STUDY COMMITTEE D2

INFORMATION SYSTEMS AND TELECOMMUNICATION

cigre

For power system expertise

Inhoudsopgave

- SCD2 Strategy
- Relevant Topics & Preferential subjects
  - 3 papers
- Future works & New working groups

STUDY COMMITTEE D2
STRATEGIC PLAN

2018-2028

Missie and Objectives SCD2

- To facilitate and promote the progress of engineering and the international exchange of information and knowledge in the field of **information systems** and **telecommunications** for **power systems**. To add value to this information and knowledge by means of synthesizing state-of-the-art practices and making recommendations.

- SC D2 will:
  - be more customer oriented
  - foster the participation in the working bodies
  - be well balanced between Information systems, Telecommunications, Telecontrol and Automation
  - draw the interest of the customers for the work done in the SC

Scope SCD2

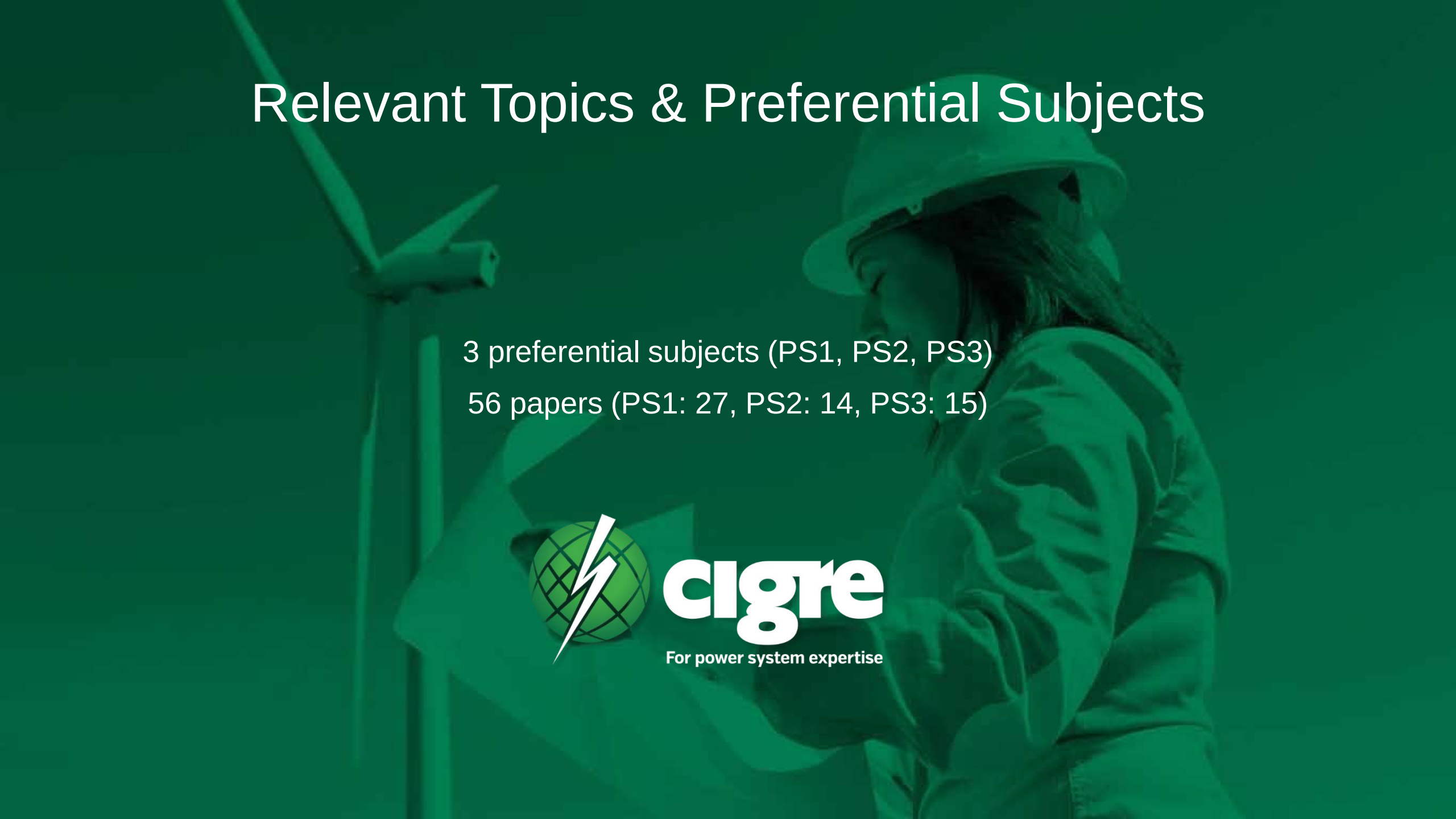
- Study Committee D2 focuses on the study of information systems and telecommunication technologies and their application in the power utility environment. Its scope is:
  - ICT applied to digital networks from UHV to distribution (smart meter, IoT, big data, EMS, etc...).
  - Communication solutions for information exchange in the smart delivery of electrical energy
  - Interoperability and data exchange (file format, frequency, etc.) between network operators, market players, off-grid premises
  - Cyber security issues from field equipment to corporate IT (Governance constraints, system design, implementation, testing, operation and maintenance...)
  - Technologies and architecture to ensure business continuity and disaster recovery
  - IT systems to support the decision-making process in Asset Management

SCD2 Strategie

Strategic Plan 2018 – 2028

- 3 strategic directions:
  - Networks of the Future: Core Telecom network technologies, Strategies to deploy new Technologies, New IT operational architecture
  - Energy efficiency support: New applications to improve efficiency, New telecom architectures and technologies
  - Common aspects: New operational and maintenance concepts and requirements, Technologies and architecture to assure business continuity and disaster recovery
- 4 technical directions:
  - TD1: Telecom network technologies and management
  - TD2: Implementation of the networks of the future
  - TD3: New digital trends used by EPU and new business services
  - TD4: Cyber security: Overcoming security threats, Assessing security risks, defining the proper security framework, architecture and best practices

Relevant Topics & Preferential Subjects



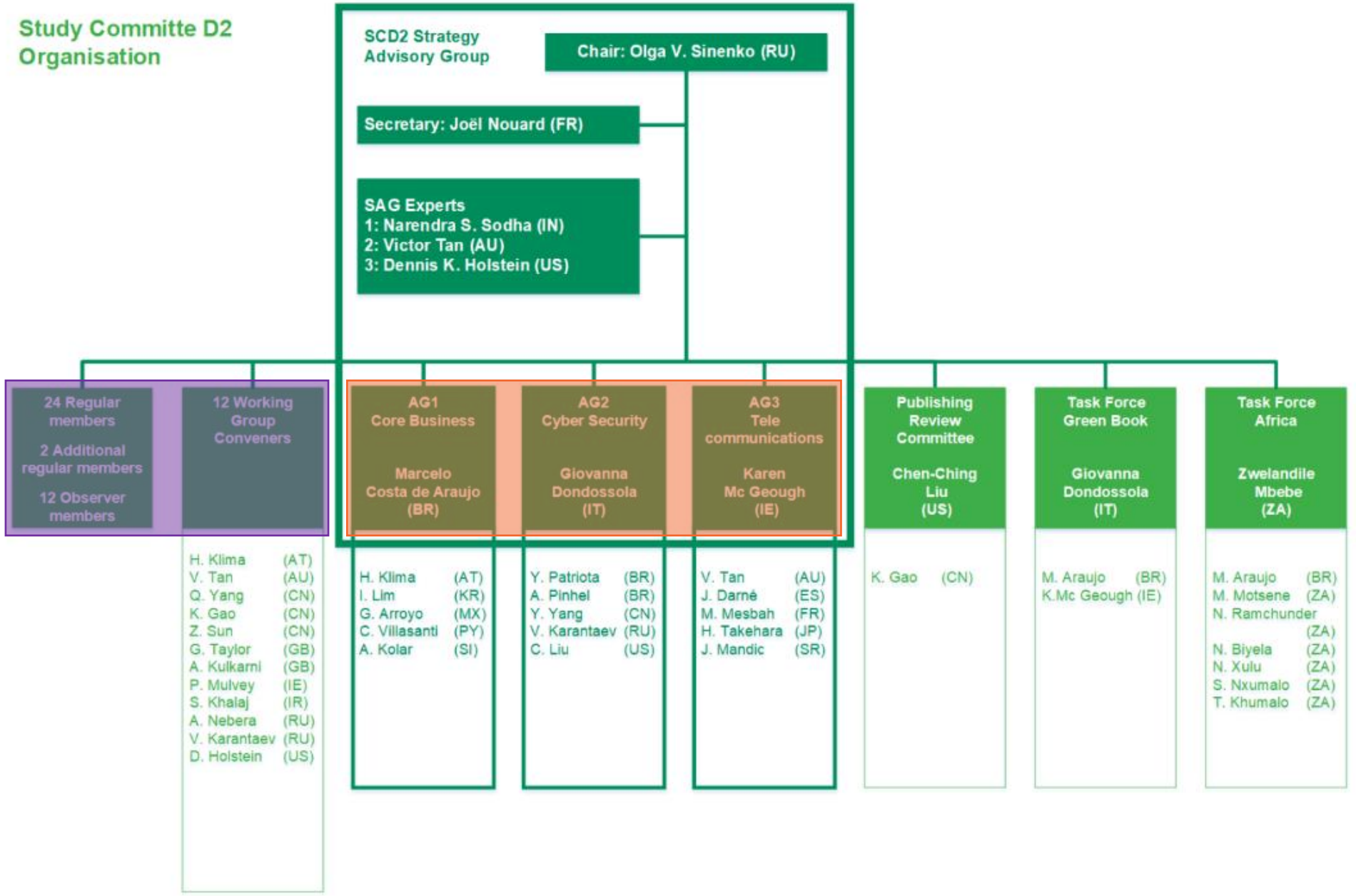
3 preferential subjects (PS1, PS2, PS3)

56 papers (PS1: 27, PS2: 14, PS3: 15)

cigre

For power system expertise

Study Committe D2 Organisation



Annual Country Report

AG Relevant Topics

Preferential Subjects

Relevant topics for AGD2.01 (Core Business)

- Big Data technology-based business models in power utilities: Many people talk about it, but we hear no news if such a business model exists or not. This was also chosen as a priority in the AGD2.01 meeting
- SCADA Data Integration with other IT Systems. No utilities are doing that today, and it would bring great value for the business
- Artificial Intelligence applications:
  - AI applications to gather useful information from data collected by IoT systems and improve situational awareness: in the meeting, an application for distribution was mentioned and that China has many use cases on that.
  - AI applications for Asset and Risk Management
  - Computer vision combined with machine learning for anomaly detection in transmission lines and primary assets (transformers, reactors, etc)
- Cloud Computing Applications to OT

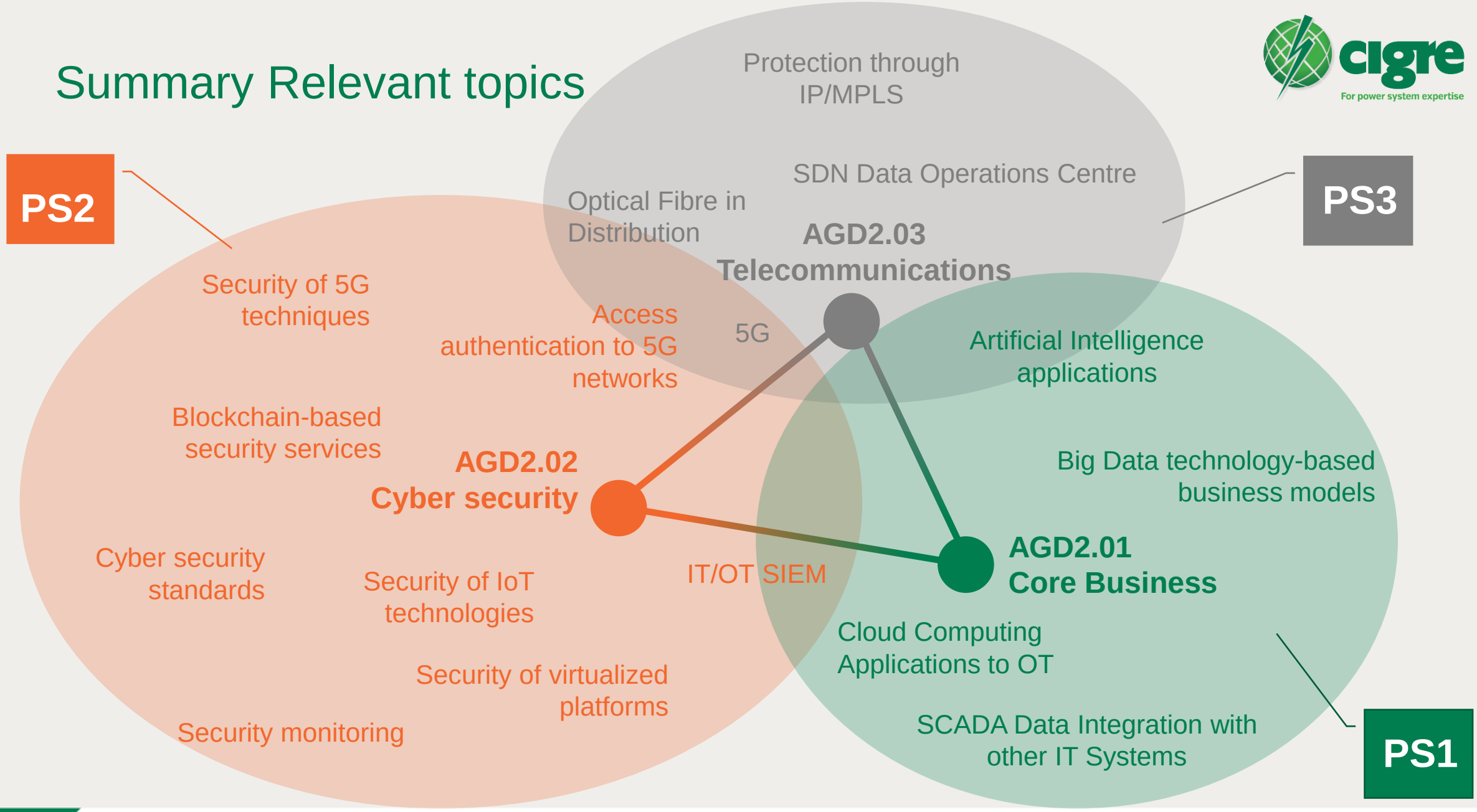
Relevant topics for AGD2.02 (Cyber Security)

- Security monitoring, anomaly detection and incident management
- IT/OT SIEM, security information event management
- Cyber security measures for power system resilience
- Security of IoT technologies within the electricity sector
- Security of virtualized platforms such as fog and cloud computing
- Security of 5G techniques such as Network Function Virtualization and SDN
- Access authentication to 5G networks in OT environment
- Blockchain-based security services for EPUs
- Cyber security standards for EPUs

Relevant topics for AGD2.03 (Telecommunications)

- Communication of Protection through IP/MPLS Systems
- 5G for Utilities
- Framework for an EPU SDN Data Operations Centre
- Optical Fibre on Distribution Network Infrastructures

Summary Relevant topics



Preferential subjects

PS1: THE IMPACT OF EMERGING INFORMATION AND COMMUNICATION TECHNOLOGIES ON ELECTRIC POWER UTILITIES (AI, Machine learning, Big Data, Analytics, Blockchain to improve AM and Operations)

PS2: NEW CYBERSECURITY CHALLENGES IN THE CHANGING ELECTRICITY INDUSTRY (Cybersecurity challenges related to IoT, Big Data, and Cloud-based platforms, DERs, …)

PS3: INCREASING OPERATIONAL EFFICIENCY USING PACKET SWITCHED COMMUNICATION TECHNOLOGIES (Migration to packet switched networks)

3 Papers were pre-selected for CIGRE Science and Engineering proposal:

- PS1 D2-119 Mr N. Jung (Korea)
- PS2 D2-209 Mr J. Lin (Taiwan)
- PS3 D2-312 Mr C.M. Son (Korea)

PS1 D2-119

Development of an AI Algorithm and Drone Operation System for Diagnosis of Transmission Facilities in KEPCO (Korea Electric Power Corporation)

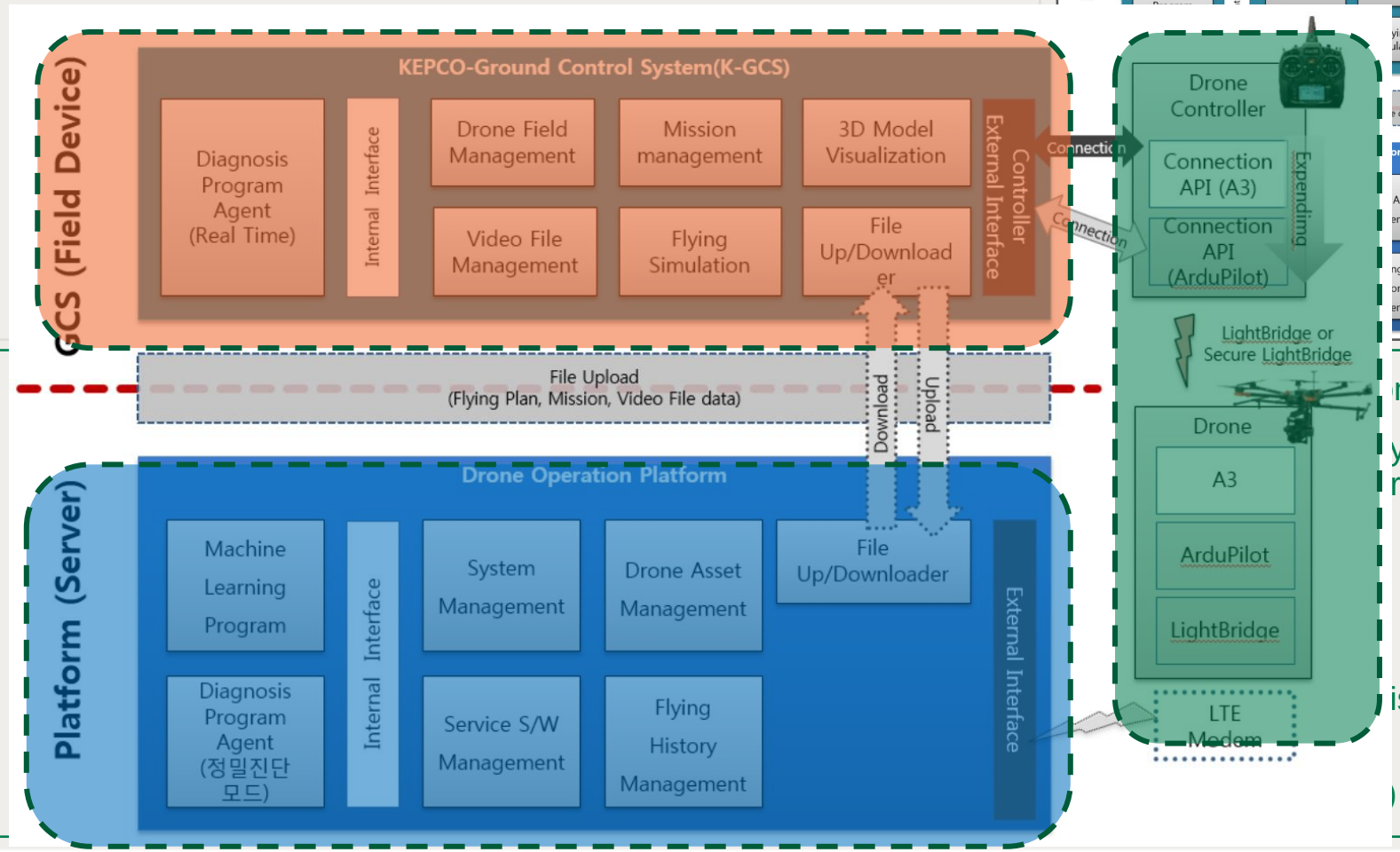
Background

Challenge(s)

Issue(s)

- Inspection and diagnose status of transmission lines and facilities using drone (GCS and drone operation system)

Proposed solution & Bevindingen



matic diagnostics.

y development and regard to artificial

is not suitable for **long-**

PS2 D2-209

Boosting Cybersecurity in Communication Gateways for Better Substation Protection and Control

Background

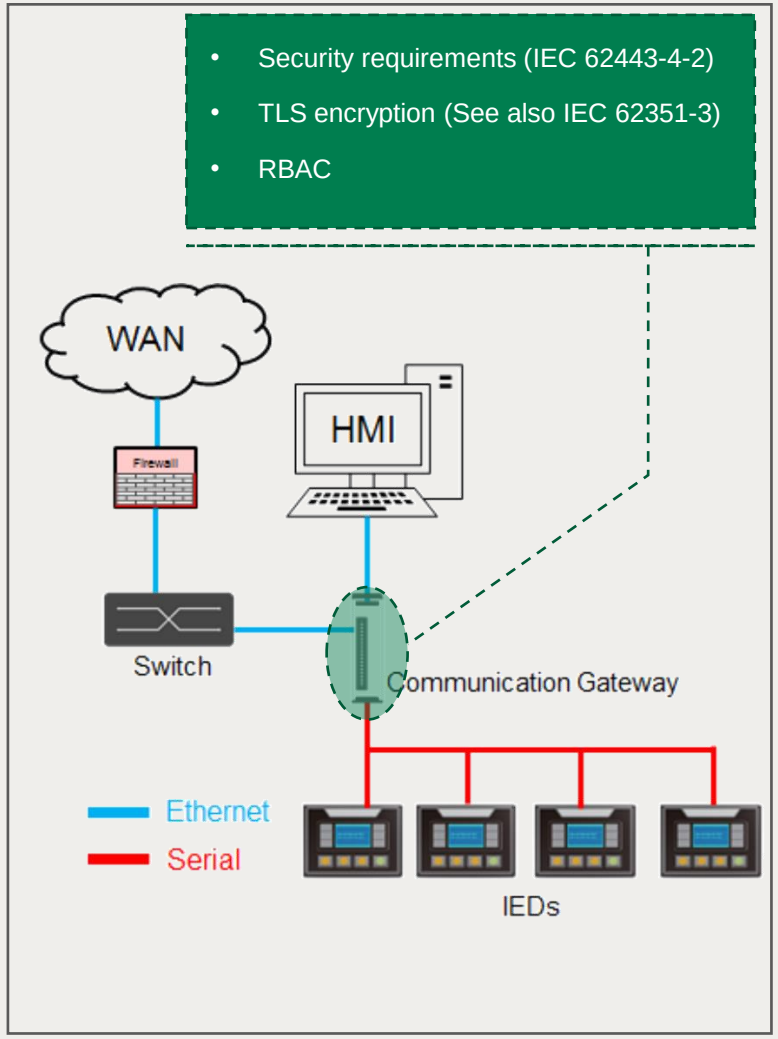
Challenge(s)

Issue(s)

- Converting all substations to digital at once is not so straightforward due to limited budgets to retrofit the large number of serial-based legacy devices.
- Communications gateways offers a solution by allowing serial-based legacy RTUs to communicate with Ethernet-based networks
- BUT Ethernet-based networks are prone to cyberattacks and Communications gateways rarely incorporate adequate security measures, putting the issue of cybersecurity in retrofit power substations at the forefront.

Proposed solution

- Baseline security requirements for communication gateways (IEC 62443-4-2 compliant),
- Communication protocol encryption (TLS v1.2 or later is highly recommended for e.g.: IEC 60870-104 of IEC 61850),
- Role-based access control (RBAC)
- More **stable** and **secure** network infrastructure (At least SNMPv3 capable)
- Network access based on roles of individual users within the network, and communication gateways should be capable of assigning the necessary permission for access to the different role players.



PS3 D2-312

Development of IoT Sensor System for Monitoring/Diagnosis of the Power Distribution System

Background

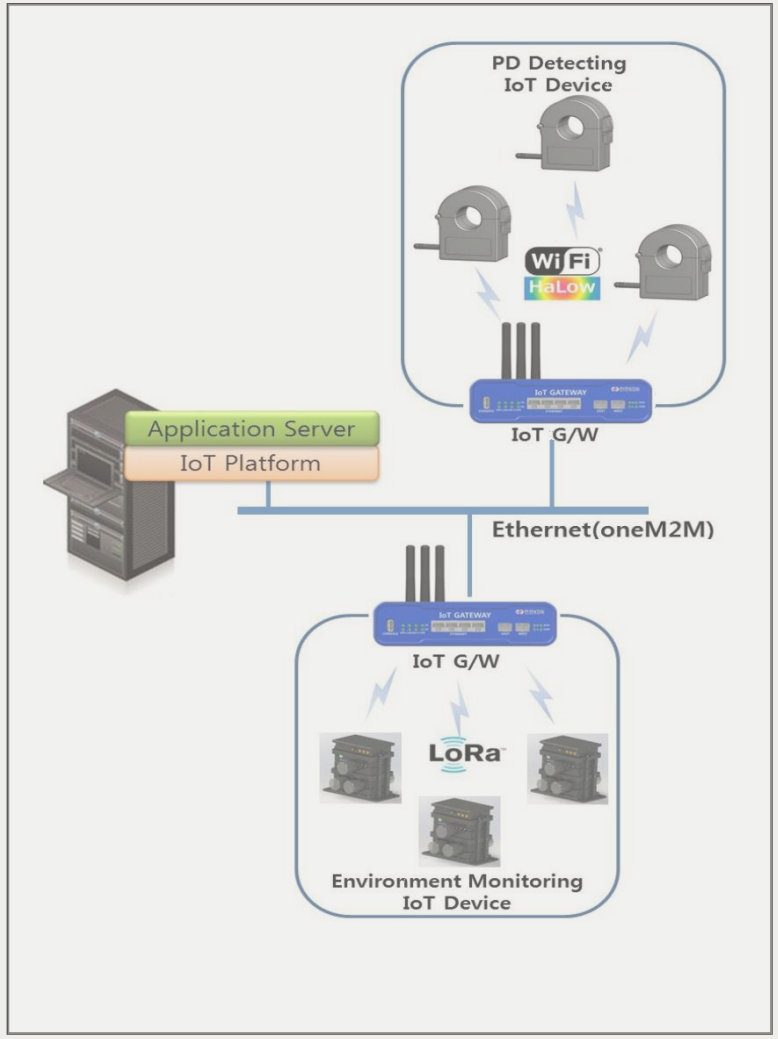
Challenge(s)

Issue(s)

- More fire and safety accidents caused by an increase in old power equipment failures
- Traditional wire-based systems are costly
- Existing Power systems have limitations in accommodating sensors for condition monitoring/diagnosis of a power facility and those for preventing fire and safety accidents

Proposed solution

- IoT-based power facility monitoring and diagnostic system
  - IOT Sensors; IOT gateway; IOT platform
  - Wireless communication (LoRa, WIFI HaLow)
  - Temperature & Humidity; Partial discharges
- Future expectations: Innovative power facility monitoring and diagnosis system by combining with **big data** and **artificial intelligence** technology



Achievements & Future works

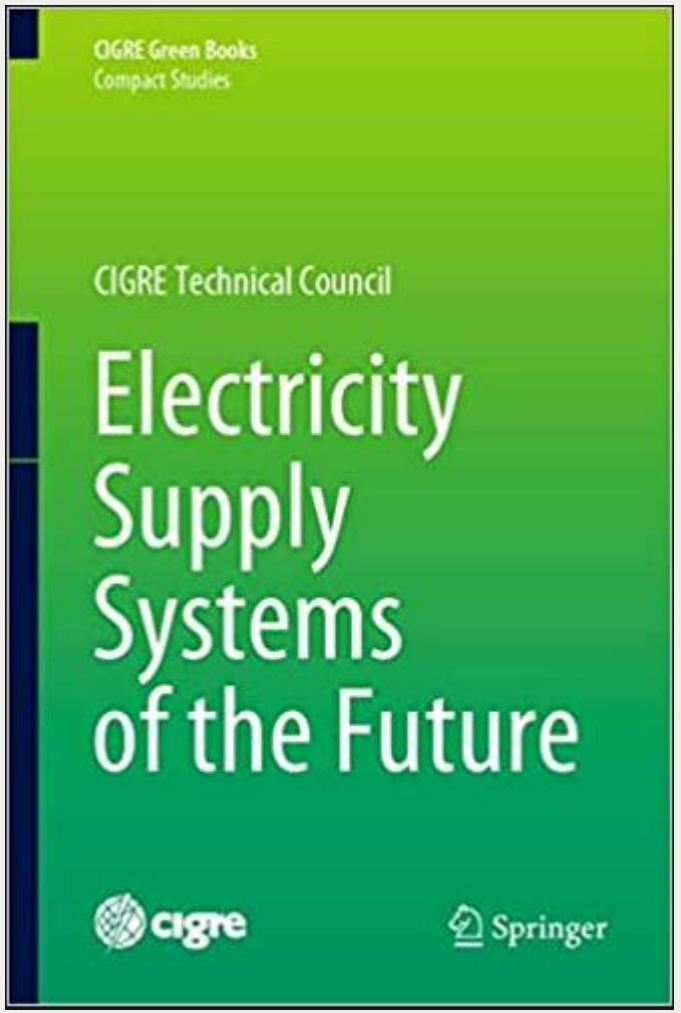
Achievements

- 2 Technical brochures
- Contribution in Green book
- Task Force – Dissemination of CIGRE knowledge in Africa

Publications

- The following Technical Brochures have been published since the last regular meeting:
  - TB 782 “Utilization of Data from Smart Meter System”
  - TB 796 “Cybersecurity: Future threats and impact on electric power utility 150organizations and operations”

- Green book: Electricity supply systems of the future,
  - published in the CIGRE Green Book series in August 2020,
  - comprises contributions from all SCs,
  - Unique and unbiased technical views for the current and future state of electricity supply systems.
  - Current state of the art, available technologies or methods are discussed, but the main focus is on the long-range evolution of each area. A major added value is that the book addresses impacts in a broader sense for society, education, the environment, the economy, etc.



Future Events

- Paris (FR) Session – 21st to 25thAugust 2021SCD2: Regular Meeting for 2021 is to be held in Paris.
- Kyoto (JP) Symposium – 3rd to 8thApril 2022
- Paris (FR) Session – August 2022: SCD2 Regular meeting for 2022 is to be held in Paris along with the Session
- Cairns (AU) Symposium – 4th to 7thSeptember 2023: Active Distribution Network Planning, Operation and Control

New Working Groups

D2.54

D2. 55?

cigre

For power system expertise

WG D2.54: Regulatory approaches to enhance EPU’s cybersecurity frameworks

Start: Januari 2021 – Final report: December 2024

1. Achtergrond

De meningen verschillen over de noodzaak om cyberrisico's te reguleren. Een van de opvattingen is dat de zich ontwikkelende aard van cyberrisico's niet vatbaar is voor specifieke regelgeving en dat cyberkwesties kunnen worden aangepakt met bestaande regelgeving met betrekking tot technologie en / of operationeel risico. De andere mening is dat een regelgevingsstructuur nodig is om het hoofd te bieden aan de unieke aard van cyberrisico's, en gezien de toenemende dreigingen die voortvloeien uit een steeds meer geautomatiseerde energiesector.

2. Scope

- Literatuurstudie (Toepasselijke normen, richtlijnen en rapporten m.b.t. het onderwerp) die kunnen worden gebruikt om, regelgevingsbenaderingen aan te pakken om de cyberbeveiligingskaders van EPU te verbeteren.
- Wereldwijde enquête/onderzoek om EPU-aanbevelingen over hun voorkeuren te vragen, en om hun behoeften beter te begrijpen, verbeterde regelgeving. (Behoefte toezichthouders …).
- Documenteer bevindingen

cigre
For power system expertise

WG D2.55?: Cyber-Physical Power System (CPPS)

Start: Januari 2021 – Final report: December 2022

1. Achtergrond

Modern power systems heavily rely on communications and computer infrastructures for their sensing, protection, control, and real-time operation, hence qualifying power systems as typical CPPS, which changes the way we interact with physical world and power world. The disturbance, failure or attack inside the cyberpart will definitely jeopardize the physical power system operation. The modeling, operation, and stability control of power systems should therefore consider the interdependence between cyber and physical systems.

2. Scope

- Identify and analyze the specific accidents of power systems or blackouts caused by cyber-physical coupling cascading failures
- Application of digital twin (DT) in high-precision real-time simulation and pre-decision-making of CPPSs.
- joint-simulation methodologies for co-simulation of physical power grids and communication network in power systems such as based on Simulink/ OPNET, DIgSILENT/ NS3

cigre
For power system expertise

STUDY COMMITTEE D2

INFORMATION SYSTEMS AND TELECOMMUNICATION

cigre

For power system expertise