts MPLS-TP and IP/MPLS for deterministic utility services and shows how MPLS-TP cores, circuit emulation, quality of service engineering, and private 5G edges can support teleprotection, SCADA, and IEC 61850 GOOSE traffic in future grids.

Paper 11003 tests Pseudo Wire Emulation Edge-to-Edge over MPLS-TP and IP as a practical migration path from SDH/PDH. Results with a protection relay, analog telephone, and remote supervisory-control device show that packet networks can meet transmission-delay requirements for legacy utility applications.

Paper 11006 presents a proof of concept for MPLS-TP as a next-generation packet transport technology for Japanese power-control applications. It examines enhanced delay control, guaranteed bandwidth, interworking with PDH systems, and interoperability with IP-based line differential protection relays, confirming that strict delay and differential-delay requirements can be satisfied.

Paper 11008 presents a Japanese case study on migrating analog monitoring and control lines to IP networks. Covering around 900 sites, the approach uses IP converters, dual independent IP networks, and jitter-buffer delay compensation to maintain E&M, FXS, and FXO services while reducing dependence on aging TDM equipment and lowering future operational workload.

Paper 11394 presents the upgrade of Argentina's 500 kV transmission communication network from legacy SDH microwave equipment to hybrid TDM/packet systems. It focuses on maintaining coexistence during migration, carrying mission-critical services such as line protection, SCADA, and synchrophasors, and using MPLS-TP over microwave to combine deterministic performance with new data-intensive applications.

Paper 11644 describes how the Spanish TSO has built multiprotocol services into an MPLS critical-infrastructure network. VPRNs, circuit emulation, IEEE 1588 time synchronization, quality of service, firewalls, and whitelisting are combined to migrate legacy TDM services while supporting teleprotection, telemanagement, video, VoIP, and other operational applications on a resilient multiservice platform.

Discussion and Questions

Relevant papers: 10349, 10543, 10547, 11006, 11008

Q3.01 Many utilities require a hybrid solution in which legacy TDM-based systems like SDH and PDH with packet-based networks must coexist for an extended transition period. Which approach ensures service continuity without impacting the performance of the protection applications and avoids excessive complexity and duplication of infrastructure?

Relevant papers: 10333, 10349, 10547, 10549, 11003, 11006

Q3.02 Ít is of vital importance to validate the packet-based transport networks for mission-critical services such as current differential protection before deployment because if its nondeterministic behavior. Which test methodology is best suited for utilities to demonstrate that latency, asymmetry, jitter and failover performance are meeting the stringent power utility requirements and are acceptable for live operation?

Relevant papers: 10333, 10543, 10549, 11003, 11006

Q3.03 New packet-network options are emerging, next to MPLS-TP / IP/MPLS we see now the introduction of SR-MPLS and SRv6 for mission critical OT networks. Do these new technologies meet the requirements for the most critical power utility traffic and which technologies support both legacy TDM-based teleprotection services in combination with packed-based protection and automation applications?

Relevant papers: 10349, 10543, 10549, 11006, 11008

Q3.04 Network migration is not only a matter of transporting data, but also a question of timing, cybersecurity and workforce readiness. What is the best approach for utilities to integrate synchronization, cybersecurity, legacy compatibility, and operations skills into a migration roadmap so that the transition to packet-based networks doesn't introduce new vulnerabilities or performance issues?

Relevant papers: 11394, 11644

Q3.05 When migrating your mission-critical teleprotection services, are you leaning toward TDM circuit emulation over your new MPLS networks, or are you utilizing hybrid transport equipment to keep TDM native until the end devices are upgraded to Ethernet? What operational challenges have you faced with either approach regarding latency, jitter, or asymmetry?

Q3.06 With the phase-out of SDH, synchronization is moving from the physical layer to packet-based protocols like IEEE 1588 PTP. How are your organizations redesigning your synchronization planes? Are you relying heavily on PTP to achieve the microsecond accuracy required for future IP-based differential protections and Sampled Values, or are you deploying localized GPS/GNSS clocks at every substation?

2) Next-generation technologies in enhancing coverage and resilience of wireless communication networks for power systems

Paper 10401 details preparation for deploying hybrid microwave technology for a Queensland DSO. The laboratory work validates a TDM-plus-packet microwave platform for teleprotection and SCADA, covering interoperability with existing PDH multiplexers, latency and asymmetrical delay, radio protection configurations and payload encryption.

Paper 10933 assesses private LTE in the 450 MHz band as a resilient wireless option for medium-voltage teleprotection. EDF's R&D work tests whether LTE 450 MHz can meet the low-latency, reliable and deterministic requirements of islanded DSO systems, offering a potential alternative to public mobile networks and costly fibre deployment.

Paper 10934 presents a hybrid communication architecture combining optical MPLS-TP links with Private LTE backup paths for critical DSO applications. The laboratory implementation evaluates latency, delay symmetry, packet loss, and failover time, providing evidence that combining optical and wireless technologies can improve resilience where a single communication medium is insufficient.

Paper 11004 reports field testing of communication technologies for smart maintenance at remote hydroelectric facilities. SHDSL, VDSL2, high-speed PLC, and Wi-Fi HaLow are assessed for use with existing cables or difficult terrain, and the paper proposes a selection flowchart to match each technology to site conditions such as cable availability, distance, and wireless coverage.

Paper 11007 continues previous work on resilient packet-based networking over wireless microwave links. Using actual microwave radio and MPLS-TP equipment, the study verifies legacy-service migration, protection switching, bandwidth utilization, and communication behavior under simulated weather-related radio degradation.

Paper 11010 describes a smart safety wireless network for power stations built on Private 5G outdoors and Wi-Fi indoors. Practical results across multiple sites show how the approach can support smart safety devices while addressing wireless performance, interference coordination, security, and efficient deployment.

Paper 11343 frames 5G as an enabling architecture for smart-grid IoT. It links URLLC, eMBB, and massive machine-type communication to use cases such as wide-area protection, distribution automation, AMI data streams, video monitoring, and DER orchestration, while also considering hybrid CPE, mesh extension, and fallback options for legacy or remote devices.

Paper 11436 evaluates private 5G for protection automation and control in fully digital substations. Hardware-in-the-loop tests with real PACS devices, process interface units, SV, and GOOSE traffic show that present 5G configurations can transport such traffic, but latency remains too high for the fastest protection functions; less time-critical GOOSE-based applications appear more feasible in the near term.

Paper 11576 introduces a passive and semi-passive IoT sensing system for monitoring UHV equipment. Using electromagnetic and solar energy harvesting, the solution avoids batteries and combines MEMS temperature sensors with OOK backscatter and semi-passive BPSK communication, achieving stable field communication and accurate temperature tracking under severe electromagnetic conditions.

Paper 12026 studies the use of 5G for inter-substation teleprotection in medium-voltage radial networks. GOOSE blocking signals were transported via VXLAN over public 5G NSA and SA networks and a laboratory 5G-SA cell; after accounting for background traffic and 5Qi prioritization, 5G-SA met the 100 ms selectivity requirement, while 5G-NSA exhibited tail latency unsuitable for reliable protection use.

Discussion and Questions

Relevant papers: 10401, 10933, 10934, 11004, 11007, 11010

Q3.07 Multiple wireless technologies like Microwave, Private LTE/5G, 450Mhz and Wi-FI HaLow are being evaluated to address several power utility use cases. Which requirements must be met to determine which wireless technology, or combination of technologies, is best suited for their applications according to to latency, coverage, resilience, and operational criticality?

Relevant papers: 10401, 10933, 10934, 11007, 11010

Q3.08 As not all services have the same tolerance to performance variation, wireless technologies need to be carefully evaluated for each type of service. For which applications can wireless be entrusted for their primary path, backup path, and are there any applications that must remain on the fixed network?

Relevant papers: 10933, 10934, 11004, 11007, 11010

Q3.09 Electric power utilities are expanding private wireless networks, hence there is a need to balance to balance the resilience, ownership, scalability and cost. Which provides the most long-term sustainable model for the power utility wireless infrastructure? Fully private networks, hybrid fiber-wireless architectures, selective use of public networks or a combination of the above?

Relevant papers: 11436, 12026

Q3.10 How are different grid operators defining the performance boundaries between public and private 5G deployments for critical protection? Which specific control schemes have proven successful over cellular links, and where your organizations are drawing the hard line on what must remain on physical fiber.

Relevant papers: 11343, 12026

Q3.11 When integrating legacy serial protocols or non-routable Layer-2 traffic like GOOSE over Layer-3 wireless domains, what architectural approaches is your organization adopting at the edge? How can your organization balance the use of software encapsulation methods, like VXLAN, versus deploying multi-protocol hybrid gateways.

Relevant papers: 11343, 11576

Q3.12 Scaling up asset monitoring in UHV switchyards introduces severe challenges with electromagnetic interference and edge battery management. What alternative sensing architectures, such as Passive IoT or backscatter technologies, are you exploring, and how do their field deployments compare to traditional active cellular IoT sensors in your experience?

3) Telecommunications technologies and techniques for a highly resilient and mission critical power system

Paper 10486 sets out the automation requirements for the 500 kV interconnection between Argentina, Brazil, and Paraguay. Its main focus is the transition from point-to-point teleprotection to IEC 61850-90-1-based R-GOOSE and R-SV wide-area control, with a strong emphasis on latency, jitter, multi-vendor interoperability, PTP synchronization, and cross-border cybersecurity.

Paper 10544 presents the first POWERGRID deployment of an Optical Services Transport Platform using Remote Optically Pumped Amplifier technology on the Raigarh-Pugalur HVDC communication link. The solution combines ROPA, Raman amplification, and EDFA to avoid intermediate repeater stations, achieving sufficient gain margin and more than three years of successful operation.

Paper 10545 introduces a Unified Network Management System for the Southern Region power communication network in India. As a manager-of-managers platform, it brings multi-vendor SDH, PDH, OPGW, PLCC, VSAT, and MPLS/IP systems into one operational view, improving alarm correlation, inventory and topology management, circuit provisioning, availability reporting, and fault isolation.

Paper 10550 describes the implementation of an OT Network Operations Centre with automation and AI/ML capabilities at Tata Power in Mumbai. The solution consolidates monitoring of multi-vendor communication, cybersecurity, fibre, MPLS-TP, SDH and teleprotection systems on a centralized dashboard, reducing the effort required for fault analysis and restoration.

Paper 10885 explains how Routed GOOSE can run over IP/MPLS using multicast VPNs. The paper's core contribution is a scalable approach to wide-area protection and control messaging that preserves deterministic multicast behavior, traffic isolation, quality of service, rapid recovery and cybersecurity.

Paper 10935 describes co-simulation platforms for assessing the ICT resilience of zonal congestion-management systems. By coupling electric-network simulation, telecontrol-network simulation and controller simulation, the work evaluates whether existing communication infrastructures can support real-time renewable curtailment controls and how alternative architectures behave under telecommunications hazards.

Paper 11005 explores the application of All-Photonics Network technology to power utility communications. Long-term field verification over in-service OPGW shows that even lightning-related polarization changes did not degrade post-FEC performance, suggesting APN as a promising low-latency, high-capacity successor for teleprotection and future data-intensive grid applications.

Paper 11009 investigates the accuracy of Precision Time Protocol synchronization in IP networks used by Japanese TSOs. It compares delay mechanisms, one-step and two-step operation, switch capabilities, and traffic-load conditions, concluding that Transparent Clock or Boundary Clock functions are essential for applications such as current differential relays and PMUs, and narrowing the practical network allocation options to three promising patterns.

Paper 11047 discusses the evolution of teleprotection toward multipoint grid-control applications over mixed communication networks. It focuses on how protection signaling

devices can support wide-area protection and control, including remedial action schemes, while legacy wired I/O, TDM, IEC 61850, Ethernet, and packet-based WAN technologies coexist during long migration periods.

Paper 11168 proposes a hybrid Operational Support System framework for utility telecommunications. The paper contrasts commercial mobile-network OSS practices with utility requirements and argues for a dual-layer model: an OT-hardened core for deterministic, asset-centric and safety-critical services, combined with an IT-agile service layer for operational efficiency and digital innovation.

Paper 11177 introduces an adaptive traffic-shaping framework for IEC 60870-5-104 SCADA communication over converged IP/MPLS utility networks. It combines machine-learning traffic analysis with protocol-aware prioritization and deterministic quality of service enforcement, using DSCP marking, MPLS EXP mapping and class-based queuing to preserve low latency for critical control traffic under congestion and failure conditions.

Paper 11234 examines the transition of SCADA/EMS systems in large power systems toward cloud-based architecture. It analyses how regional dispatch-center installations could be replaced or complemented by corporate or external cloud resources, while addressing secure access, cybersecurity, operational continuity, and the need to preserve autonomy of dispatch functions during communication disturbances.

Paper 11238 positions adaptive OFDM power-line communication as a multifunctional tool for distribution-grid automation. The proposed modems support robust communication over medium- and low-voltage lines, enable condition monitoring and predictive analysis, and may also be suitable for teleprotection where latency can be kept within 20 ms.

Paper 11275 reports preliminary South African laboratory work on line differential protection over packet-switched networks. It creates virtual line-differential trip signals using both proprietary and GOOSE-based approaches and observes their behavior over IP-based communication paths, providing an initial basis for future interoperable protection solutions using existing utility telecommunications infrastructure.

Paper 11378 benchmarks line differential protection under emerging communication infrastructures. A traditional fiber-based protection approach is compared with edge-computing implementations using IEC 61850 Sampled Values and GOOSE over fixed packet networks and public 5G Standalone networks, with CHIL results showing that fixed-network implementations can perform comparably to the traditional solution.

Paper 11379 describes Vattenfall Eldistribution's pilot project for line differential protection over Ethernet. The work moves beyond serial C37.94 emulation by transporting time-tagged current phasors in UDP streams, with Precision Time Protocol distributed over the utility WAN from ground-based atomic clocks. It reports experience from laboratory and live 130 kV substation deployment.

Paper 11406 proposes the use of Intent-Based Networking for IEC 61850-based protection, automation, and control networks. By treating the SCD file as a source of network intent, the controller derives VLAN, multicast, quality of service, and PTP requirements and translates

them into multi-vendor device configurations, reducing manual engineering effort while supporting continuous assurance of GOOSE and Sampled Values traffic.

Paper 11577 presents the deployment of IPv6+ and SDN technologies in China Southern Power Grid's smart-grid data network. The approach addresses limitations of traditional MPLS networks in service visibility, SLA-aware routing, and dynamic bandwidth allocation, with implementation results demonstrating full latency compliance and significant throughput gains during traffic bursts.

Paper 11645 presents a real-time intrusion detection framework for digital substations, moving from laboratory development toward field deployment. It combines operational and laboratory IEC 61850 traffic, trains a machine-learning IDS for GOOSE-related anomalies, and embeds the model in a SecureBox device capable of real-time packet capture, feature extraction and alert forwarding.

Paper 11852 introduces an open-source universal substation gateway to integrate IoT-driven power infrastructure data with SCADA systems. Its microservice architecture, real-time database and CIM-aligned object model enable protocol conversion, data normalization, historical storage, redundancy and controlled exchange with external IoT platforms while preserving process-network security.

Paper 12109 describes the use of industrial Mesh Wi-Fi to support digital transformation in high-voltage substations. The pilot implementation provides segmented OT and IT wireless services for IoT sensors, cameras, mobile maintenance tools, and remote expert support, using VLAN separation, MAC-based access control, and WPA2/AES security to operate in a demanding electromagnetic environment.

Paper 12208 reports a real-life implementation of Routable GOOSE over MPLS-TP for teleprotection on the Santa Rosa-Carapongo 220 kV line in Peru. The work replaces a legacy PLC channel with an R-GOOSE architecture secured via IPSec/GRE tunneling and delivers faster, deterministic transfer times that meet IEC 61850 performance requirements for inter-substation protection.

Paper 12340 provides field experience with extending process bus communication beyond substation boundaries for multi-vendor line differential protection. Sampled Values, GOOSE, and PTP synchronization are transported through an operational MPLS-TP network, with VLAN segmentation and gateway demarcation supporting cybersecurity, interoperability, and several months of operation in the CKW grid.

Paper 12341 presents a hybrid migration solution for line distance protection using an IEC 61850 GOOSE gateway integrated into an MPLS-TP WAN. It connects legacy contact-based protection with modern GOOSE-based schemes, reducing transmission times and allowing CKW to modernize substations step by step without abandoning existing protection investments.

Paper 12344 validates precise time synchronization for mission-critical inter-substation protection in a multi-vendor laboratory setup. Two digital substations, PIUs, and protection IEDs from three vendors were synchronized via an MPLS-TP wide-area network using IEEE 1588, while GOOSE and Sampled Values were exchanged through proxy/gateway functions;

the tests showed stable system behavior under both synchronization and communication failure scenarios.

Discussion and Questions

Relevant papers: 10486, 10544, 10885, 11005, 11009, 11047

Q3.13 Protection, automation and control applications operate best with deterministic network behavior. The end-to-end performance should remain unaffected in hybrid communication networks Which power utility network design is the most optimal to ensure latency, time synchronization accuracy and service resilience for a mission critical WAN telecom backbone?

Relevant papers: 10486, 10885, 11009, 11047

Q3.14 GOOSE and R-GOOSE are becoming more prevalent for protection and control applications over the telecom backbone. Multicast VPN's and multipoint L2VPN's are commonly for the protocol transport. But which is the most efficient and resilient for the power utility use cases like teleprotection and multipoint control schemes for example? And how can utilities best standardize and scale these functions without creating excessive engineering complexity or undermining interoperability?

Relevant papers: 10545, 10550

Q3.15 In a multi-vendor and multi-technology utility telecom network it is becoming ever more important to have visibility and access to operational intelligence through unified management, monitoring and automation platforms. What level of centralization is required for such use case and what is an acceptable level of automation and AI driven decision making in mission critical networks?

Relevant papers: 10935, 11047

Q3.16 There is a growing interest in simulation, pre-validation and offline engineering of protection and control schemes over packet-based networks. Which tools and approach is required for system-level validation to make a thorough assessment of the service resilience and time synchronization accuracy in complex failure scenarios of the telecommunication network before deploying it on the live grid?

Relevant papers: 11275, 11378, 12208, 12340, 12341

Q3.17 As the industry shifts inter-substation protection away from dedicated serial links to shared packet-switched WANs, what is your organization's primary transition strategy? Are you pushing for native IEC 61850 WAN deployments like Routable-GOOSE and extended

Process Bus, or are you heavily relying on hybrid gateways to bridge existing conventional relays over the new IP/MPLS infrastructure?

Relevant papers: 11379, 12344

Q3.18 Distributing precise time over operational WANs requires strict mitigation strategies for potential GNSS loss or grandmaster failures. How are your organizations addressing these synchronization vulnerabilities? Please share your practices regarding required oscillator holdover durations, PTP Telecom profile tuning, and how you configure protection systems to degrade gracefully rather than immediately blocking during temporary synchronization islands.

Relevant papers: 11177, 11406, 11577

Q3.19 With the convergence of IT and critical OT traffic, traditional static QoS configurations are becoming a bottleneck. What is your utility's roadmap for automating network engineering and dynamically managing congestion? Have you piloted advanced traffic engineering concepts such as SDN-driven Segment Routing (SRv6), ML-based traffic shaping, or Intent-Based Networking driven directly by substation SCD files?

Relevant papers: 11168, 11234, 11852

Q3.20 The modernization of grid control involves integrating cloud-based SCADA/EMS architectures, hybrid OSS platforms, and microservice-driven IoT edge gateways. How is your organization managing this IT/OT convergence at the system architecture level? Please share your experiences or regulatory perspectives on mapping modern IoT data to CIM structures and hosting mission-critical control functions in cloud or advanced edge-compute environments.

Relevant papers: 12208

Q3.21 When utilities transmit time-critical binary protection signaling like R-GOOSE across a wide-area network, securing the packet transit is non-negotiable. What strategies or tunneling standards is your utility using to encrypt inter-substation protection data, and what has been your operational experience regarding the impact of cryptographic encryption latency on your total fault-clearing times?

Relevant papers: 11645

Q3.22 Moving from signature-based perimeter firewalls to active, protocol-aware anomaly detection at the substation edge is a major topic in OT security. For those who have piloted machine learning or network-behavior IDS platforms within your digital substations, what have been your experiences regarding false-positive management during grid disturbances, and how are your teams handling the processing overhead of real-time packet inspection on embedded switchyard hardware?

Relevant papers: 11238, 12190

Q3.23 As utilities look to maximize their telecommunications investments, infrastructure is increasingly being leveraged for multi-functional use. How is your organization pushing communication networks beyond simple data transport? We invite you to share your experiences with securely converging previously isolated IT and OT services onto a single

wireless network inside the substation, or utilizing physical telecom mediums for value-added grid diagnostics, such as PLC-based cable sensing.