D2 - 00

SPECIAL REPORT FOR SC D2 – INFORMATION SYSTEMS, TELECOMMUNICATIONS AND CYBERSECURITY

R. BERRYMAN, DE & J.M. SIQUEIRA, BR (PS1)
G.P. MBOUYAP, CA & H. KLIMA, AU (PS2)
A. LOUH, NL & H. DOI, JP (PS3)
Special Reporters

Victor Tan (Chair) and Joel Nouard (Secretary)

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 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.

Three Preferential Subjects are presented in this special report:

PS1: IT/OT solutions to improve the efficiency and resilience of electric power systems

- Internet of things (IoT) architectures and applications in improving the resilience of electric power systems.
- Applications and platforms of artificial intelligence, big data and analytics in operational technology.
- Improving efficiency and resilience of power utilities with cloud technologies

PS2: Cybersecurity in emerging application domains and technologies for securing energy organisations

- Cybersecurity for DER, microgrid and energy communities’ control infrastructures.
- Cybersecurity for electric vehicle charging and discharging control.
- Cybersecurity in cloud-based applications of power utilities.

joyce.meireles@ons.org.br, rachel.berryman@eliagroup.eu, amadou.louh@stedin.net, doi@criepi.denken.or.jp,

PS3: Meeting the challenges of energy transition with reliable, scalable, and efficient telecommunications networks

- Building scalable and resilient networks with management, automation and orchestration solutions and methods.
- Integration of current and new wireless technologies in meeting the requirements of power utility applications.
- Techniques and methods in building resilient networks and migrating legacy networks to support critical utility applications.

Contributors are welcome to prepare contributions in accordance with the questions raised by Special Reporters in the Special Report and add their valuable expertise to **SC D2 Group Discussion Meeting**, which will take place on:

- **Friday, August 30, 08:45-18:00 (CEST)**

The Contributors' meeting for SC D2 where the contributor attendance and timing of program is checked is going to be held on :

- **Thursday, August 29, 12:30 - 15:30 (CEST)**

IMPORTANT: only contributors who physically attend the Session at the Palais des Congrès can present their contribution(s) during the Group Discussion Meeting as well as only authors who physically attend the Session at the Palais des Congrès can make a presentation during the Posters.

Procedure for contributions:

- *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 Click here .***
- ***Contributors should upload their contribution*** *on the Registrations platform – "Contributions to Group Discussion Meetings" section - using their existing account and own credentials* ***by August 10, 2024****. Contributions uploading will be open at the end of May.*
- *Contributions should consist of: a written word version with max 1000 words per contribution, a powerpoint presentation with max 3 slides, a short summary of the contribution (3-5 sentences). A guide for contributors as well as templates and sample pages will be available on the CIGRE 2024 Session webpage/.*
- *Contributions will be made available to Study Committee Chair and Special Reporters for reviewing and comments. Contributors are encouraged to visit their account on the Registration Platform to see the result of this review. Any recommendations or changes to the contributions will be provided to the contributors by Special Reporters on the Registration Platform between* ***10th of August and 16th of August 2024****.*
- *All contributors with accepted/finalised contributions will be contacted by the Special reporters of SC D2 by email between* ***10th of August and 16th of August 2024****, to finalize the presentation and receive the instructions regarding the session.*
- *Deadline for sending the poster session for your paper is* ***10th of August 2024****. SC D2 Poster Session will be held on* ***Thursday, August 29, 14:00 - 18:00 (CEST).*** *SC D2 Poster Session Convener is* ***Olga Sinenko*** *(olga.sinenko_scd2@rtsoft.ru).*

Preferential Subject 1 (PS1): IT/OT solutions to improve the efficiency and resilience of electric power systems

Introduction

As the power grid continuously evolves and integrates new components and features, the necessity to incorporate IT/OT solutions to improve the efficiency and resilience of electric power systems has become more urgent. Digital tools being combined with physical assets is becoming the norm, rather than the exception, and use cases where digital technologies are applied to increase the efficiency and reliance of the world's power grids are growing in maturity.
This Preferential Subject concerns the trend towards digitalization of power grids, which continues to accelerate around the world. The subject covers three sub-topics related to Internet of Things (IoT) architectures and applications in improving the resilience of electric power systems; applications and platforms of artificial intelligence, big data, and analytics in OT; and cloud technologies to improve the efficiency and resilience of power utilities.
This year's papers show a rise in integrated, end-to-end digital platforms and software solutions that allow holistic understanding, visualization, and analysis across entire asset fleets and asset lifecycles. The papers also addressed a trend towards more solutions that combine a more comprehensive array of digital technologies and methods, such as AI, augmented and virtual reality, and advanced data collection and visualization methods, together in solutions.

A total of 40 papers were accepted within the SC D2 PS1:

Paper Reference	Title	Country
10270	Exploration and Practice of Cloud Orchestration in New Power System Distribution Scenarios	China
10273	Design of smart planar antenna array with optimal directivity in eight directions detecting ISM band wireless sensors for IT/OT solutions and substation asset condition monitoring & deep learning applications	Egypt
10300	A possible win-win cohabitation of open-source and standardization	France
10344	OMEGA-X: Energy Data Space for improving efficiency of electric power systems leveraging semantic interoperability and AI	France
10397	The journey of digitalization: how Smart Digital Substations can drive the Industrial Internet of Things revolution	Italy
10398	Digital twin for asset management of electric power systems based on IEC CIM and BIM integration	Italy
10399	Market driven architecture for remote monitoring of HV assets	Italy
10400	Orchestrated ICT architecture for grid monitoring of distribution power grid	Italy
10559	Development of Common Distribution Power System Model (CDPSM) based profiles and the proposed validation process	Netherlands
10565	Integrating Artificial Intelligence Models and Synthetic Image Data for Enhanced Asset Inspection and Defect Identification	USA
10568	A.I. Searchable Synchrophasor Database for Power System Protection	USA
10570	AI and Cloud-based Digital Transformation of Utility Asset Management and Inspections	USA

10653	Digitalization of distribution assets by use of DSO-API-REST	Spain
10780	Development and HILS Test of an AI Model for Optimal Operation of ESS in Renewable Energy Integrated EV Charging Station	Korea
10830	Data Verification in Power System Modelling	Russia
10831	Improving the Accuracy of RES Generation Forecast to Ensure Their Reliable Operation in the Power System	Russia
10832	Big Data Processing and Representation in the Low-frequency Oscillations Analysis	Russia
10833	Symbiosis of Artificial Intelligences in Automated Systems of Supervisory Control of the Electrical Grid of a Distribution Grid Company	Russia
10858	Virtual Reality and gamification as tools for training operation teams, maintenance of substations and energy transmission lines	Brazil
10859	Advanced Management and Control of Grid Substation's IEDs and Communication Devices in the Electric Power Utility	Brazil
10860	Enhancing WAMPAC Systems in the Digital Transformation Era: Applied Research on IEC 61850 over 5G	Brazil
11009	Leveraging Machine Learning for Multi-Step Failure Forecasting in RTU Analog Modules and Estimating Key Performance Indicators to Support Management Decision-Making	Paraguay
11045	Probabilistic framework for resilience enhancement of distribution grids	USA
11048	Optical Fiber Monitoring and Management System (ONMS)	Argentina
11114	Digital Edge Platform applied on Power Systems as a Key to Energy Transition	Argentina
11221	Data collection considerations for AI and machine learning in wind power equipment	Japan
11262	Augmented Operator Advisor based on Augmented Reality	India
11267	Upgradation of SCADA/EMS System at National Level – A Case Study	India
11270	Convergence of Information Technology and Operational Technology Systems – Business Operational Requirements in a Secure Manner	India
11277	UDAAN - Creation of a Unified Asset Management Platform via IT/OT Integration for Big Data Management in POWERGRID	India
11280	Innovative Approaches for Improving Efficiency and Resilience in Electric Power Systems: A Focus on IT/OT Architectures and Solutions	India
11288	Monitoring of remote S/S through Robotics, Augmented Reality and Artificial Intelligence	India
11294	Grafana for Grid data Monitoring and Visualization at Western Regional Load Despatch Centre (WRLDC), GRID-INDIA	India
11298	Energy Optimization in Blockchain Enabled Smart Distribution Grid	India
11304	State-of-the-Art Algorithms for short-term residential Load forecasting for Smart Grids	Greece
11658	Enhancing Power Grid Failure Data by Leveraging AI-driven Text Classification: A Danish Case Study	Denmark

11714	Analyses of Lightning Induced Faults Recorded by Diverse Monitoring Systems in the Transmission Network Based on a New Concept of Data Lake Design	Croatia
11777	IT/OT Convergence and Standard Architectures for DERs Considering Companion Specifications, Interoperability, IoT Technologies and Cloud Solutions	Colombia
11779	Driving and Empowering Digital Transformation: Successful Implementation of IIoT Pilots for Advanced Monitoring	Colombia
11812	Artificial Neural Network-Based Peak Demand Forecasting and Biogas Power Plant Control for Peak Demand Reduction in Factory	Thailand

Table 1 - Papers for PS1

Paper 10270 showcases a platform-based distribution network, which replaces the one-way pipe-based distribution network of yesterday and allows for flexible resource allocation. It focuses on the use of intelligent terminal transformer units (TTUs) that enable bi-directional interaction of a very high number of end devices, and on concrete use cases such as real-time line loss analysis.

Paper 10273 presents a novel design and simulation analysis of the two proposed electronically beam steerable microstrip antennas, which can be mounted on the surfaces for wireless network applications in the Industrial, Scientific, and Medical (ISM) band. The proposed switched beam antennas are designed to address the challenges of Wireless Sensor Network (WSN) positioning and they are suitable for Direction of Arrival (DoA) estimation. According to the authors, the smart antenna can enhance the implementation of WSN, which provides real-time monitoring, diagnosis, and control for IT/OT applications to improve efficiency in Electric Power Systems.

Paper 10300 discusses the synergy between open-source principles and standardization in the ICT (Information and Communication Technology) domain, particularly in the energy sector. It emphasizes the benefits of creating Open Digital Commons or Code Components to enhance efficiency and innovation in standardization. The authors suggest that Standardization Development Organizations (SDO), such as IEC, and the open-source community should work together to collaborate on creating digital standard projects where it makes sense. The paper presents successful examples of open-source and standardization cohabitation, particularly with IEC 61850 and CIM standards. It suggests that open source can significantly contribute to the development of digital standards, enabling AI to play a crucial role in standard creation and maintenance.

Paper 10344 describes OMEGA-X, part of the Energy Data Spaces initiative of the European Commission. It shows how OMEGA-X enables data interoperability for four use case families across renewables, local energy communities, electromobility with a novel semantic data model, AIME (Agile Interaction model based Methodology for Energy dataspaces).

Paper 10397 presents an application of an APM (Asset Performance Management) solution in a Brazilian wind farm, providing predictive maintenance for high voltage and protection equipment. The paper addresses the benefits of using digitalization and IIOT (Industrial Internet of Things) resources to process the asset's existing information and how this can improve its performance. The APM solution was designed to analyse all the offline (historical data, operators' inspections, offline reports) and online (interconnected sensors, protection and control IEDs, and SCADA parameters) data of the Smart Digital Substation that connected the wind farm to the grid.

Paper 10398 presents a novel approach to using digital twins for asset management over the complete lifecycle of the assets by combining three information models: the IEC Common Information Model, Industry Foundation Classes, Building Information Modeling methodology and Industry Foundation Classes to promote interoperability and completeness.

Paper 10399 presents a portfolio of solutions to overcome issues related to the integration of OT and IoT (Internet of Things) devices and systems into remote monitoring solutions. The paper presents the challenging aspects of introducing cloud infrastructure and applications in operators' environments in the context of remote monitoring of high voltage assets. Recent regulations for data sharing, such as the new EU regulation, are also mentioned as an important aspect to provide a framework for operators and service providers.

Paper 10400 proposes an ICT (Information and Communication Technology) architecture for integration of Phasor Measurement Units (PMUs) installed in distribution networks, based on a decentralized computing continuum between various nodes, from cloud to edge resources, using the FLUIDOS (Flexible, scaLable, secUre, and decentralIseD Operating System) European Project. The authors made an evaluation of use case requirements and developed specific features in the FLUIDOS project, addressing scenarios involving ICT outages and grid reconfiguration. Initial tests of the presented architecture were conducted on the experimental portion of a distribution grid, prospecting future works to develop a resilient and scalable ICT architecture.

Paper 10559 focuses on the main aspects of developing a Common Information Model (CIM) profile for Distribution System Operators (DSOs). The paper addresses the challenges in data structuring for DSOs and highlights the benefits of CIM standards for efficient information exchange in the context of decentralized and decarbonized energy systems. It discusses the implementation of the CIM profile for a United States Independent System Operator, along with a novel approach for validating CIM datasets using a cloud-hosted automated testing tool. It highlights the matter of Conformance and Interoperability in data exchange and the related testing. The paper contributes to the advancement of CIM-based data structuring for DSOs and provides practical examples for CIM profile development and validation.

Paper 10565 shows a method for improving outcomes from drone-based asset inspections using synthetically-generated images. The synthetically-generated images have the advantage of improving asset inspection outcomes on rarer defects, as well as decreasing the manual effort required to label images.

Paper 10568 proposes a novel approach to power system protection, utilizing searchable structured database tables and Phasor Measurement Unit (PMU) technology. The approach enables real-time monitoring of grid states by leveraging high-speed measurements and advanced signal processing, which can enhance grid security through related applications. The paper focuses on developing comprehensive phasor database tables for line sections under various contingencies, which can improve some analysis in the field of AC Studies. For future works, the study proposes the integration of machine learning and artificial intelligence to enhance the potential for improved grid security and operational efficiency.

Paper 10570 describes an application developed for streamlined damage assessment of transmission and distribution grid assets. It explains how a mobile application for field workers combines with a cloud-based AI platform to improve the efficiency of damage assessment and even reduce related power outages on the affected grids.

Paper 10653 presents a method for integrating various digital assets efficiently, flexibly, and at scale, particularly for medium and low-voltage distribution grids experiencing increased complexity due to the rise of renewable energies. The authors also highlight the vendor independence of the solution, which promotes more interoperability in their architecture. The specifications of these digital assets are designed to adhere to the REST-API concept, utilizing common technologies like HTTP and XML, thus ensuring scalability. Additionally, the paper outlines four data models essential for DSOs (Distribution System Operators) using conventional common data models. It comprehensively describes the Digital Asset Management (DAM) system necessary for DSOs, offering valuable insights for operators worldwide. Moreover, security concerns are addressed by discussing the applicability of conventional HTTPS protocols.

Paper 10780 showcases a deep reinforcement learning model for optimizing charging at a renewable energy-integrated electric vehicle charging station with an energy storage system with batteries. The paper describes how the model was trained, as well as its successful testing with a hardware-in-the-loop simulation and an actual energy management system.

Paper 10830 reviews various data verification approaches used in power system modeling. It elaborates on the specific needs of power system models and underscores the need to apply various methodologies, together with both robust and relatively simple analysis methods (from statistical methods to AI), in order to increase the chances of rapidly identifying and correcting errors and inaccuracies and assuring complete and accurate data.

Paper 10831 contributes to a well-known problem in our contemporary energy system: that of inaccurate renewable energy forecasts, which makes grid operations increasingly difficult as renewables penetration increases. The paper reviews best practices across various forecasting horizons and shows how combining methods can bring significant improvements in accuracy.

Paper 10832 tackles the issue of analyzing low-frequency oscillations, one of the critical analyses needed for situational awareness of operational dispatching personnel. It shows novel ways of combining and organizing various methods for analyzing low-frequency oscillations for improved situational awareness by the operators.

Paper 10833 presents a novel advanced distribution management system (ADMS) that uses AI in many steps to improve grid management outcomes. AI is used in forecasting grid conditions, such as active and reactive power flows, as well as for recommending grid topologies to operators and simulating network security contingencies on the grid. The authors show how various AI models were combined within the ADMS to achieve good results for grid operators.

Paper 10858 showcases a platform for virtual training of substation maintenance and operations workers that combines virtual reality (VR) and gamification. The paper explains the design of the various games in the platform and how they are played using VR, providing multiple examples in various voltage levels and scenarios.

Paper 10859 provides a new perspective on management and monitoring in the digital grid covering both communication network and substation Intelligent Electronic Devices (IEDs) evolving from present-day siloed implementations to a coordinated, aggregated, or integrated design, covering deployed systems and their evolutions. The authors address the similarity between the management of IEDs and telecom devices, and they enhance the potential value of merging systems in each power system segment, such as customer smart metering, medium voltage distribution, transmission grids, and energy farms, among others. Evolution and prospects for the use of all the data acquired are addressed.

Paper 10860 presents the benefits of using 5G networks attached to the IEC 61850 protocols to enable the applications of Wide Area Monitoring, Control, and Protection (WAMPAC) systems. The study presented seeks to evaluate the latency of R-GOOSE messages in the exchange of information between Intelligent Electronic Devices (IEDs) for different combinations of message encryption and signature. The IEDs used in the testbed were two emulators based on Raspberry Pi and Python code with standard libraries for encryption and signing. The work concludes that adding encryption could increase the average end-to-end time delay of the R-GOOSE message. According to the authors, more investigation about the impact of cyber-security in this field should be explored.

Paper 11009 shows the results of various machine learning algorithms for forecasting the annual failure count of Remote Terminal Units (RTUs) analog modules at a hydroelectric dam plant, as well as other KPIs for the operation of the TRU analog modules. Random Forest algorithms are shown to be the most effective for these predictions, and the paper highlights the necessary data pre-processing and model training steps to achieve the final model.

Paper 11045 proposes a new probabilistic framework for assessing and enhancing grid resiliency using proactive grid hardening strategies of topology reconfiguration and load control to mitigate the impact of extreme weather events by rerouting power flow away from the network components that have a high failure probability and reduce the severity of power outages. The proposed probabilistic framework is based on Monte-Carlo simulations that analyse multiple scenarios and provide grid-hardening decisions to enhance network resiliency. The case study used to validate the framework was the modified IEEE 123-bus distribution system in a probabilistic evaluation environment using real-world load and weather datasets.

Paper 11048 addresses the principle of operation of the ONMS (Optical Network Management System). Through its software, this system allows the configuration of a series of parameters that alert the company about the real-time status of its installed optical fibers. The paper indicates the advantages of the possible use of the ONMS from the point of view of the associated communications systems to the 500 kV transmission system. The author explains that, with the installation of an ONMS System, the concept of maintenance of optical fibers changes, and we move from the perspective of preventive maintenance, or in the event of failures, to a predictive maintenance perspective.

Paper 11114 presents a Digital Edge Platform developed to facilitate the process of energy transition through the integration of new technologies and innovative solutions. This platform allows a two-way communication and data exchange between the electrical facility and the cloud infrastructure. The collected data is used for two different solutions: the first one focuses on allowing grid monitoring and optimization using dynamic line rating technology, and the other one considers the management and analysis of post-fault data collected by the protection devices. The paper brings aspects of resilience and cybersecurity and mentions the need to evolve the internal process of the TSO to incorporate the agile methodologies applied.

Paper 11221 presents methods for enhancing training data for AI models for inspecting wind power equipment, with a focus on data collection methods, such as collecting images under different exposure conditions. The author shows how improving the data on which AI models are trained significantly improves the performance of the AI model.

Paper 11262 showcases an augmented reality application called Augmented Operator Advisor used for condition monitoring of extra-high voltage assets. The paper explains some of the main painpoints that the application solves and its key features, such as automatic identification of equipment using AI and augmented reality and virtual view for assets.

Paper 11267 discusses upgrades made to the SCADA/EMS systems at a national level in India. It discusses additional features that were added, such as automatic generation control and dynamic system assessment for improving stability and control of the networks. It also discusses challenges faced during these upgrades and mitigating measures.

Paper 11270 introduces the secure integration and convergence between IT and OT systems at the North Eastern Regional Load Despatch Centre (NERLDC) of India. Guidelines and regulations for cybersecurity in power systems are brought, and the authors address the need to update the design and architecture of the IT/OT bridge to enhance cybersecurity. In this matter, the paper highlights the importance of ensuring that methodologies, practices, and implementations in integrating OT and IT systems should comply with the latest cybersecurity standards and fall in line with the associated guidelines and regulations in the power sector.

In paper 11277, a unified asset management platform is presented. The platform addresses challenges in asset management, such as the rapidly increasing scale and complexity of assets, and further explains the platform architecture, which includes features such as unified data storage and an intelligent integration layer. KPIs showing the platform's performance are also shown.

Paper 11280 addresses the concept of the Transmission Asset Management Centre (TAMC), which is a system that integrates several applications already existing in the electric system operation environment, like SCADA, RAS, and Visual Monitoring Systems, among others. The aim of this system is to build a centralized asset management and to enable remote operation of substations, aiming to improve power system efficiency and resilience. This paper delves into a range of strategies focused on utilizing IT/OT architectures and solutions in TAMC systems, also addressing the challenges encountered in the TAMC system's design phase and the strategies to mitigate them.

Paper 11288 presents the experiences of an Indian utility using features such as Robotics, Augmented Reality (AR), and Artificial Intelligence (AI) to enable the monitoring of remote substations. The paper mentions the limitations of the traditional monitoring using manual patrolling and describes the phases of the implementation of the Robotic system developed. Remote monitoring was successfully implemented in three major substations of the energy company through extensive utilization of AR and AI applications. The entire process was automated, applying multiple robots to conduct simultaneous condition monitoring activities. The communication was supported by a fiber communication network, providing real-time AR dashboards and reports for the user.

Paper 11294 showcases an analytics software solution that combines data from multiple source systems, including the supervisory control and data acquisition (SCADA), renewable energy management center (REMC), and unified real time dynamic state measurement (URTDSM). The solution combines and enriches this data, using it to derive new calculated measures and create visualizations and dashboards. Paper 11298 shows a distributed architecture for energy management in distribution grids, which addresses the issues arising in distribution grids with increasing numbers of prosumers and more distributed generation assets. The authors explain how energy is optimized in the architecture using particle swarm optimization algorithms and traded using a double auction mechanism, enabled by a permissioned blockchain.

Paper 11304 addresses the evolution of distribution networks into smart grids, focusing on predicting the consumption behavior of residential users. The paper presents an extensive study on residential load forecasting and uses different algorithms to build up models in order to predict their electricity energy consumption. According to the authors, this contribution can enhance the functioning of Smart Grids and their integration with electricity markets. The study makes a comparative analysis of the performance of five deep learning algorithms, using several error metrics to compare the accuracy of the model’s predictions with the actual values.

Paper 11658 presents a use case of text classification based on supervised machine learning to estimate the root causes of medium-voltage cable failures. The study used a large database of unstructured text combined with structured data in failure reports provided by maintenance personnel over the last ten years to train the machine learning models. The models presented were able to transform that data into structured information, thus enhancing the overall failure data quality. The results obtained are presented, and future developments are prospected towards the application of state-of-the-art Large Language Models and Easy Data Augmentation techniques to increase the robustness of the current models.

Paper 11714 presents the development of a Data Lake concept to improve the analysis of lightning-induced faults within the transmission network. This innovative approach addresses the challenge of managing and analyzing heterogeneous, sometimes unsynchronized, and potentially inaccurate or incomplete data generated by various monitoring systems across the transmission network. The proposed architecture outlines a method for aggregating and processing data from diverse sources such as overvoltage transient monitoring systems, SCADA, and lightning location systems (LLS), among others, to facilitate efficient fault analysis, post-mortem analysis, and the assessment of stress on high voltage (HV) equipment. The paper details the technical implementation of the Data Lake, including its architecture, key features, performance characteristics, and the integration of different data sources.

Paper 11777 describes an interoperable data model combining information and operation technologies using Internet of Things (IoT) standards for remote operation of small-scale Distributed Energy Resources (DER). The paper presents a general architecture of the solution. It presents the advantages of implementing this data model and its contribution to the DER domain, providing a solution that allows utilities to collect information about the behavior of their customers and to understand energy consumption and generation in an interoperable and reliable way.

Paper 11779 proposes an Industrial IoT communication architecture designed for substations based on the advances of interoperability and data exchange. The paper presents three pilot projects applied in a Colombian substation, using LoraWAN and Xbee nodes to transmit data from sensors to gateways, aiding maintenance processes in power transformers. It looks at both wireless technologies, taking into consideration Cyber Security, and compares the performance between the two technologies. The proposed architecture allows subscription at Level 3 or SCADA, enabling data transfer to historical systems or storage such as Azure, providing opportunities for descriptive analysis and predictive analytics.

Paper 11812 shows another application of AI, specifically, neural network algorithms. In this paper, they are applied to the problem of peak demand forecasting on the demand side, and for controlling a biogas power plant on the generation side. The paper then discusses how these models work together as part of a holistic energy management platform to drive cost savings and improve efficiency at the plant.

Discussion and Questions

Question 1.1: How can grid operators bring more openness to their solutions, so that they can benefit the electric power industry at large? Open source software development paradigms support continuous improvement of software solutions, while simultaneously decreasing development and maintenance costs and increasing quality. How can open source development be incentivized in the electric power industry?

Question 1.2: Generative Artificial Intelligence (AI) has exploded into the public consciousness in the last years, making it easy to quickly generate believable text, image and video outputs. What is the potential of this novel new area of AI for the electric power industry? How can Generative AI help make our grids more efficient and sustainable? What are the potential drawbacks of Generative AI for our industry?

Question 1.3: Combining IT and OT together in new solutions for power grids significantly changes the way grid management tasks are completed, as well as the way solutions are developed. What do these changes in solution technology mean for organizations? What new organizational models, business models and ways of working can help support organizations in adopting and integrating IT/OT solutions for improved outcomes in grid resilience and efficiency?

Question 1.4: New technologies are constantly coming to maturity in other industries. How can organizations in the electric power industry quickly test and validate new, upcoming technologies for our industry and foster cross-industry innovation? What innovation models can enable our industry to test and integrate new solutions more rapidly, and use these technologies to create valuable new solutions more quickly?

Question 1.5: There is an increasing development of new IoT solutions for both industry and the power grid. What applications are currently being developed using the Industrial Internet of Things (IIoT) concept? What benefits and challenges are energy companies deriving from these new applications?

Question 1.6: What are the expectations and prospects of the electric power utilities from the new developments in asset management tools? What purposes does the acquired data expect to be used in future applications?

Question 1.7: With the increasing development of the energy sector, effective data management and structuring are crucial for maintaining system efficiency and reliability. What are the key challenges in data management and structuring for energy systems, and how are innovative approaches helping to address these challenges?

Question 1.8: An adequate data transfer of communication technologies, such as cellular networks, optical fiber, and Wireless communication, is essential to enable applications in smart grids. How can electric power industry validate the performance of these technologies? What new features and tools are being developed, and what parameters must be addressed to guarantee adequate performance?

Preferential Subject 2 (PS2): Cybersecurity in emerging application domains and technologies for securing energy organisations

Introduction

Utilities are increasingly dependent on Industrial Control Systems (ICS), cloud services and ICT systems to monitor and control their operations. While these systems enhance operational efficiency, they also present a larger attack surface for cyber threats.

Cybersecurity is essential as emerging technologies reshape the energy industry. Distributed Energy Resources (DER), microgrids, and energy communities' control infrastructures offer efficiency and resilience but introduce new vulnerabilities. TSOs are involved as well regarding more ICT services offered in the cloud. Furthermore, the degree of digitalization and automation using more ICT systems are also increasing. Hence these aspects got impacts for DSOs and DER as well. Electric vehicle (EV) charging and discharging systems add complexity and require robust cybersecurity to prevent unauthorized access and operational disruptions. The shift to cloud-based applications in power utilities, while beneficial, presents risks related to data privacy and network security.
The preferential subject explores cybersecurity challenges and solutions for DER, microgrids, energy communities, EV systems, and cloud-based applications, highlighting the need for a comprehensive cybersecurity strategy to ensure the resilience and reliability of modern energy systems.

A total of 13 papers were accepted within the SC D2 PS2:

Paper Reference	Title	Country
11205	A Strategy for Cyber Risk Mitigation in Smart Grids Through Traffic Management	COLOMBIA
11782	Analysis of High-Impact Scenarios for Cybersecurity in the Colombian Power System	COLOMBIA
11296	Cyber Security Assesment of Digital Substation using Petri Net	INDIA
11206	Cybersecurity for Communication Systems for Digital Electrical Substations Leveraging Emerging Network Technologies	COLOMBIA
10401	Cybersecurity In the Loop for multi energy infrastructures	ITALY
11839	Enhancing Cybersecurity in Critical Infrastructure: Leveraging Next Generation Firewalls (NGFW) for Robust Protection in OT and Substation Environments	SOUTH AFRICA
11780	Evaluation of the Maturity of Cybersecurity in the Colombian Power System	COLOMBIA
11312	Hardened (Air-gapped) IT-OT Interconnection – A Case study on Proof of Concept in Context of Power System Operation	INDIA
11291	Implementation of Cyber Security in IEC 61850 based Substation Automation System – Experiences, Challenges and Enhancement in Prevailing Practices	INDIA
11228	Implementing a Protection Management System in AWS Cloud: Strict Cyber Security Standards & Rules and experience of system in Production	PERU
11204	Lessons Learned from Infrastructure Attacks on Substations A Lens on North and South America.	COLOMBIA
10770	Performing Risk Assessments of EV Charging Systems	BOSNIA AND HERZEGOVINA
10656	The Elektrilevi's Advanced Remote Engineering Platform (AREP)	CANADA

The preferential subject is focused on three topics:

- Cybersecurity for DER, microgrid and energy communities' control infrastructures.
- Cybersecurity for electric vehicle charging and discharging control.
- Cybersecurity in cloud-based applications of power utilities**.**

The following were the summary of items discussed in each paper, grouped by the sub-topics:

A) Cybersecurity for DER, microgrid and energy communities' control infrastructures.

Paper 11205 proposes a strategy for managing cyber risks in digital substations of smart grids through traffic management. By focusing on VLAN segmentation and multicast filtering, it optimizes security and Quality of Service (QoS) without additional risk detection technologies. The results show that these techniques effectively mitigate attacks such as DoS and spoofing, thereby improving both protection and operational efficiency.

Paper 11782 examines cybersecurity in the Colombian power system, identifying ten high-impact cyber-attack scenarios on critical infrastructure. The scenarios include attacks on generation control, dam gate systems, protection systems, and transformers, leading to potential blackouts, explosions, and loss of life. The research highlights common vulnerabilities, such as outdated technology and lack of secure communication, proposing an architecture based on the ISA/IEC 62443 standard to mitigate these risks. The study emphasizes the need for robust cybersecurity measures and collaboration among stakeholders to protect critical infrastructures.

Paper 11296 presents a cybersecurity assessment of digital substations (DS) using Petri Nets to evaluate cyber secure operations and controls. It analyzes various vulnerability scenarios, including network, system, process/access, and human factors, within a DS. The study formulates a simplified DS architecture and uses Stochastic Petri Nets (SPNs) to assess cybersecurity, focusing on availability as a key metric. A case study illustrates the impact of cyber-attacks on DS components and their availability, providing insights into securing operations in power systems.

Paper 11206 investigates the role of Software-Defined Networking (SDN) and Programmable Data Planes in enhancing the efficiency and security of communication systems in digital electrical substations. By implementing SDN, the research demonstrates improved network management and adaptability, crucial for the stringent requirements of protocols like GOOSE and SV in Smart Grids. The findings highlight the potential of SDN to provide flexible, centralized control, leading to more robust and secure energy infrastructures. The hybrid model combining SDN with traditional networks offers a viable pathway for modernizing critical infrastructure.

Paper 10401 focuses on enhancing cybersecurity for multi-energy infrastructures by integrating advanced cyber-physical control systems. Utilizing a "security by design" approach, the CIL demonstrator incorporates preventive and defensive measures, including data encryption, communication authentication via Public Key Infrastructure (PKI), and Security Information and Event Management (SIEM) for real-time monitoring and anomaly detection. The project aims to validate these measures through operational tests at RSE facilities, ensuring resilient and secure energy systems capable of mitigating cybersecurity threats.

Paper 11839 discusses the role of Next-Generation Firewalls (NGFWs) in enhancing cybersecurity for critical infrastructure, particularly in Operational Technology (OT) and substation environments. NGFWs offer advanced features like granular application visibility, intrusion detection/prevention, SSL/TLS traffic decryption, and intelligent security automation, enabling real-time threat detection and response. Despite limitations in intra-VLAN communication, integrating NGFWs with Network Intrusion Detection Systems (NIDS) and Network Access Control (NAC) forms a robust defense-in-depth strategy. This approach, combined with Security Information and Event Management (SIEM) systems, significantly strengthens the cybersecurity posture of critical infrastructure.

Paper 11780 evaluates the cybersecurity maturity of the Colombian power system. It identifies various types of cyber attackers and their potential impacts on the electrical sector. The study assesses the implementation and maturity levels of cybersecurity practices using the NIST CSF v 1.1 framework and NARUC's maturity model. Findings reveal that most cybersecurity practices are only partially implemented, requiring improvements in several areas. Recommendations include enhancing cybersecurity management across all levels and promoting standardization to mitigate gaps in the sector's cybersecurity posture.

Paper 11312 examines the implementation of a hardened IT-OT interconnection using Data-Diodes in Indian power grid control centers. It addresses the cybersecurity challenges in integrating SCADA and IT systems while maintaining secure, unidirectional data flow to prevent cyber-attacks. The proof of concept demonstrated successful, secure data exchange between IT and OT networks, highlighting the effectiveness of Data-Diodes in creating an air-gapped network. This solution ensures robust cybersecurity without compromising the necessary operational data exchange for grid management and analytics.

Paper 11291 discusses the implementation of cybersecurity in IEC 61850-based substation automation systems (SAS) at Gujarat Energy Transmission Co. Ltd. The paper highlights the increased cyber threat to digital power grids and the need for robust security measures. The implementation includes threat-vulnerability analysis, adopting standards like IEC 62443, and practical measures such as BIOS and OS hardening, secure communication protocols, and disabling unused ports. The goal is to enhance the cybersecurity posture of SAS using a defense-in-depth approach, ensuring secure operations and resilience against sophisticated cyber-attacks.
Paper 11204 reviews physical attacks on electrical substations in North and South America, emphasizing the critical need for enhanced infrastructure security. Highlighting incidents like the 2013 Metcalf substation attack, it underscores vulnerabilities and the necessity of comprehensive physical security measures. It details regulatory responses, including NERC's CIP rules and state initiatives, advocating for proactive strategies and collaboration with law enforcement. The study also explores advanced technologies like AI, blockchain, and real-time monitoring to bolster defenses and calls for a forward-thinking, collaborative approach to safeguard critical infrastructure.

Discussion and Questions

Question 2.1: The increasing deployment of Distributed Energy Resources (DER) and microgrids enhances the resilience and efficiency of energy systems but also introduces new cybersecurity challenges. What are the primary cybersecurity threats facing DER and microgrid control infrastructures, and how can these threats be effectively mitigated to ensure secure and reliable operations?

Question 2.2: Energy communities rely on interconnected control systems to manage local energy generation, distribution, and consumption, which can be vulnerable to cyberattacks. How can energy communities enhance the cybersecurity of their control infrastructures, and what best practices should be implemented to protect against potential cyber threats?

Question 2.3: The integration of advanced technologies, such as IoT devices and real-time data analytics, into DER and microgrid control systems offers numerous benefits but also expands the attack surface. What strategies can be employed to secure IoT devices and data analytics platforms used in DER and microgrid control systems, ensuring both functionality and cybersecurity?

Question 2.4: Cybersecurity incidents in DER and microgrid infrastructures can disrupt energy supply and impact the overall stability of the energy grid. What are the potential impacts of cybersecurity incidents on DER and microgrid operations, and how can organizations develop and implement effective incident response plans to minimize these impacts?

Question 2.5: Regulatory frameworks and industry standards play a critical role in guiding cybersecurity practices for DER, microgrid, and energy community control infrastructures. How can organizations ensure compliance with relevant cybersecurity regulations and standards, and what role do these frameworks play in enhancing the overall security posture of DER and microgrid systems?

Question 2.6: The integration of several advanced technologies, such as IoT devices and real-time data analytics, into DER and microgrid control systems offers numerous benefits but also expands the attack surface. Which possibilities rather than the only cyberattack can also offer an attack surface?

Question 2.7: Cyber security incidents can occur from more than only virtual access. Which possibilities can gather unauthorized access to DER, microgrid and energy community control infrastructures to generate fraudulent intrusion? Which measure can be taken against this?

Question 2.8: A comprehensive risk management helps to strengthen the resilience of a system. Which measures regarding risk management will improve the cyber security resilience of the concerning system?

B) Cybersecurity for electric vehicle charging and discharging control.

Paper 10770 evaluates cybersecurity risks in Electric Vehicle Charging Systems (EVCS), emphasizing the integration of IT and OT systems. Using an automated agile risk assessment tool, the study identifies inherent cybersecurity risks and proposes mitigations for EPBiH's EVCS. Key risks include system deception, data corruption, and payment disclosure. The recommended security controls are tailored to enhance system protection against identified threats. The agile approach allows for rapid reassessment, ensuring timely and effective mitigation in response to evolving threats and system changes.

Paper 10656 Elektrilevi, Estonia's largest Distribution System Operator, developed the Advanced Remote Engineering Platform (AREP) to enhance cybersecurity and efficiency in managing Intelligent Electronic Devices (IEDs). The AREP provides secure remote access, granular user control, and comprehensive audit trails, supporting over 10,000 IEDs. Funded by the European Union, AREP aims to reduce travel, improve staff safety, and lower CO2 emissions. Its implementation addresses cybersecurity challenges, integrates IT and OT policies, and supports automated management tasks, establishing a benchmark for secure remote engineering in power grid automation.

Discussion and Questions

Question 2.9: The integration of electric vehicles (EVs) into the energy grid through charging and discharging processes introduces new cybersecurity vulnerabilities. What are the main cybersecurity risks associated with EV charging and discharging control, and how can these risks be mitigated to protect both the vehicles and the grid?

Question 2.10: Secure communication between EVs and charging infrastructure is crucial to prevent unauthorized access and potential cyberattacks. What protocols and technologies should be implemented to ensure secure communication in EV charging and discharging systems, and how can these be standardized across the industry?

Question 2.11: The increasing connectivity of EV charging stations creates more entry points for potential cyber threats. How can power utilities and service providers enhance the cybersecurity of EV charging stations, and what are the best practices for monitoring and responding to potential threats?

Question 2.12: The financial and operational impacts of a cyberattack on EV charging infrastructure can be significant, affecting both users and energy providers. What are the potential impacts of cyberattacks on EV charging and discharging systems, and what contingency plans should be in place to minimize disruption and ensure quick recovery?

Question 2.13: As the adoption of EVs grows, the cybersecurity of charging infrastructure becomes a shared responsibility between manufacturers, service providers, and regulators. How can collaboration between EV manufacturers, charging infrastructure providers, and regulatory bodies be strengthened to enhance cybersecurity standards and practices in the EV ecosystem?

Question 2.14: There are different groups involved, like industry, consumers und suppliers. Sometimes is more stakeholder involved, for instance offering the ChargePoint. Which measure shall be taken to ensure cybersecurity having several participating stakeholders.

Question 2.15: Regarding comprehensive networking of the participating systems a cyberattack can cause an entire breakdown of the charging system in a region. Which measures should be taken for a proper disaster recovery?

C) Cybersecurity in cloud-based applications of power utilities.

Paper 11228 details the implementation of a Centralized Protection Management System (CPMS) in the cloud by ENEL Distribution Peru (EDP). The project aimed to enhance operational efficiency, cybersecurity, and data management for high voltage substations. It included robust cybersecurity measures in compliance with IEC 62443 standards and improved remote access for maintenance and fault detection. The CPMS has successfully reduced service interruption indicators (SAIFI and SAIDI), optimized protection relay management, and provided significant cost savings and operational benefits, particularly during the COVID-19 pandemic.

Discussion and Questions

Question 2.16: Cloud-based applications provide significant advantages for power utilities, but they also present unique cybersecurity risks. What security protocols and standards should be adopted to ensure the protection of data and operations in cloud-based applications used by power utilities?

Question 2.17: Cloud-based applications offer power utilities significant benefits in terms of scalability, flexibility, and cost-efficiency. However, they also present unique cybersecurity challenges. What are the primary cybersecurity risks associated with the adoption of cloud-based applications in power utilities, and how can these risks be effectively mitigated?

Question 2.18: The transition to cloud-based solutions necessitates robust data protection measures to ensure the confidentiality, integrity, and availability of sensitive information. What are the best practices for implementing strong data protection measures in cloud environments for power utilities, including encryption, access controls, and data loss prevention?

Question 2.19: The shared responsibility model of cloud service providers requires power utilities to clearly understand and manage their security responsibilities. How can power utilities effectively navigate the shared responsibility model with cloud service providers to ensure comprehensive cybersecurity coverage?

Question 2.20: Identity and access management (IAM) is a critical component of securing cloud-based applications, ensuring that only authorized users have access to sensitive systems and data. What strategies should power utilities employ to optimize IAM in cloud-based applications, and how can they balance ease of access with stringent security controls?

Question 2.21: Cybersecurity incidents in cloud environments can disrupt operations and lead to significant financial and reputational damage for power utilities. What are the key elements of an effective incident response plan for cloud-based applications in power utilities, and how can organizations ensure they are prepared to respond swiftly and effectively to cybersecurity incidents?

Question 2.22: In Cloud based systems several stakeholders meet each other. There are critical infrastructures as well as non-ones. The utilities still got their responsibility to provide their services. How can utilities obtain the responsibility for proper and high secure operation?

Question 2.23: The cloud systems necessitate a comprehensive data network as well. The data lines are outside of the critical infrastructure of utilities. Unauthorized physical access is relieved. How can a utility be prepared respectively which measures can provide efficient cyber security?

Preferential Subject 3 (PS3): Meeting the challenges of energy transition with reliable, scalable, and efficient telecommunications networks

Introduction (Amadou Louh / Hiroki Doi)

Electric Power Utilities (EPUs) in the worldwide tackle the challenges of building scalable and resilient networks, integration of current and new wireless technologies, and migrating from legacy networks to the packet switched networks. Those efforts dedicate to lead to not only “Grid revolution” with energy transition but also “Green revolution” with CO_2 reduction.

This preferential subject focuses on identifying the current challenges of energy transition with reliable, scalable, and efficient telecommunications networks.

As can be seen in Figure 1, the papers accepted in this preferential subject address the following main topics:

1. Migration from legacy networks to the packet switched networks, include MPLS-TP and IP networks.
2. Full digital substation with process bus, include IEC 61850 and PTP.
3. New network technologies, including SD-WAN / SDN.
4. Wireless cellular technologies, including LTE and 5G.
5. Network management and monitoring system, include multi-vendor system and SNMP / NetFlow.

Figure 1 - Keyword distribution (wordcloud) in all papers in PS3

A total of 23 papers have been accepted for PS3:

Paper Reference	Title	Country
10101	Exploring the Reliability of Commercial 5G Standalone Networks for Virtual Fault Passage Indication	Finland

Paper Reference	Title	Country
10109	Applicability of 5G Communication to Line Differential Protection for Distribution Networks	Finland
10110	Migration from TDM Networks to MPLS-TP, Field Experiences	Finland
10376	Optical Systems Performance for Line Protection Schemes	Panama, Peru
10571	The Next Generation of Joint-Use Utility Infrastructure	USA
10572	Redundant Passive Optical Network (PON) Transport for Grid Intelligence	USA
10573	PLTE Testing of Utility Use Cases in Support of Grid Modernization	USA
10648	Migration from MPLS-TP & SDH Hybrid Networks to OTN Optical Transport Networks	Argentina
10652	Mapping Multiprotocol Services into a MPLS Critical Infrastructure Network	Spain
10758	Quantum Key Distribution for MPLS-TP Traffic Encryption	Switzerland
10992	Electric Power Industry of Serbia IP MPLS network application for communications of technical information systems	Serbia
11209	Implementation of “Software-Defined Networking” as an Alternative for Efficient Traffic Management in Digital Substations	Colombia
11222	IP Network Availability Improvement Initiatives	Japan
11227	Techniques and methods in building resilient networks that support critical applications for Electricity Power Utilities	Japan
11229	Requirements for resilient packet-switched network using MPLS-TP and wireless microwave technology	Japan, Belgium
11233	A Fast and Accurate Calculation Method of Availability for Protection Relays Applying the IEC 61850 Process Bus	Japan
11260	Implementing Telecommunications Network For Remote Operation Of Substations From National Transmission Asset Management Centre (NTAMC) By POWERGRID – A Novel Experience	India
11264	Implementation of HVDC-Emergency Power Control at HVDC Raigarh by Integrating Two Different Geographical Locations Through IEC 61850 Platform Over SDH Network	India
11283	Overview of State-of-the-Art Unified Network Management System for Managing Multivendor and Multi-Technology Power System Communication Network and attaining more Reliable, Scalable & Efficient Communication Network	India

Paper Reference	Title	Country
11492	Development of Wireless Communication Environments for the Smart Industrial Safety in Power Plants	Japan
11773	Strengthen cybersecurity and device management of cellular communication systems	Taiwan
11781	MPLS-TP as a communication protocol for Critical Infrastructure transport networks: Challenges in the implementation of the protocol in WAMPAC systems of ANDE - Paraguay	Paraguay
11850	Implementation and Impact of Network Management and Monitoring Systems on ANDE's Operational Technology (OT) Network	Paraguay

Table 3 - Papers for PS3

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

A) Building scalable and resilient networks with management, automation and orchestration solutions and methods
B) Integration of current and new wireless technologies in meeting the requirements of power utility applications
C) Techniques and methods in building resilient networks and migrating legacy networks to support critical utility applications

The following were the summary of items discussed in each paper, grouped by the sub-topics:

A) Building scalable and resilient networks with management, automation and orchestration solutions and methods

The objective of the **paper 11209** is to demonstrate the ability of SDN switches to be integrated into hybrid communication architectures along with traditional switches, taking advantage of the benefits of both technologies. This paper explores the crucial digital transformation in the electricity sector, focusing on Digital Substations (DS). It addresses the operational challenges of these substations, such as the required speed of relay actuation in the event of faults and the management of the voluminous information flow. In addition, the vulnerability of DS to cyber-attacks is considered, highlighting the importance of effective and secure traffic management.

Paper 11222 describes TEPCO's experiences on theoretical and practical implementation of IP network triple redundancy. Triple modular network enhances network availability by introducing N+1+1 Criterion on the network. The cost associated with this may be a major factor for most Electric Power Utilities. However, the Author cited the natural disasters faced by TEPCO as one of the contributing factors to consider this solution.

Paper 11260 provides a high-level summary of Powergrid's experiences in upgrading its telecommunication network to realize a new operating philosophy using remote control centres. It describes some challenges in its journey that would be familiar to those in the industry. More detail on the technical aspects, and more emphasis on the novel aspects of Powergrid's experiences when compared to other power utilities would help maintain reader engagement.

Paper 11283 presents a unified network management system to monitor, manage and configure a multi-vendor and multi-network communication network in the Indian power sector. This replaces the architecture of using a different NMS for each vendor specific equipment, thus reducing complexity when configuring new circuits or dealing with defects or failures.

Paper 11850 illustrates the Paraguayan Electric Power Network and how they have implemented Wide Area Monitoring on the 110 substations. It also addresses the challenges of integrating and scaling up of the solution to cover the integrated part of the network.

Question 3.1: In the future, SDN may play an important role in communication networks within substation premises. It is also necessary to comply with IEC 61850. Is it possible for SDN to communicate in accordance with IEC 61850 even in the event of faults in the power system?

Question 3.2: It is very important to design the redundant network configuration for telecommunications for electric power systems. How to design the bandwidth of path on a double or triple modular redundant configuration? It is easy to design that the all backup paths to be empty (ex. 1 : 1 protection). But that is a network design that uses communication lines inefficiency. Is it possible to share a backup path for each main path?

Question 3.3: There are many various tools that use SNMP or NetFlow to collect device status information and log information. Please show a use case where you performed troubleshooting using this information.

B) Integration of current and new wireless technologies in meeting the requirements of power utility applications

Paper 10101 provides interesting aspects in the application possibility of commercial 5G networks for power system protection operations. In this paper, suitability of a commercial 5G SA network in Finland has been studied for a virtual FPI application, reporting that the latency requirements of virtual FPI have been reached. This paper also summarizes future work for improving reliability. In addition, a selected case when the fault indication could not be successfully performed due to communication network issues was investigated to understand the impact of communication network issues to grid applications.

Paper 10109 discusses the latest experiences and learnings regarding 5G based distribution network protection applications, including line differential protection in various 5G network architecture deployments. Experiments have been conducted in several countries, and the performance of differential protection over 5G has been evaluated.

Paper 10571 describes the characteristics and scalability of AMI (Advanced Metering Infrastructure) network. This AMI network is connected to AMI electric meters, relays, smart streetlights, as well as smart water meters and gas meters. The characteristics and benefits of AIM network are summarized as use cases in this paper.

Paper 10573 provides the Private Long-Term Evolution (PLTE) architecture and methodology for PLTE communication testing, User Equipment (UE) configurations and comparisons, and redundancy testing with a fibre primary path failed over to a PLTE secondary path. This paper will also discuss the test cases that were developed providing information on use-case applications and benefits to the utility and customers. It will also serve as a benchmark for other utilities who are seeking to establish an AMI as a platform for enabling use-cases and achieving greater reliability and resiliency of the power grid.

Paper 11492 discusses the communication requirements for the smart industrial safety in power plants and the desirable wireless communication methods. The authors explain Japan's regulations concerning 5G, one of the wireless communication methods and focuses on the development of a wireless communication environment suitable for power plants. Finally, this paper introduces the results of the verification tests of the smart industrial safety.

Paper 11773 discusses cybersecurity, manageability, and hardware design challenges of industrial cellular gateways and proposes solutions using deep packet inspection, network device management system, and tailored hardware design.

Question 3.4: 5G wireless communications have the potential to be low-latency and highly reliable. Those features are essential for the communication in EPUs. On the other hand, 5G communications also suffer from unstable delays. In order to stabilize the delay, what kind of technology should be used in the network configuration and under what conditions?

Question 3.5: There are many attractive wireless communication technologies, Wi-Fi, 5G/6G, Li-Fi, satellite communications and so on. How can these communication technologies be applied to communications for EPU's applications to maximize their effectiveness?

C) Techniques and methods in building resilient networks and migrating legacy networks to support critical utility applications

Paper 10110 describes field experiences about migration from SDH to MPLS-TP at substation-to-substation communication channels. The main services were IEEE C37.94 based teleprotection for distance and differential protection devices. To see possible differences between SDH and MPLS-TP, four network topologies were implemented and tested: SDH only, SDH to MPLS-TP, mixed SDH-MPLS-TP and MPLS-TP only. Test results show emulated C37.94 can be transmitted within specifications.

Paper 10376 provides that the Multi-Protocol Label Switching–Transport Profile (MPLS-TP) Multiplexer under evaluation represents a secure, reliable, and efficient communication platform which allows preserving the integrity of the information exchanged between network nodes with higher priority in critical services such as teleprotection, differential protection and Generic Object Oriented Substation Event (GOOSE) messaging.

Paper 10572 shows an industry redundant Passive Optical Network (PON) solution. The PON has been designed to meet the requirements for power Distribution Automation (DA), Voltage Optimization (VO) and Advanced Metering Infrastructure (AMI). Also, the PON infrastructure core is very robust with no single points of failure and is architected in a self-healing ring topology or point-to-point with backup circuit redundancy.

Paper 10648 presents the requirements and technical specifications (guidelines) for the migration from Multiprotocol Label Switching - Transport Profile (MPLS-TP) and Synchronous Digital Hierarchy (SDH) Hybrid Networks to Optical Transport Networks (OTN) for linking substations that make up the 500 kV extra-high voltage transmission network.

Paper 10652 describes the migration from TDM networks to IP MPLS networks for services in high power grids. In particular, the following points are summarized as key points: cybersecurity technologies in the IP network, time synchronization service, IP MPLS technology on an underlying DWDM optical transport network.

Paper 10758 presents a solution where for the first time QKD technology is utilized by MPLS-TP encryptors to successfully exchange keys for the use of symmetric encryption. Symmetrical encryption is then used to encrypt the services such as differential protection application. The presented solution does not only meet all the requirements in terms of communication channel performance such as latency or channel symmetry, availability or cybersecurity but also allows a gradual implementation and later addition of cybersecurity elements (e.g., a QKD system) once it is deemed as needed.

Paper 10992 discusses the application of the IP MPLS network for the purposes of interconnecting the SCADA systems of the Electric Power Industry and Transmissions System Operator. The paper considers various communication and service requirements, which are stated before the telecommunications system, and shows their fulfillment using the IP MPLS network as a universal platform to provide high availability and capacity of services with guaranteed quality of services.

Paper 11227 presents a method for building resilient IP networks that house critical data for a stable power supply, such as SCADA, using multiprotocol label switching-traffic engineering (MPLS-TE) technology to combine transmission lines with different characteristics (optical fibre cables and microwave wireless communications). The network suffered several disasters, but the system housed in this network continued to operate in each case.

Paper 11229 outlines the inherent requirements, associated challenges, and the applicability of Multiprotocol Label Switching Transport Profile (MPLS-TP) to build a packet-switched wireless microwave network for Japanese utilities. A Proof of Concept (PoC) covering Ethernet, J1 (1.5M) and 2/4W+E&M analogue voice services over MPLS-TP was conducted to verify whether MPLS-TP satisfies the stringent requirements for an independent Japanese packet-switched wireless microwave utility network.

Paper 11233 introduces a novel methodology for rapid and accurate availability calculation in systems utilizing process buses with PRP and HSR configurations for the IEC 61850 process bus. This method pre-calculates the availability of MU and IED groups, integrating these calculations into the truth table approach. This integration markedly diminishes the truth table method’s computational patterns.

Paper 11264 discusses Powergrid's experience of implementation of communication technology in HVDC transmission network. The authors have analysed and found that the most appropriate way to

transmit Emergency Power Control signals between two substations over a distance of 100 km is by applying the IEC 61850 GOOSE communication.

Paper 11781 presents the MPLS-TP network implemented for the Wide Area Monitoring Protection and Control (WAMPAC) system. The WAMPAC has 22 substations/sites or network nodes, with over 4,000 km of optical fibre. Several of these nodes have more than two communication links for redundancy. Also, as an alternative, the possibility of implementing redundancy using technologies such as Fast ReRoute, pseudowire and another multi-segment pseudowire variant is analysed. In the same sense, an analysis and comparison with traditional MPLS, OSPF and BGP are performed, indicating some of their advantages and disadvantages for implementation in a WAMPAC system.

Question 3.6: Legacy networks are becoming difficult to maintain and support, and we need to establish a method for migrating from them as soon as possible. What is the most efficient way to migrate without impacting services?

Question 3.7: The 1+1 protection introduces a delay jump on the service when switching between the short and the long path on the network. It is very important point for the delay time sensitive applications. Also, it means that a buffer is required at the terminating router to absorb the delay difference for multiple paths. How should we set up the buffer or how to estimate the buffer size?

Question 3.8: The SDN allows for a more flexible, dynamic, and efficient network management and control, overcoming the limitations inherent in traditional network architectures. MPLS-TP also incorporates Traffic Engineering (TE) capabilities, offering mechanisms for network protection and recovery in the event of link failures and deterministic control over network resource utilization. How to realise the precision and reliability of MPLS-TP in packet delivery, along with the flexibility and programmability of SDN by integrating MPLS-TP and SDN?

Question 3.9: How to guarantee the strict latency and jitter requirements, such as current differential protection on IP, MPLS-TP or L2 networks?

Question 3.10: How to design the paths which are guaranteed the availability, not only in the substation but also between substations. Here, assume that the network topology connected to the substation is a star, ring, or mesh type network topology.