ESMAP
Energy Sector Management Assistance Program

MINISTERO DELL'AMBIENTE E DELLA SICUREZZA ENERGETICA

WORLD BANK GROUP

Terna

RSE Ricerca Sistema Energetico — we move research

CESI — Inspired with innovation

acea

gridspertise — accelerating your electric future

ESMAP Knowledge Exchange & Study Tour on Grid Digitalization and Cybersecurity

May 20 - 27

Italy

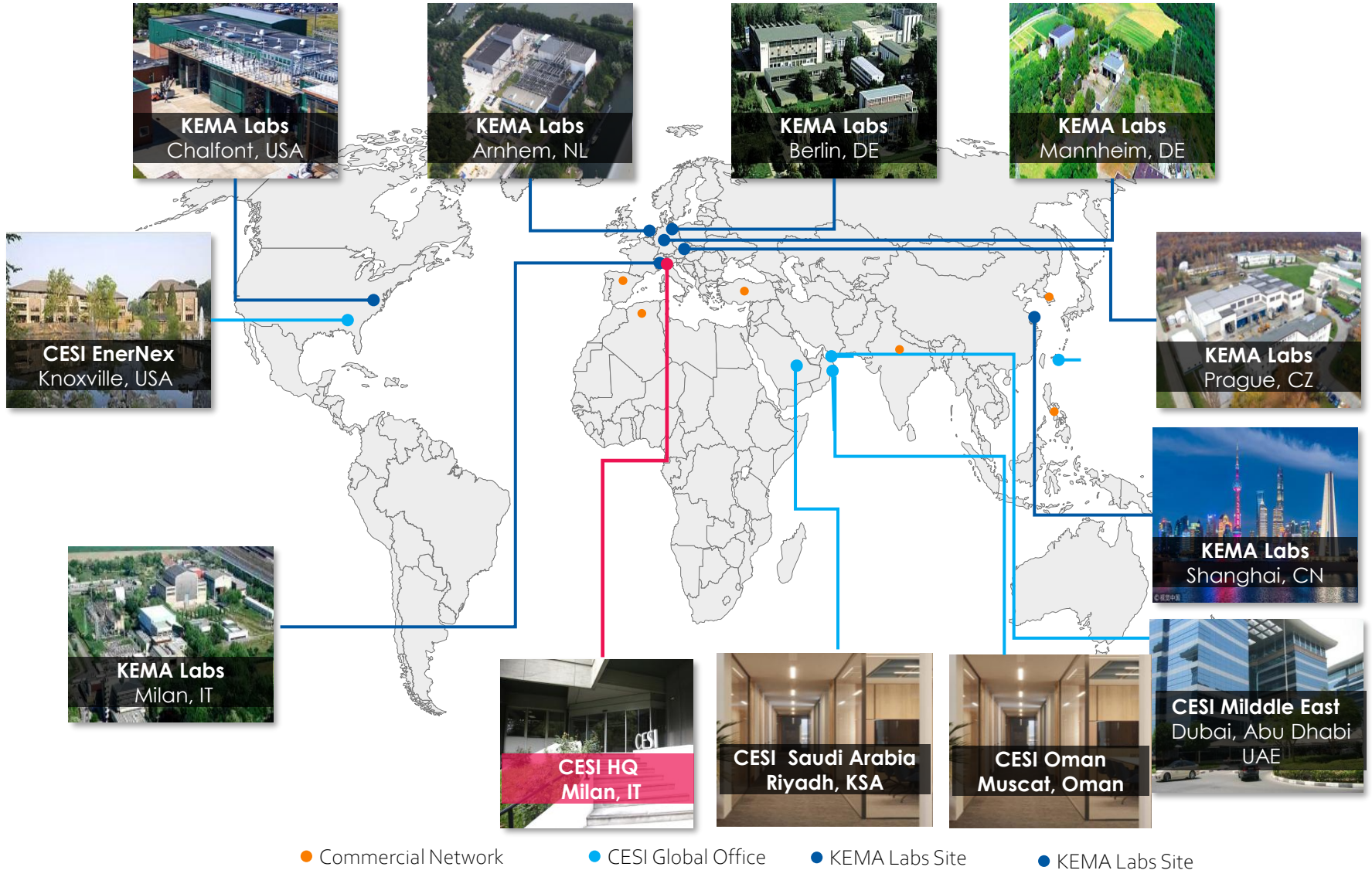
A Global Player in Engineering, Testing and Power Systems Consulting

~2,000
Professionals

2,000+
Clients

70+
Countries Served

12
Global Sites



High-end, Tailor Made Solutions for our Global Clients

Testing, Inspection & Certification

KEMA Labs

The Global Leader in Independent Testing, Inspection and Certification for the Electricity Sector

Energy Consulting

CESI Consulting

Our Expertise in The Energy Industry at Your Disposal Through Ad-hoc Consultancies

Environmental Consulting & Civil Engineering

CESI Consulting

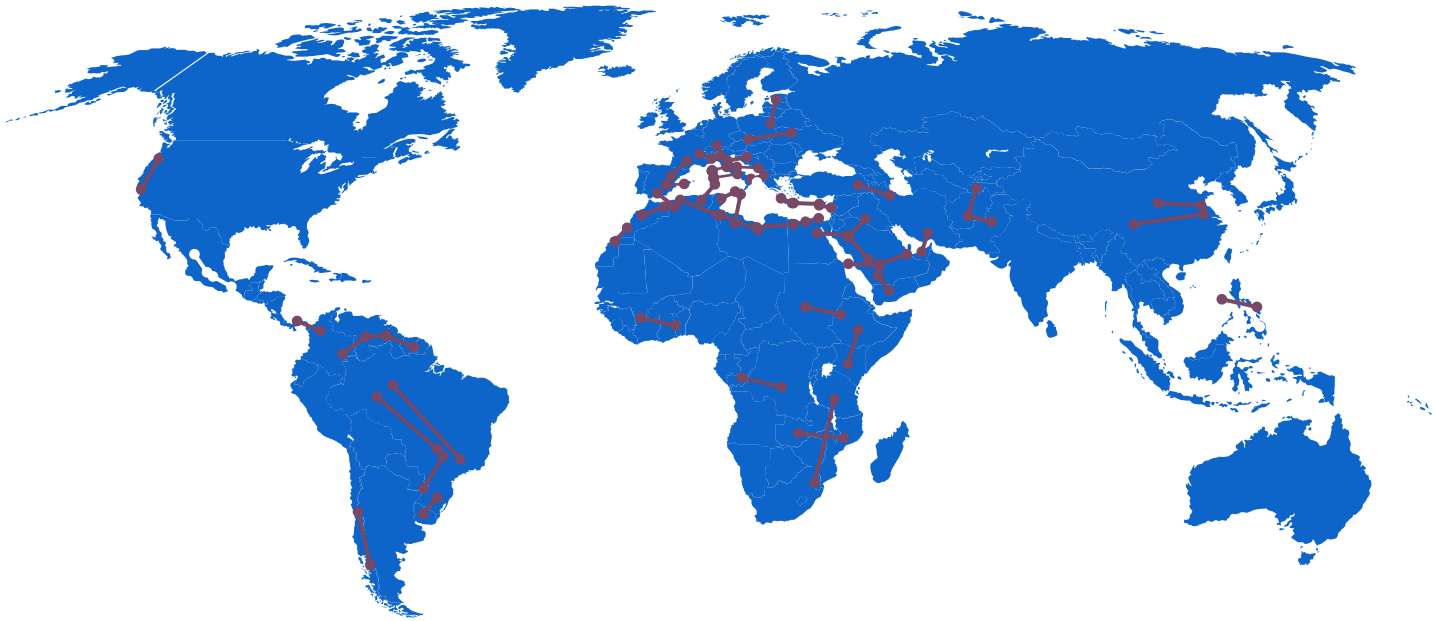
Renewable Engineering, Remediation, Compliance and Monitoring Services to Drive Circular Economy

Space Solar Cells

CESI Space

Production of Advanced Multi-junction Solar Cells for Space Applications

Energy - Transmission Planning & Engineering



> 30 HVDC projects realized

> 100.000 Km OHTL and power Cables

> 50 different power systems analyzed

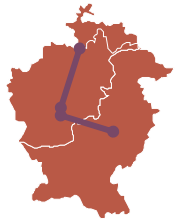
Services for the entire Project life-cycle

- Feasibility and Power System studies, Master Plans, CBA, Market studies
- Technical specification and Procurement support, Design Review and QA
- Construction and Commissioning supervision

Crossing the Mediterranean

Since the 80's walkable ways to cross the Mediterranean with submarine cables.

The CASA-1000 Project



Full owner's engineering for the 500kV HVDC transmission line in Afghanistan.

Linking the Arab World

CESI is entrusted in fostering regional interconnections to enhance power export.

Energy - Grid Modernization

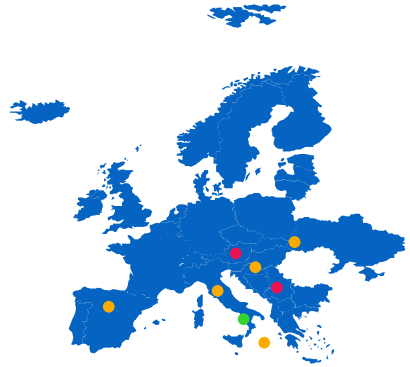
AMI Infrastructures · Distribution Grid Mod · Smart Grid for Transmission

Americas

Next Generation Demand Response

EnerNex evaluated DR for CAISO integration identifying technologies for different DR applications

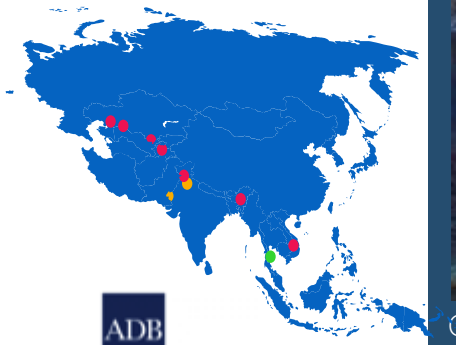
Europe



Control Center Terna

CESI as strategic partner of TERNA in the development of tailor tools and methodologies for its Control Room

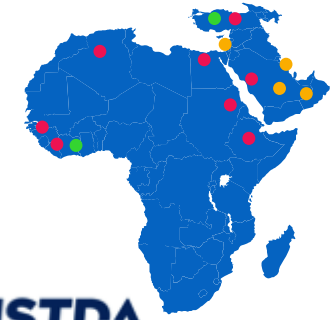
Asia Pacific



Advance Metering Infrastructures Pakistan

CESI is the owner's engineer of the first two stages of the AMI program in Pakistan, funded by ADB covering IESCO and LESCO DISCOs

Middle East & Africa



Smart Grid Roadmap Ivory Coast

EnerNex is supporting CI-ENERGIES on reducing losses and improve its electricy network tech & commercial performance

Digital Grids & System Operations in the Data Era

Massimo Salvetti

Power Transmission Operation Director

From operational complexity to data-driven stability

Digital Grids & System Operations in the Data Era

Grid transformation drivers

Digital Grids & System Operations in the Data Era

Impact on system operations

Without structured data governance, grid operation becomes unsustainable

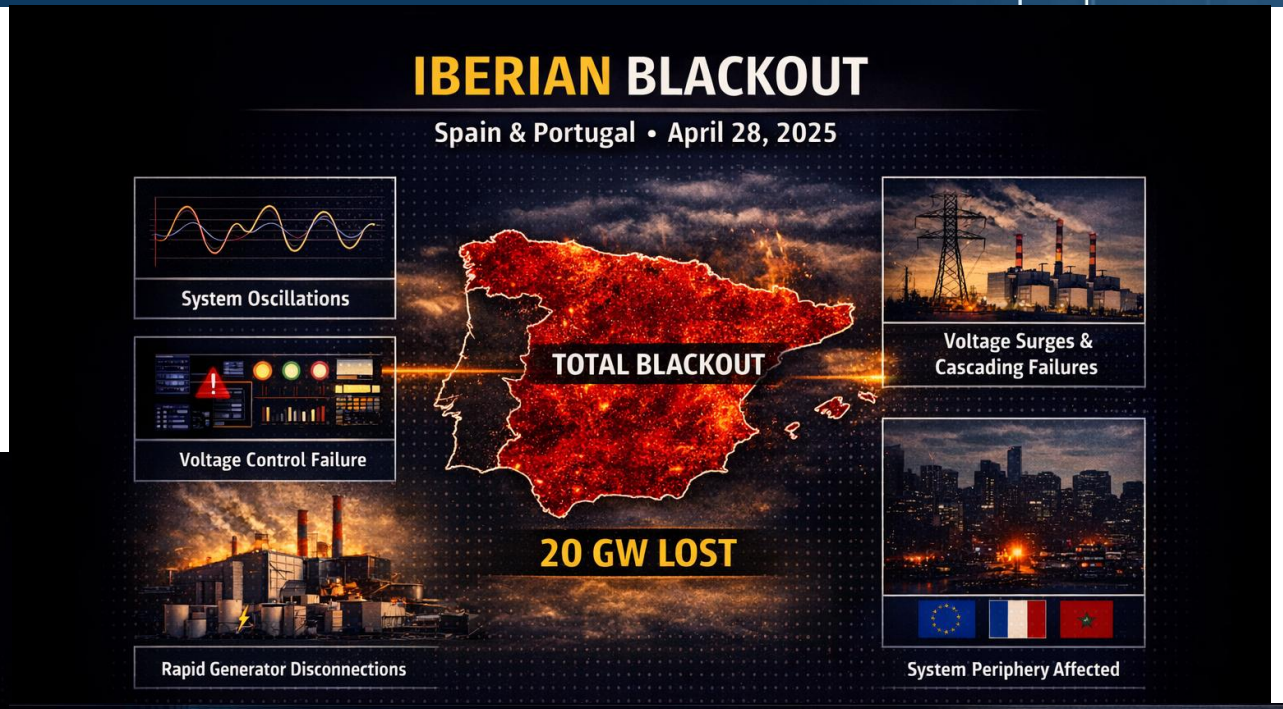
Digital Grids & System Operations in the Data Era

The real challenge: governance

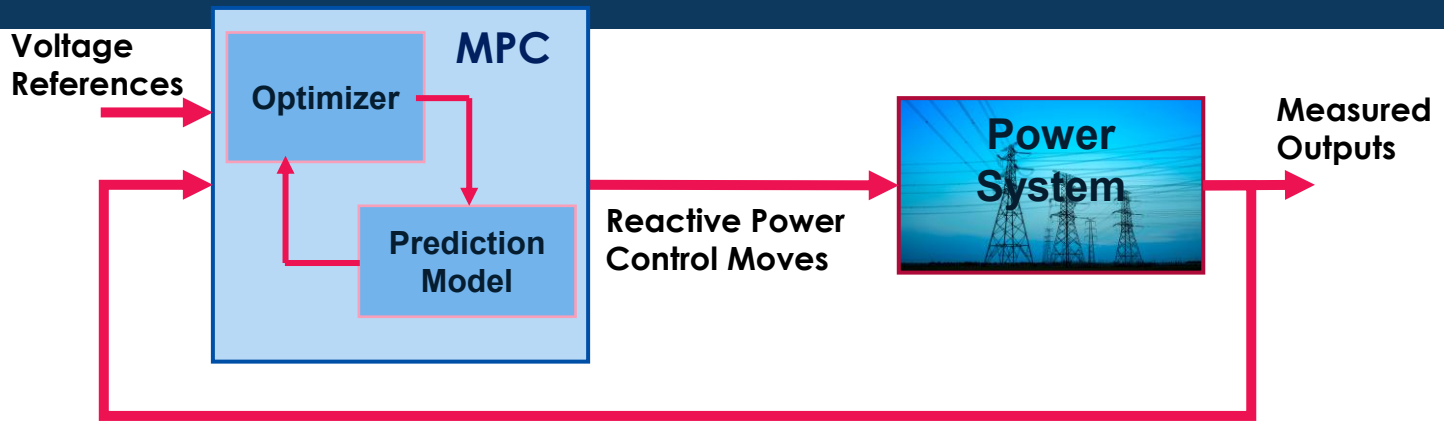
- Operational (SCADA/EMS)
- Network studies & models
- Asset & GIS
- Generation & DER
- Load & AMI
- Forecast & Weather
- Market
- Events & Alarms
- Cyber & Telecom

Digital Grids & System Operations in the Data Era

The real situations

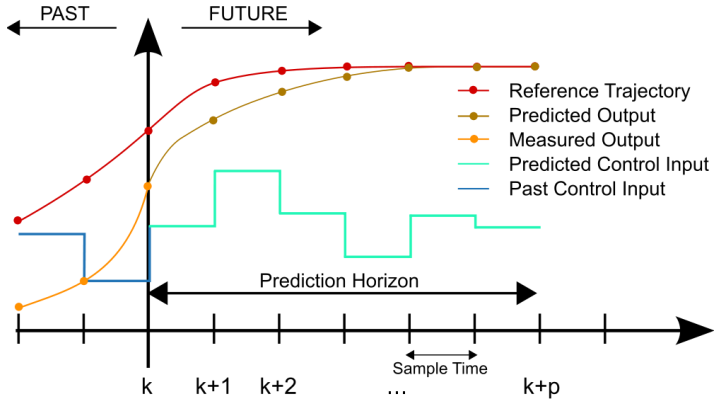


Data Driven Approach: Voltage Regulation on TSO network



Optimizer: the optimization is based on the future evolution of the process (predicted by the model)

- At time **k**:
  - It solves an optimal control problem on a future horizon of N steps:
    - ➢ Minimize g(·)
    - ➢ Subject to physical constraints
- Only the first of the optimal sequence of moves is applied
- Once new measurements are obtained, the optimization is repeated at time **k+1**



Predictive model: A model of the process to be controlled is required to predict the future behavior of the process itself

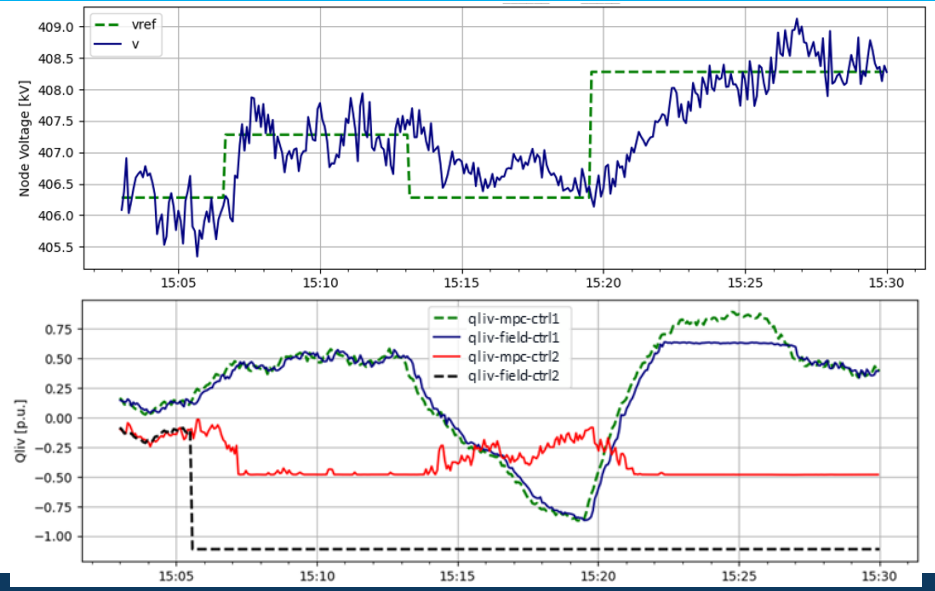
State-space model:

$$\mathbf{x}_{k+1} = \mathbf{A}\mathbf{x}_k + \mathbf{B}\mathbf{u}_k$$
$$\mathbf{y}_k = \mathbf{C}\mathbf{x}_k + \mathbf{D}\mathbf{u}_k$$

Identification technique: Dynamic Mode Decomposition with Control (DMDc)

Results

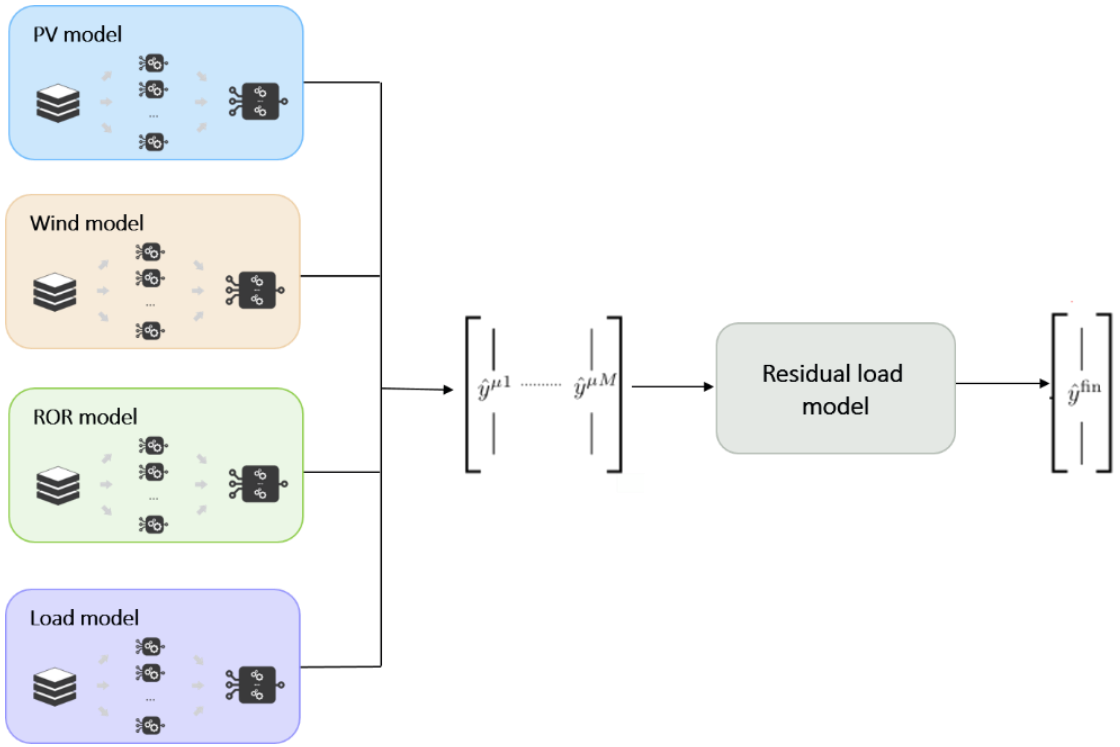
- Based on the predicted future states, the **MPC algorithm computes the optimal reactive power levels** to achieve the desired nodes voltage references.
- The feedback loop **allows the MPC to adapt and adjust its control strategy based on real-time data**.
- Being "offset-free", it guarantees **zero-offset tracking of reference signal**.
- The **data-driven MPC leverages available data to build a data-driven model** of the system behavior directly from measured or simulated input-output data.
- This data-driven approach offers advantages in terms of system understanding as **it can handle complex and nonlinear MIMO systems without explicit mathematical models**.



Machine Learning for Nowcasting: Short-term Balance on TSO network

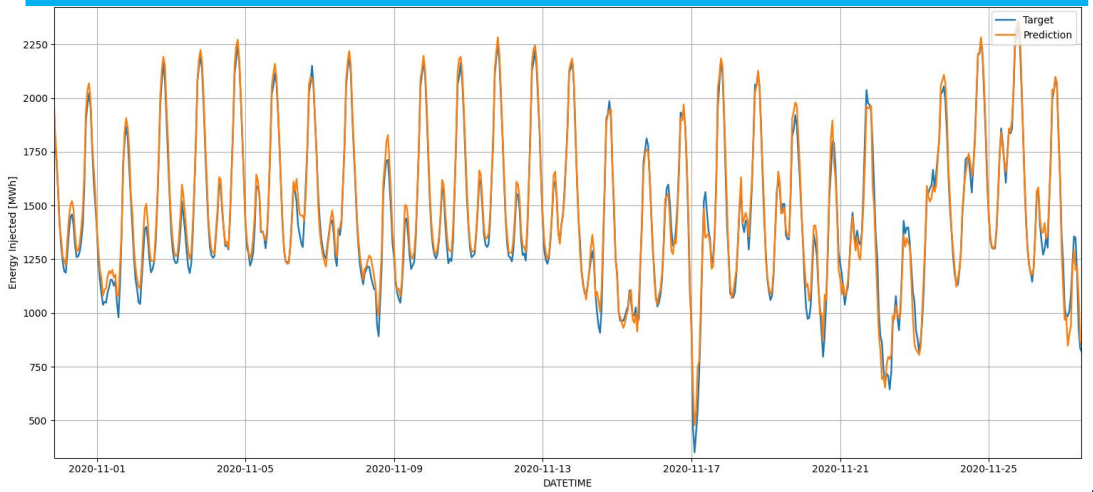
- The objective of the project is the **short-term forecasting of the energy imbalance** (i.e., residual load) and of its components (photovoltaic, wind, hydro power generation and electric load) for the market zones.

- The solution benefits from two short-term forecasting model:
  - **Meteorological model**: to generate historical data with a spatial resolution consistent with the target.
  - **Imbalance model**: to integrate the meteorological model into the imbalance forecasting process. The imbalance model is structured to forecast individually the imbalance components and then reconstruct the imbalance equation.



Results

- The **"virtual" meteorological stations** allow to align the spatial granularity of weather forecasting and production power plants.
- The meteorological model belongs to the family of **LEPS (Limited-area Ensemble Prediction System)**. The LEPS methodology allows through **downscaling techniques** to increase the spatial resolution of global models.
- The imbalance forecasting benefits from **a bottom-up approach** that exploits the **hierarchical nature** of the time series modeling the single contributes and then aggregating them**.**
- Each model follows an **ensemble approach** noted as **«model stacking»**, i.e., a staked form of more forecasting models.
- Different **machine learning and statical model** are combined to obtain a predictive model with a **greater predictive power** than the single models.
- The ensemble approach guarantees **high scalability**, more models can **run in parallel** to optimize the entire estimation process.

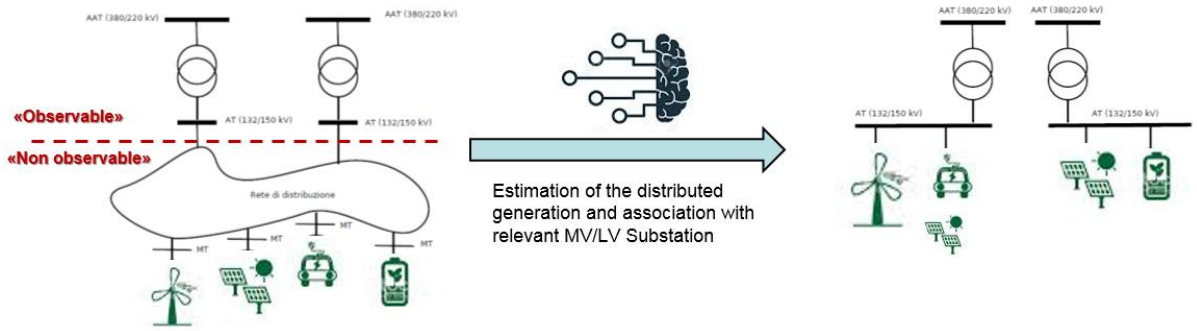


CONFIDENTIAL-LIMITED USE

Machine Learning for Pattern Identification: RES Observability

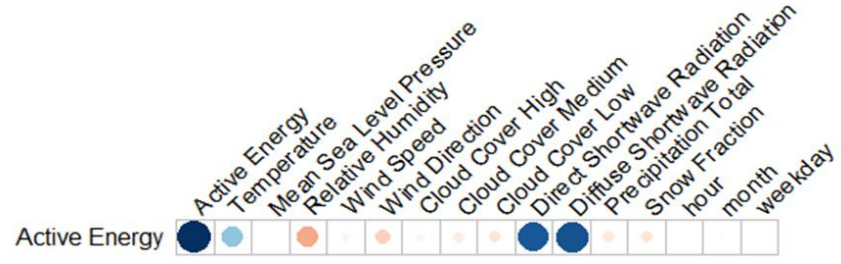
The objectives of the project are:

1. The **estimation of the distributed generation**:
2.



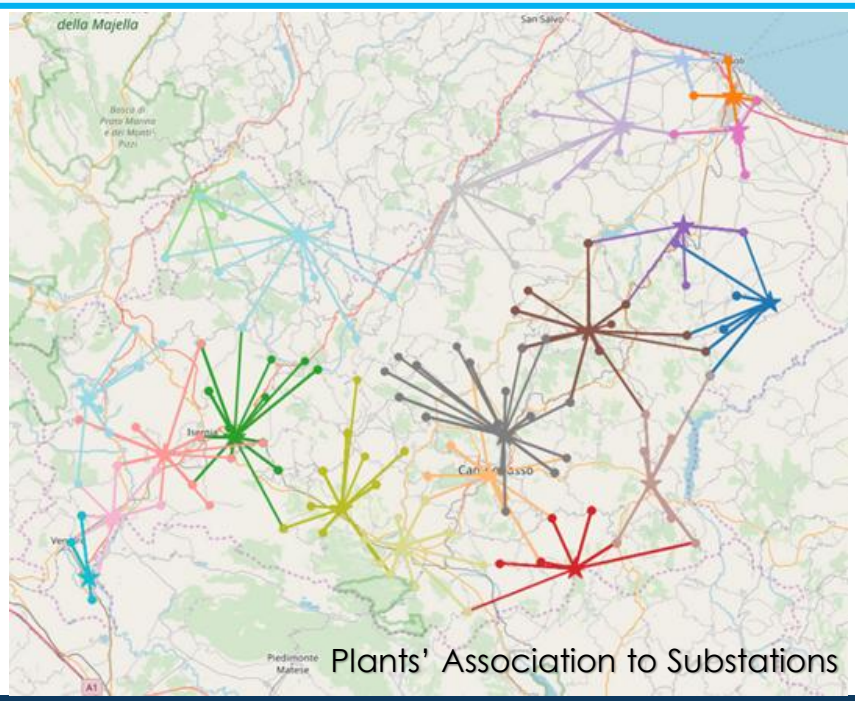
1. **Estimation of the distributed generation**: an **ensemble model approach**, where each **distributed generation family** (i.e., solar, wind, hydro and thermal power plants) is estimated independently and then the resulting forecasts are aggregated. The aggregation directly involved an estimation of the percentage of contribution of each family to the power to be given by the TSO at MV/LV Substation level.

2. **Association of DGs to the substations**: the association of each distributed generator to the substation to which it belongs is performed by an optimization process. Such process consists in an **iterative process** (**"random walk"** in the assignments space) where at each iteration a generation plant is detached from the current substation and attached to one nearby.



Results

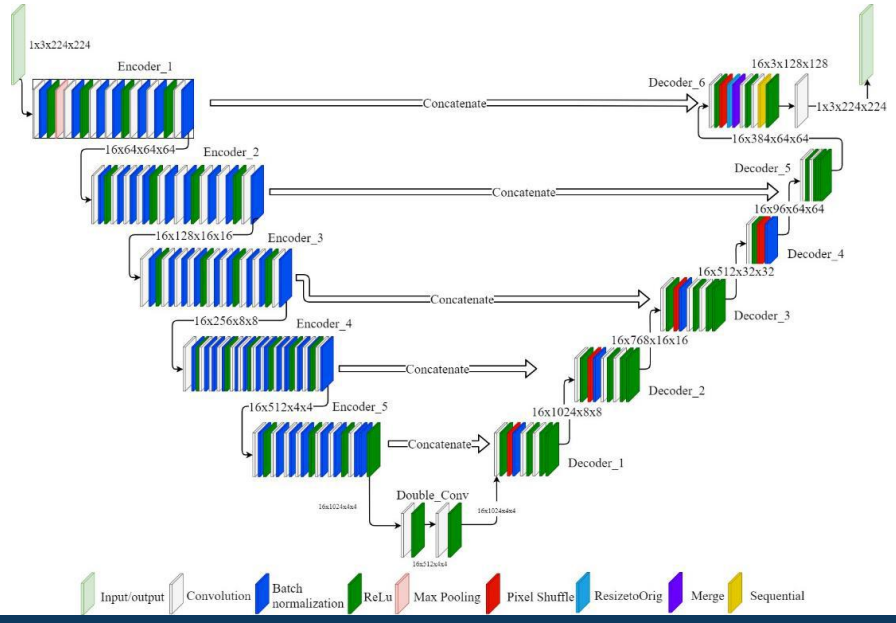
- All models are independent one from each other and can be also made with **different machine learning techniques**, completely adapting to the typical behavior of **the specific family**.
- The model selection involves **kernel methods**, **neural networks** and **ensemble methods** (as **random forests**).
- The implementation ensured the best trade-off between **data robustness and granularity** to model plants' association to the most likely substation.



Plants' Association to Substations

Machine Learning for Image Pattern Recognition: Rooftops for PV installation

- The **general objective** of this study is to conduct an opportunity analysis for increasing the contribution of rooftop solar PV to the electricity mix in Jamaica.
- The essential step is the buildings' identification and the method adopted was a **semantic segmentation analysis** applied on satellite images.
- This technique is a **supervised method** allowing to detect the rooftop footprint layer by means of a pixel-wise image segmentation.
- Since the prediction is performed for every pixel in the image, the expected output is not just a label, but an image (called **mask**) with a binary classification of two classes:
  - Building
  - Background
- The **neural network architecture** that we considered is a U-Net employing a **ResNet 34** as encoder. This network is the state of the art in the **semantic segmentation field**.



Results

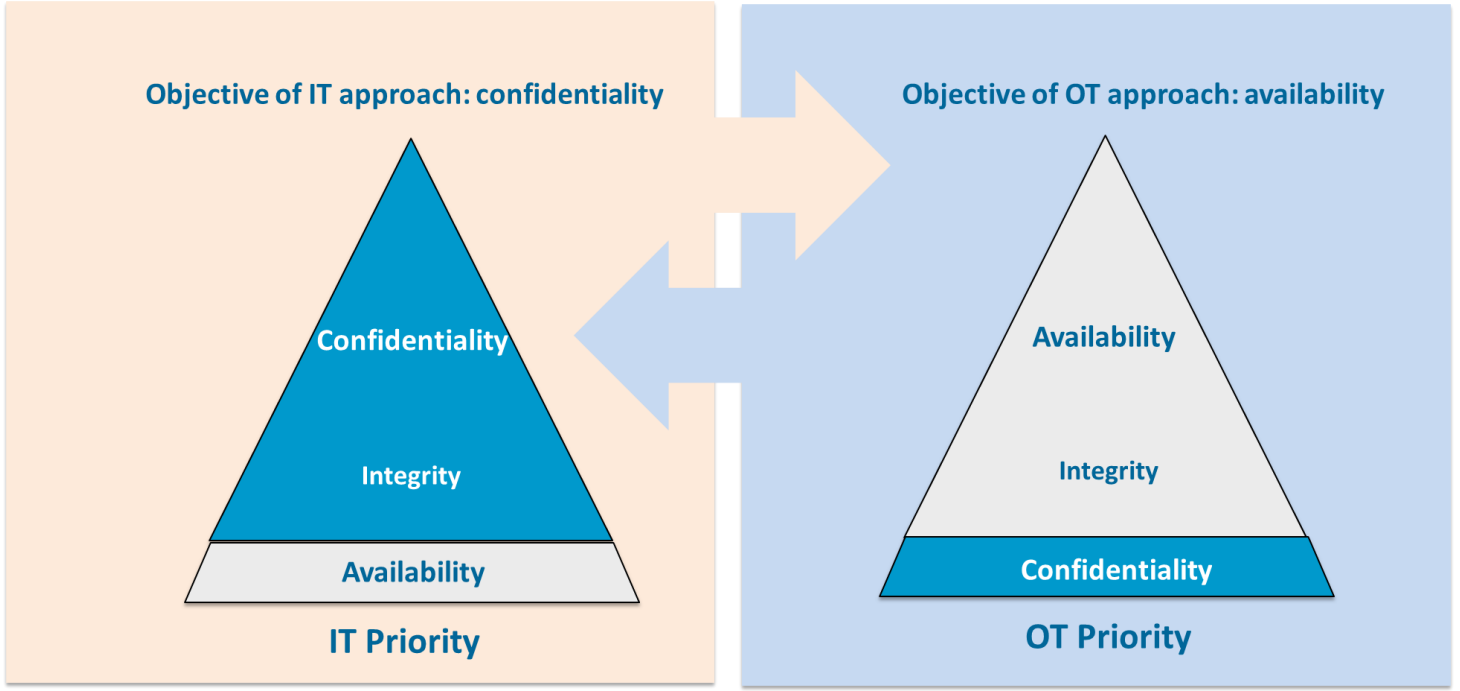
- To evaluate the model performances, we consider a metric that is broadly employed in this research field, namely the **Dice Similarity Coefficient (DSC)**.
- The DSC is usually preferred to others per-pixel accuracy metrices because it is particularly informative in scenarios characterized by a **strong imbalance between classes**.
- This characteristic **fits particularly well with the rooftop analysis** since the portion of the image referring to the background is usually greater than the area referring to buildings.
- The forecasts of the model can **identify the rooftops in both urban and rural areas.**

World Bank - ESMAP Digital and Cybersecurity Knowledge Exchange Study Tour Italy

Aldo Curtoni - Product Leader SCADA & Operational Technologies, CESI

Cyber security for Operational Technology – OT vs IT General Framework

OT technologies have different requirements compared to IT and Constraints when applying safety measures -> ensure that these systems can continue to support the same levels of safety and reliability of the power system.



The OT dilemma

Securing a system can introduce operational risk — a patch can cause instability, a firewall can block a critical command

Tailored approach

OT cybersecurity is a management of compromises — each measure must be operationally validated before deployment

Guiding Principle: Security by design

if security is not projected from the beginning surely there will be problems

Case History 1 – Secure design and technical specifications of a SCADA/EMS System

Purdue Model: based on the physical and logical separation between the different layers of the architecture. This separation reduces the risk of interference and compromise of safety between the different components of the industrial control system, while ensuring the integrity and reliability of the production process.

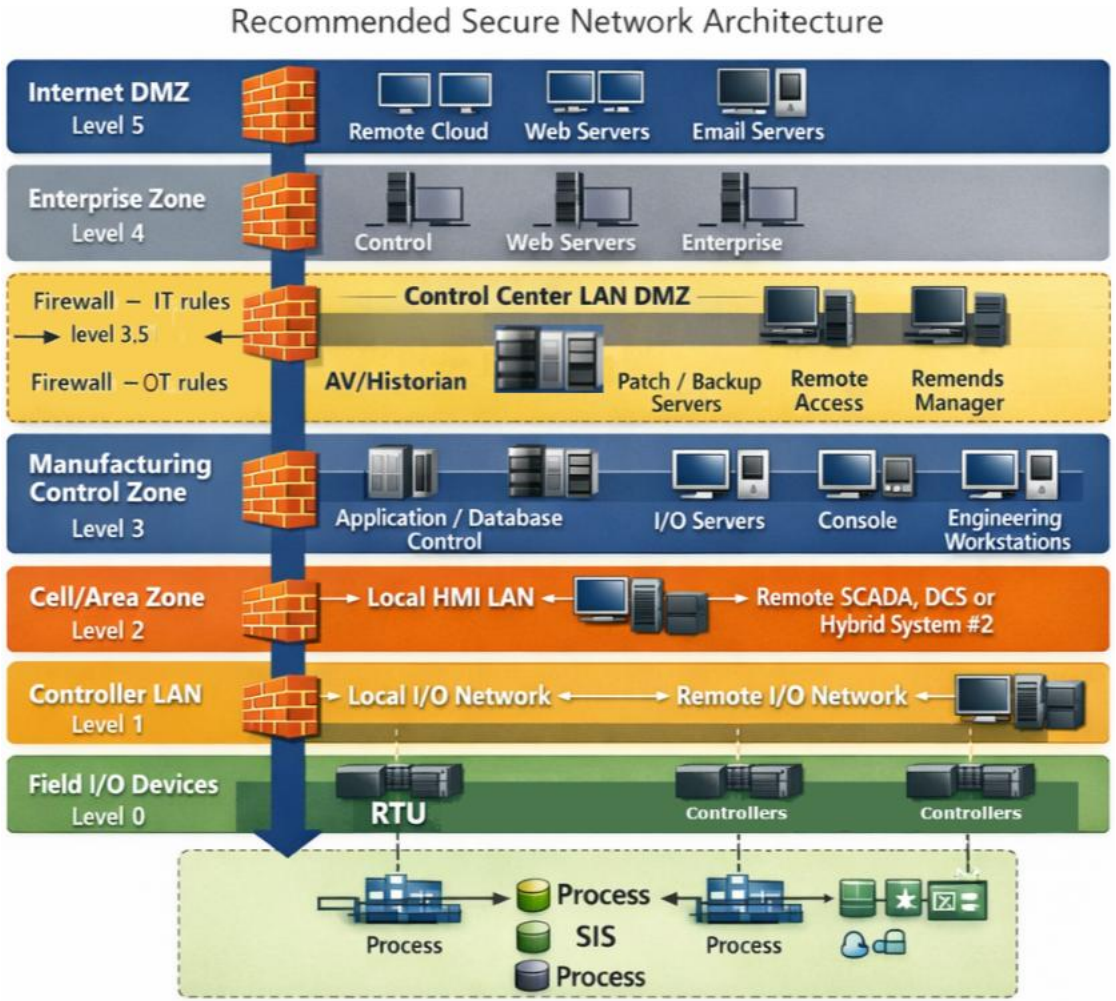
The minimum number of levels that the **SCADA/EMS system** must be organized is as follows:

Levels 0, 1, and 2: Substation area including RTUs and Telecommunications

Level 3: Communication servers and SCADA/EMS application at the National Control Center

Level 3.5: Demilitarized Zone (DMZ);

Levels 4, 5: IT and Enterprise Networks.



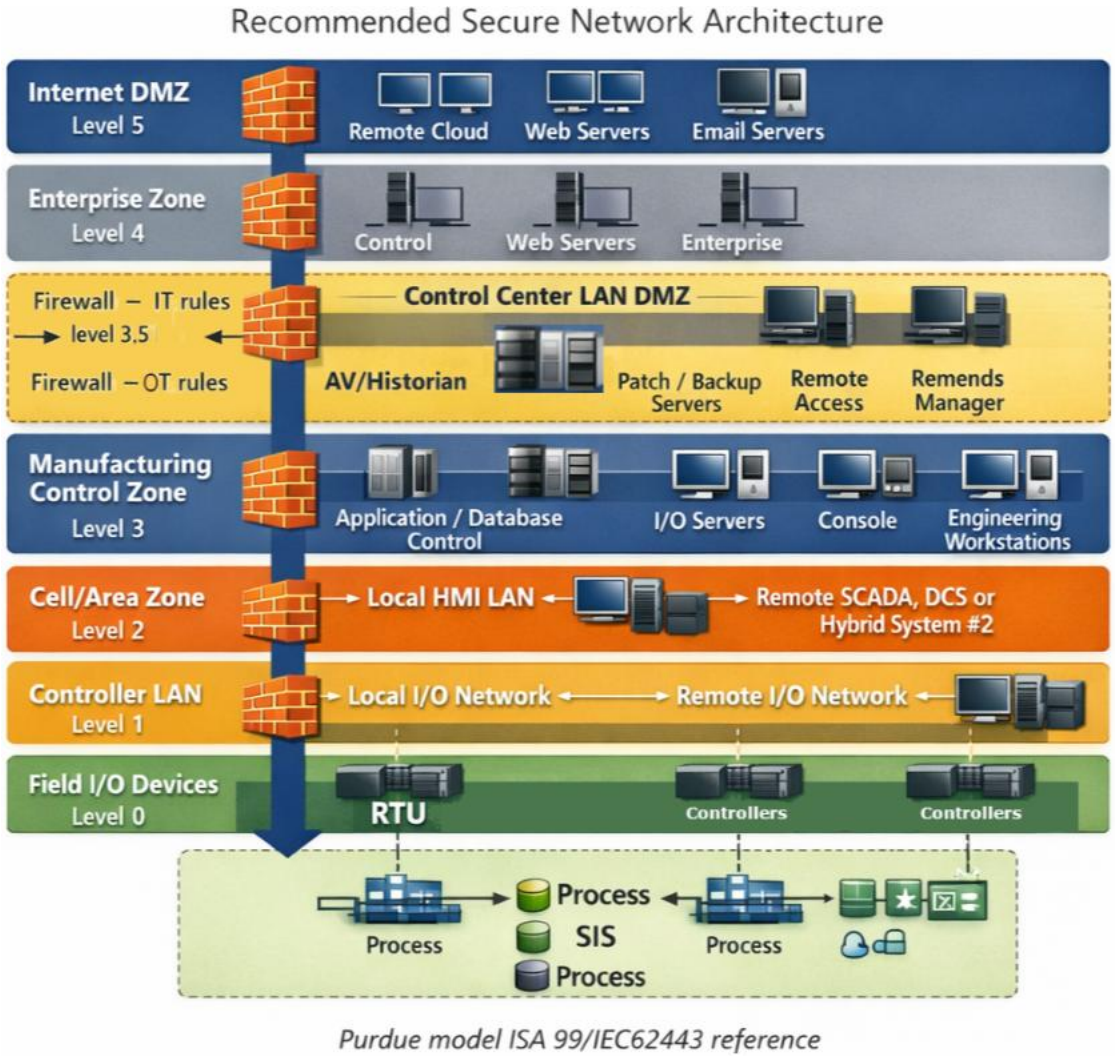
Purdue model ISA 99/IEC62443 reference

Case History 1 – Secure design and technical specifications of a SCADA/EMS System

Physical and virtual segmentation: To limit access to services and resources, the bidder must define the different security levels of each local network. The different levels will have to correspond to different access privileges, expressed according to pre-established and configurable policies.

LAN monitoring systems: Network devices such as "**Next Generation Firewalls**" and routers must constantly be monitored by specific software to identify anomalies and malfunctions.

Identity and Access Management (IAM) Infrastructure The Identity and Access Management (IAM) system must be able to centralize the management of the identities of users and services, including the identity lifecycle.



Purdue model ISA 99/IEC62443 reference

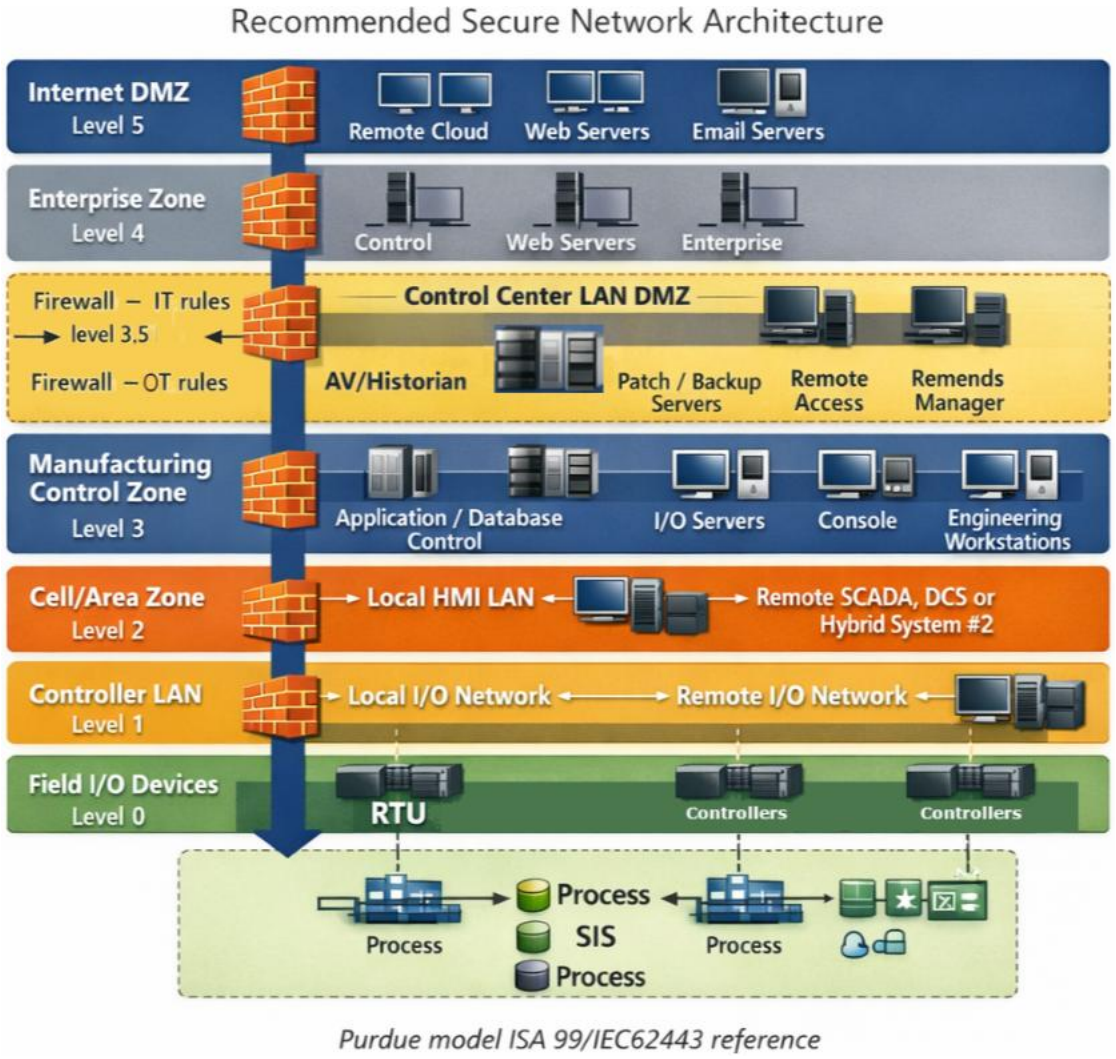
Case History 1 – Secure design and technical specifications of a SCADA/EMS System

IDS/IPS - Intrusion Detection System/ Intrusion Protection System: Products that can detect and prevent intrusions in the SCADA/EMS system based on protocol analysis.

Extended Detection and Response (XDR) cybersecurity framework that unifies threat detection, investigation, and response across multiple layers acting as a SCADA for cybersecurity.

Cybersecurity Standards

Standard	Description
NERC CIP-002	BES Cyber System Categorization
NERC CIP-003	Security Management Controls
NERC CIP-005	Electronic Security Perimeter(s)
NERC CIP-006	Physical Security of BES Cyber Systems
NERC CIP-007	System Security Management
NERC CIP-008	Incident Reporting and Response Planning
NERC CIP-009	Recovery Plans for BES Cyber Systems
NERC CIP-010	Configuration Change Management and Vulnerability Assessments
NERC CIP-011	Information Protection
NERC CIP-012	Cyber Security – Communications between Control Centres
IEC 62443-1-1	Terminology, Concepts and Models
IEC 62443-3-3	System security requirements and security levels
IEC 62443-4-1	Product security development life-cycle Requirements
IEC 62443-4-2	System security requirements for industrial automation and control systems (IACS)
IEC 27001	Information security, cybersecurity and privacy protection — Information security management systems
IEC 27002	Information security, cybersecurity and privacy protection — Information security controls.
IEC 27005	Information technology — Security techniques — Information security risk management.
NIST CSF 2.0	National Institute of Standards and Technology Cybersecurity Framework (CSF) 2.0
NIS/NIS2	European Network and Information Security legislation / version 2
NIST-SP800	NIST series on computer/cyber/information security guidelines, recommendations and reference materials
IEC 62351-Series	Gestion des systèmes électriques et échanges d'informations associés – Sécurité des données et des communications.



Purdue model ISA 99/IEC62443 reference

Case History 2 – Cybersecurity assessment and impact evaluation of NIS for a DSO

- **CyberRisk Assessment** is a complete security consultancy service, which involves all engineering processes.
- **Identify, evaluate and estimate** the level of risk considering threats as well as their consequences.

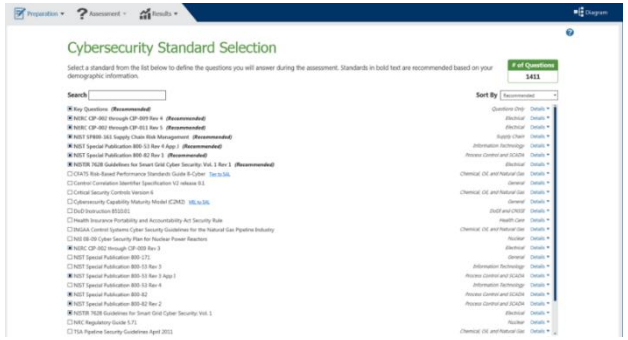
Risk Assessment Matrix

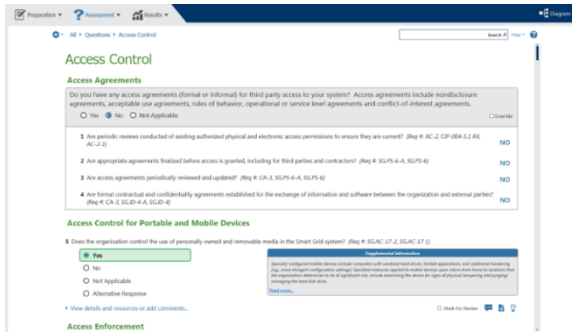
		Likelihood of Incident Scenario				
		Very Low	Low	Medium	High	Very High
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

Bow-Tie models used for process risk evaluation

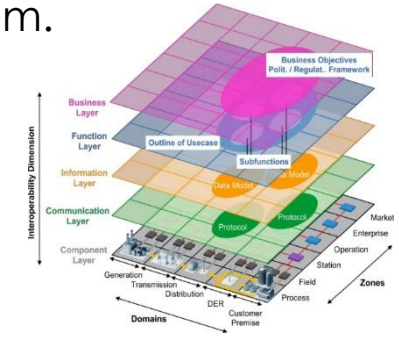
- An **acceptable level of risk** is determined both by the safety levels achieved, but also by the application context of the systems and infrastructures concerned.

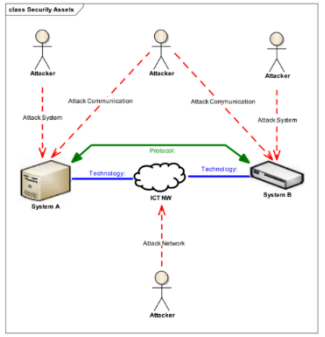
- **Q&A approach:** consisting of an appropriate list of questions (typically based on one or more international standards); based on related answers, it is possible to build summary reports useful for highlighting the critical points of the system.





- **Modeling approach**: a system model is constructed using a standard modeling language (i.e. UML) also describing the possible vulnerabilities and sources of risk directly connected to the elements of the system.

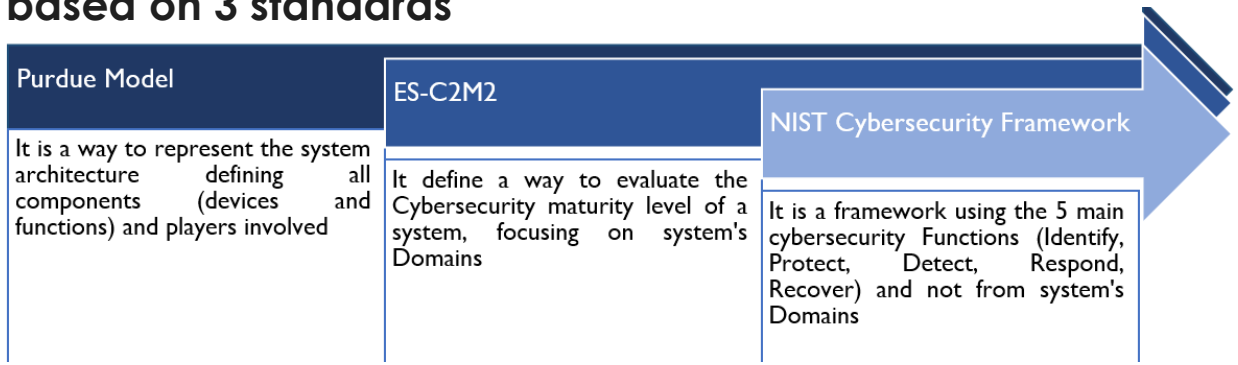




Sources:
- **CSET (U.S. Department of Homeland Security)**
- **SGAM Toolbox (UML Language)**

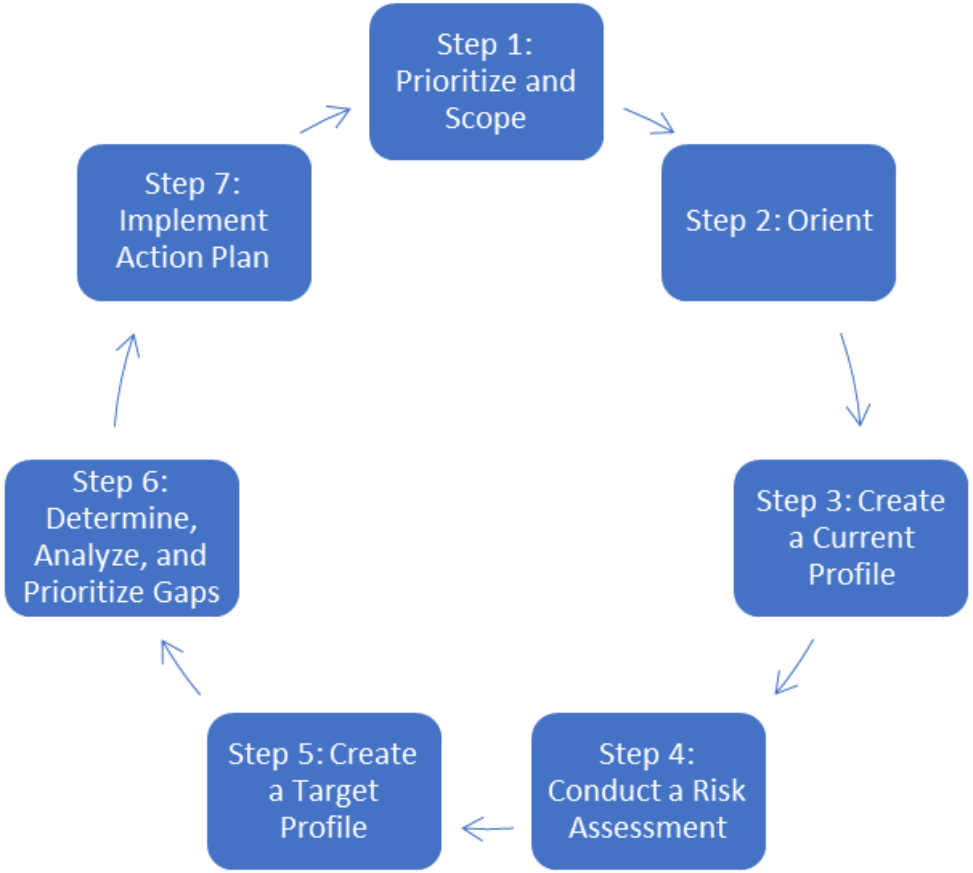
Case History 3 – Definition of a Common Cybersecurity Plan for a Multi-Country Project

Definition of a Cybersecurity Plan and roadmap based on 3 standards



Outputs

Step 1: Framework usage scope: guide the improvement of the organization's cybersecurity capabilities
Step 2: Identifies in-scope systems and Assets (e.g., people, information, technology, and facilities)
Step 3: Creation of the "as-is" profile of the company
Step 4: Conduct risk assessment
Step 5: Define the improvements: Target Profile
Step 6: Prioritized implementation plan
Step 7: Implement Action Plan with investment evaluation



CESI 1956 -2026

Inspired with innovation

AMI & Simulation impact on DSO

Francesco Cappuccio | Product Leader,
Advanced Metering Infrastructure

CONFIDENTIAL-LIMITED USE

Where AMI & Simulation Deliver Immediate Impact

Stop measuring digitalization success determined by the number of operational decisions it enables per month.
Three operational dimensions for case history: Losses, Resilience, Efficiency.

LOSSES

- Loss reduction program
- AMI Standardization

Where do Utilities struggle?

- Loss reduction programs are not actionable
- AMI interoperability / interchangeability

RESILIENCE

- Resilience Assessment Framework

Where do Utilities struggle?

- Unified resilience assessment methodology
- Incomplete model for data aware decisions
- Situational Awareness

EFFICIENCY

- Scalable Reliability Optimization for Distribution Networks

Where do Utilities struggle?

- Distribution network size (too big!)
- Heterogeneous asset data
- Lack of quantified reliability impact

Losses Reduction Program

Recalculation of technical losses

- Run **MV load-flow simulations** using the validated model and representative operating days.
- Simulate **representative LV networks** and annualize losses across the full population.
- **Validate model outputs** against measured energy balances and historical results.

Quantify non-technical losses

- **Classify non-technical losses** by cause and source: metering, billing, administrative gaps, theft, and authorized / unauthorized unmetered use.
- Develop a **monitoring framework** that supports monthly reporting and exception tracking.

Translate results into action

- Identify the **dominant loss drivers** by feeder, voltage level, transformer group, and LV configuration.
- Screen **technical and commercial measures** using engineering sensitivities and economic metrics.
- **Prioritize interventions** and build an implementation roadmap for DSO.

CESI Approach adds implementation value beyond the loss calculation itself.

Analytics-driven reconciliation
Link SCADA, metering, GIS, billing, and customer data into a single evidence trail that supports model validation and non-technical loss analysis.

Scalable technical modelling
Use the full MV digital twin where feasible; otherwise shift to statistically representative MV/LV networks that remain auditable and practical.

Reusable reporting framework
Provide DSO with a technical/commercial loss reporting logic, KPI structure, and model inputs that can be reused in future assessments.

Outcome-oriented recommendations
Recommendations are screened for technical relevance, benefit, feasibility, and implementation sequencing — not presented as a generic catalogue.

AMI standardization Challenges

CESI experience grounded in AMI projects worldwide – recurrent DSOs' needs that drives consultancy Support.

DSO Needs Interoperability and Interchangeability

- Foster competition among different suppliers for new tenders
- Extend AMI network due to vendor-lock
- Enhance meter capability / features due to poor initial design or limitations
- Achieve AMI integration with other systems

01 The companions currently available on the market guarantee the interchangeability of devices from different vendors requiring additional documentation or integration testing by the DSO.

02 Certification-level interoperability does not equal plug-and-play interchangeability in live multi-vendor deployments — there is a gap between two devices being able to talk and one vendor's device being replaceable by another's.

03 Closing this gap requires the DSO to define **a supplementary technical layer on top of market standards.**

Structured assessment of standardization level

Identify and address gaps by functional category

Identify Supplementary documents DSO Profile

Deliver Vendor-neutral specs

Utilities take benefit of synergies with KEMA for laboratory functional testing and simulated field environment

Resilience assessment framework

Utilities lack a unified resilience assessment model

Risk Assessment

Identify and rank hazards

- HILP events that are likely to impact the network
- Risk areas associated to HILP

Resilience Evaluation Index (REI)

Quantify Resilience

Metric	Excellent (10)	Good (8-9)	Fair (5-6-7)	Poor (4)
System Availability - SA	≥ 99.95%	99.9% – 99.94%	99% – 99.89%	< 99%
Disaster Recovery Time - DRT	< 1 hour	1 – 3 hours	3 – 6 hours	> 6 hours
System Redundancy Level - SRL	Full	Majority	Partial	Minimal

SA - in percentage, the uptime of the system against total operational time.
DRT - time required to restore normal operations after a disruptive event
SRL - based on the number and quality of redundant components and systems

Identification of technical solutions

Evaluated via Cost Benefit Analysis

Development of mitigation strategies for the exposed network area

- Dedicated processes / procedures / reporting for HILP events
- Network reinforcements **simulation** & CBA
- Evaluate and prioritize investment **based on REI improvement**

Scalable Reliability Optimization for Distribution Networks

How to evaluate investments in network optimization with focus on performance?

THE CHALLENGE

- Networks serving millions of customers — too large for feeder-by-feeder detail
- Heterogeneous asset data across departments with varying quality and completeness
- Existing tools trade accuracy for scalability — or scalability for accuracy
- No systematic way to evaluate thousands of intervention scenarios system-wide
- Investment plans lack quantified reliability impact at the portfolio level

CESI SOLUTION

A scalable, data-driven methodology that combines probabilistic simulation and multi-year investment optimization — designed for real-world large network conditions.

1	Data model construction (assets, outages, failure rates)	2	Representative feeder identification & network simplification
3	Monte Carlo baseline reliability assessment	4	Technical intervention simulation & cost modelling
5	Scaling results to entire network	6	Multi-year investment optimization

SCALABLE

Handles complex networks with millions of customers and heterogeneous multi-department data — without sacrificing computational feasibility

FLEXIBLE

Adapts to different data availability levels across departments and asset types, from detailed feeder records to aggregate historical outage data

ACTIONABLE

Delivers a prioritised, multi-year investment plan with quantified SAIDI/SAIFI impact per intervention — ready for regulatory and board approval

Methodology & Proven Results

6-STEP METHODOLOGY

1 — Data Model Construction
Asset inventory, outage history and feeder characteristics → failure rates λ and repair times MTTR per department and asset class

2 — Network Representation
Identification of representative feeders per department to reduce computational complexity while preserving network diversity

3 — Baseline Reliability Assessment
Monte Carlo simulation on representative feeders to establish current SAIDI/SAIFI performance benchmarks

4 — Intervention Simulation
Modelling of technical interventions (replacement, renovation, maintenance) in terms of cost and reliability impact per feeder type

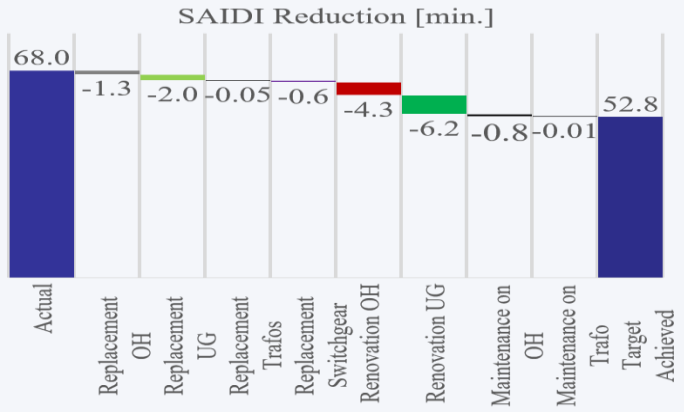
5 — Network-Wide Scaling
Extension of simulation results to all real feeders, generating a comprehensive database of possible investment actions and their expected impact

6 — Multi-Year Optimization
Identification of the most cost-effective investment strategy over a planning horizon — producing an annual budget allocation by intervention type

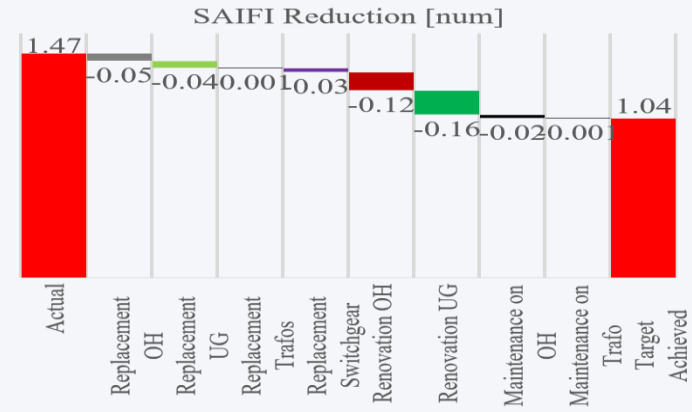
PROVEN RESULTS — Applied to Real Large-Scale Network

−22%	−29%	6	5yr
SAIDI reduction 68.0 → 52.8 min/yr	SAIFI reduction 1.47 → 1.04 evt/yr	Intervention types evaluated simultaneously	Multi-year investment plan produced

SAIDI Contribution by Intervention Type



SAIFI Contribution by Intervention Type



DELIVERABLE

A prioritised, department-level annual investment plan covering replacement, renovation and maintenance across all asset classes — with quantified SAIDI/SAIFI impact, cost per action, and regulatory-ready documentation.

Why Data Fails to Become Operational Value

"A utility can deploy 10 million smart meters and still fail to reduce losses by a single percentage point — because data without architecture, network model, and governance is expensive noise, not intelligence."

THE 5 STRUCTURAL FAILURE MODES - Each independently blocks data from reaching operational decisions

Integration Gap	Temporal Blindness	Missing Physical Layer	Analytical Gap	Governance Failure
Siloed systems (AMI, SCADA, GIS, Billing) with no common IEC CIM data model. **Data cannot be joined cross-system for coherent analysis.**	15-min AMI sampling misses sub-minute fault and PQ events. **Resolution must match the dynamics you are trying to observe.**	No calibrated, phased network model (Digital Twin). **Without it, a meter reading is operationally meaningless in isolation.**	Power engineers lack ML skills. Data scientists lack grid physics. **Advanced platforms become glorified dashboards.**	No closed decision loop: data -> insight -> field action -> measured outcome -> model feedback. **Open loops produce reports, not results.**

Most utilities suffer from at least 3 of these failure modes simultaneously. Addressing all 5 requires a structured program — not a technology purchase.

The Operational Value Stack & Key Messages

5-Layer Operational Value Stack

Each layer must be sufficiently mature before the next can deliver its potential

5	**Governance & Decision Loop** CoE . KPIs . Feedback cycles	*Without: Reports, not outcomes*
4	**Analytics & Decision Support** State estimation . ML . DMS algorithms	*Without: Dashboards, not decisions*
3	**Network Model (Digital Twin)** Calibrated . Phased . GIS-integrated	*Without: Uncontextualized readings*
2	**Communications & Integration** IEC CIM . Unified data bus	*Without: Data silos*
1	**Sensor & Metering Infrastructure** AMI . SCADA . IoT sensors	*Without: Raw data only*

^ OPERATIONAL VALUE ^

KEY MESSAGES

What to take back to your organisation

01	Measure success by operational decisions enabled per month — not data volume collected.
02	Invest in your network model (Digital Twin) before more sensors. It is the physics layer all analytics depend on.
03	NTL detection and FLISR deliver measurable ROI within one investment cycle at early digital maturity.
04	Technology failure causes <20% of programme failures. Organizational failure causes >60%.
05	Digitalization does not need a decade to deliver value. Use-case discipline and sequencing change the timeline.

Testing and certification aspects for communication protocols and cyber security

Giampiero Montagna

Head of Digital Innovation

KEMA Labs

1 **Why IED testing creates value**

2 IEC 61850 for reliable digital substation performance

3 IEC 62351 for stronger cybersecurity assurance

4 KEMA Labs services for confident project execution

KEMA LABs Trusted Testing for Secure Digitalization

As digital substations increase in complexity, stakeholders need IEDs that consistently deliver **functional performance**, **real time communication**, **reliable data** and **data (cyber) security** — helping reduce operational risk and making comprehensive testing essential for resilient digitalization.

Confidence across the full IED lifecycle

KEMA Labs helps customers validate and de-risk their Intelligent Electronic Devices through complete testing, covering functional performance, IEC 61850 communication, data integrity, cybersecurity, electromagnetic compatibility, product safety and environmental influences.

IEC 61850 validation for reliable and interoperable digital substations

- IEC 61850 is the core standard for this digital migration
- As digitalization accelerates, consistent IEC 61850 validation helps utilities and manufacturers reduce risk and deploy with confidence.
- Interoperability testing is essential to prove reliable multi-vendor IED communication and support smoother project execution.

ADOPTION OF ED. 2.1

- Driven by evolving standards and UCAIUG's testing policy.
- Mandatory certification starting January 2024.
- Optional Ed. 2.0 certification for backward compatibility.

BENEFITS OF ED. 2.1

- **Expanded scope:** covers new applications, enabling wider power system use.
- **Improved interoperability**.
- **Enhanced system engineering**: improved data modeling, robust engineering workflows.

IEC 61850 Ed2.1 Certification Features

New Testing Procedures

- Enhanced Compliance: Ensures products fully comply with the latest standard versions.
- Adaptability to Future Standards: Supports ongoing evolution of the standard with new features and technologies.
- Improved Product Quality: Rigorous testing leads to higher product reliability and performance.

Process Bus Measurements

- SV based on IEC 61869-9: Utilizes the latest standard for the digital interface of Instrument Transformers.
- Enhanced Communication: Offers greater flexibility in communication and configuration options.
- Improved Synchronization: Enables precise time synchronization across the system.

GOOSE Message Communication

- Supports Complex Distributed Automation: Facilitates communication between IEDs across wide geographical areas.
- Enhanced Cybersecurity: Introduces alternative, rotatable protocol stacks with built-in security features
- Application-Specific Enhancements: Tailored for the demands of the evolving "environment" application.

Turning communication complexity into trusted cybersecurity

Digital Substations help utilities and operators increase reliability, flexibility, and efficiency, while stronger cybersecurity protects the additional connectivity these environments require.

As communication requirements become more advanced, cybersecurity must be engineered with the same rigor to ensure resilient operations, trusted data, and long-term asset performance.

- Network security
- Device security
- Data integrity
- Physical security
- Training and awareness
- Regulatory compliance

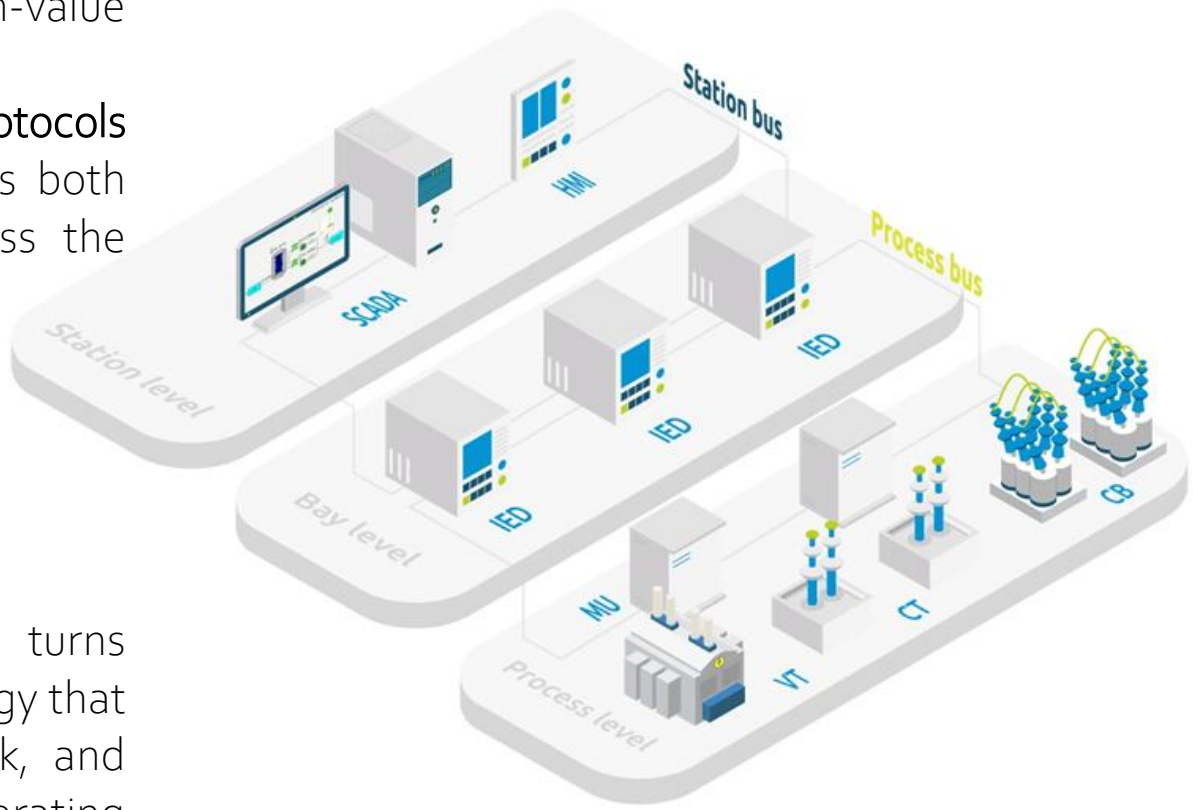
IEC 62351 helps turn cybersecurity requirements into trusted testing outcomes

The **IEC 62351** series provides the information security framework that helps power system stakeholders protect control operations and convert regulatory expectations into practical, high-value testing for digital substations and IEDs.

Its primary objective is to secure the **communication protocols** defined by **IEC TC 57**, enabling test programs to address both protocol performance and cybersecurity resilience across the standards that matter most, including:

- the **IEC 61850** series
- the **IEC 60870-5** series
- the **IEC 60870-6** series,
- the IEC 61970 series,
- and the **IEC 61968** series.

For manufacturers, utilities, and integrators, this turns cybersecurity compliance into a structured validation strategy that supports secure communication, reduces operational risk, and strengthens confidence in IED performance in real operating environments.



KEMA Labs response to IEC 62351 testing needs

Testing Focus

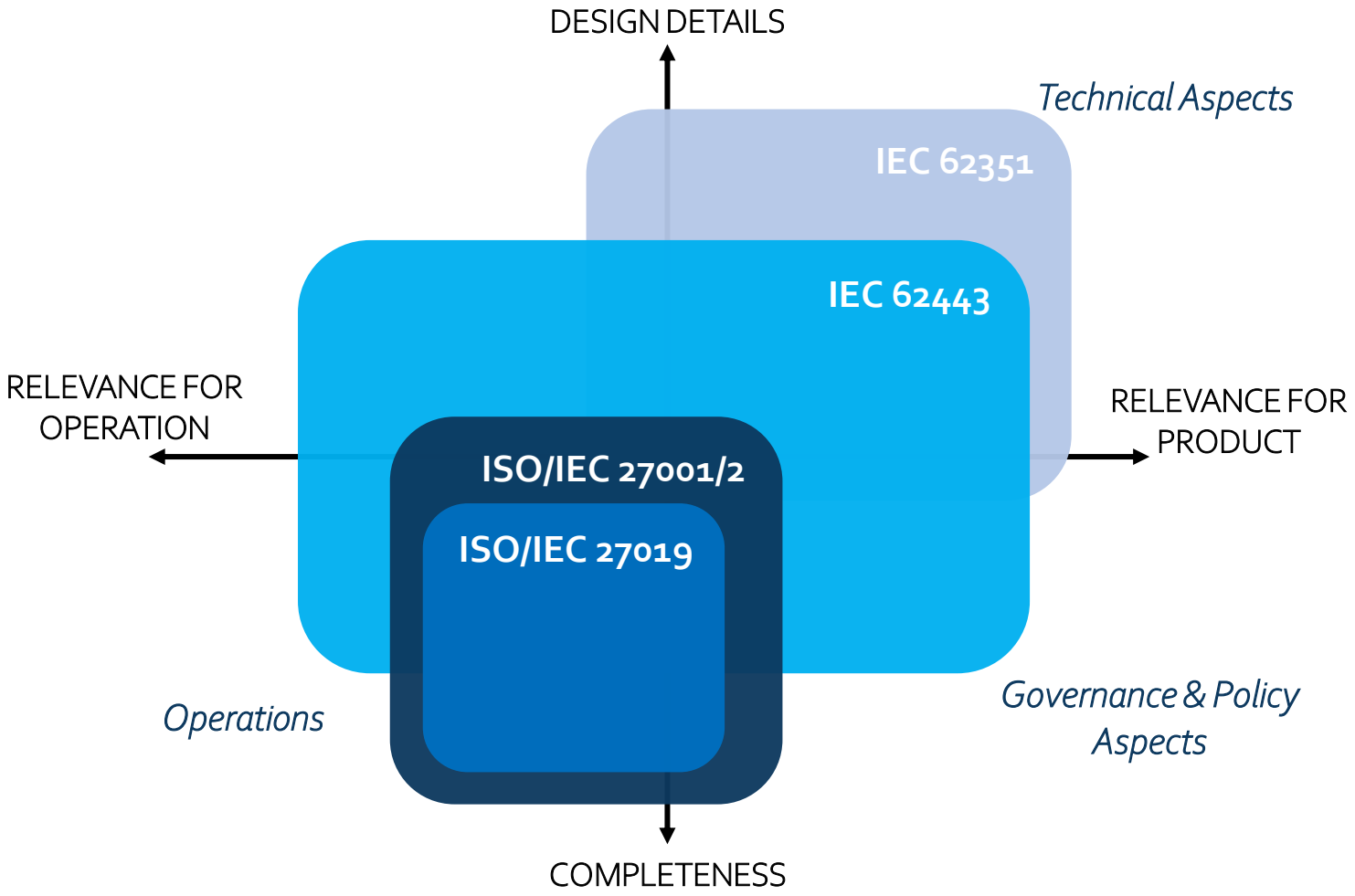
KEMA Labs translates IEC 62351 requirements into practical test programs for IEDs, communication interfaces and secure system integration.

Service Framework

Our offer combines test design, execution and reporting to address secure data exchange, interoperability and implementation compliance in digital substations.

Key Outcomes

Clear evidence of confidentiality, integrity, availability and non-repudiation for IED solutions under realistic operating conditions.



IED Service Pillars
Addressing testing and OT cybersecurity challenges

TESTING & CERTIFICATION

- Hardware / environmental type tests
- Functional Testing
- Communication Protocol Testing (including IEC 61850 Ed 2.1)
- OT Cybersecurity testing (IEC 62351 series)

EXPERT ADVISORY

- Preparation / review of test plans and/or test specifications
- Development of IEDs interoperability profiles
- Review of Conformance Statement documents
- Dedicated Test Tools for IEC 61850
- Trainings on new (inter)national standards and other specific topics

PRODUCT EXPERTISE

Protection relays

Ethernet Switches/Routers (19" rack mounting)

Ethernet Switches/Routers (DIN-rail mounting)

Bay controllers

Power-line carrier terminals

Remote Terminal Units / Gateways

Digital event & fault recorders

Stand-alone merging units

MPLS-TP multiplexers / telecommunication platforms

Teleprotection systems

Industrial computers

IEDs – Testing services offered by KEMA Labs

Hardware / environmental type tests

- Type testing according to IEC 60255-1, IEC 60255-26, IEC 60255-27, IEC 61850-3, IEEE 1613 series, IEC 61869-13, IEC 60834-1, etc.
- Electromagnetic compatibility (EMC) tests, Product safety tests, Climatic tests, Mechanical tests, others (contact performance, burden, dimensions, markings, etc.)

Functional Testing

- Functional testing of protection relays (IEC 60255-100 series)
- Accuracy testing of merging units (IEC 61869-13)
- Functional performance testing of Ethernet Switches/Routers (IEC 61850-90-4)

Communication Protocol Testing

- IEC 61850 Protocol Conformance / Certification (Ed 2.1 and Ed 2.0)
- IEC 60870 Protocol Conformance / Certification (-101, -103 and -104)
- DNP3 Protocol Conformance / Certification

OT Cybersecurity testing

- Verification / Conformance Testing (IEC 62351-3 and others): ensuring your devices to comply with industry standard protection according to IEC 62351
- IEC 62351 testing and certification services for energy management products and systems supporting IEC 60870 and/or IEC 61850 communication protocols

Communication protocols services offered by KEMA Labs

- **IEC 61850 testing and certification services**

IEC 61850 – key standard for next-generation substation automation

- **IEC 60870-5 testing and certification services**

IEC 60870–5 focuses on the communication protocols for remote control of substations and power system equipment.

including IEC 60870-5-101, IEC 60870-5-103, and IEC 60870-5-104 protocols

- **DNP3 testing and certification**

DNP3 (Distributed Network Protocol version 3) wide adopted in North America in the electric power and utility sectors in real-time data exchange and control between SCADA master stations and remote terminal units (RTUs)

Smart metering Communication protocols services

• Meters and More compliance testing for Smart meters

- KEMA Labs 's Meters and More Compliance Testing laboratory is currently the only Laboratory appointed by the Association
- Testing results are submitted to Association, which will issue the Meters and More compliance certificate

• G3 DLMS-COSEM Interchangeability tests

- Support to Client for definition of Testing procedures and tools, based on Client's Companion Standard
- Testing of companion standard of G3 meters as independent Laboratory for Distribution company, in collaboration with Meters Manufacturers:
    - Compliance of Data Model
    - Compliance of Use Cases
- Reference standards: ITU-T G.9903, IEC 62056 series, DLMS UA Coloured Books
- Kema labs is a Member of DLMS UA (DLMS User Association)

IEDs – IEC 61850 services offered by KEMA Labs

IEC 61850 Ed 2.1 Certification

IEC 61850 Ed 2.1 Server Conformance

- MMS communication
- GOOSE publish & subscribe
- IEC 61869-9 Sampled Values Subscribe & Publish

IEC 61850 Ed 2.1 Server GOOSE Performance

IEC 61850 Ed 2.0 Certification

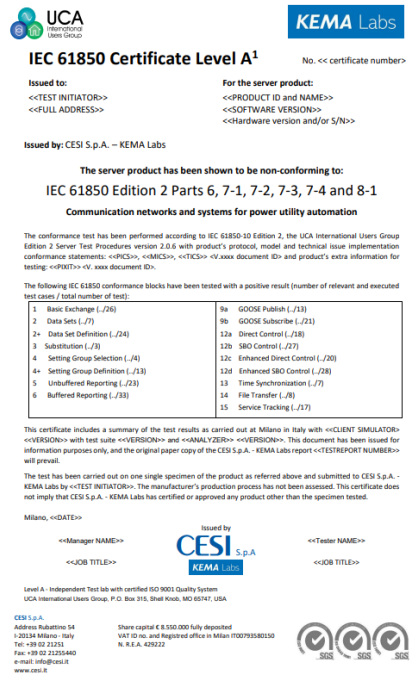
IEC 61850 Ed 2.0 Server Conformance

- MMS communication
- GOOSE publish & subscribe
- IEC 61850-9-2LE Sampled Values Publish

IEC 61850 Ed 2.0 Server GOOSE Performance

IEC 61850 Related Services

- Development of IEDs interoperability profile according to IEC 61850
- Review of Conformance Statement document and SCL files
- Testing and certification
- Pre-tests or pre-compliance tests
- Conformance tests or official certification tests
- IEC 61850 Test Tools - Gridclone's "IEC 61850 Test Tool"



UCA International Users Group

KEMA Labs

IEC 61850 Certificate Level A[1]

No. << certificate number>

Issued to:
<<TEST INITIATOR>>
<<FULL ADDRESS>>

For the server product:
<<PRODUCT ID and NAME>>
<<SOFTWARE VERSION>>
<<Hardware version and/or S/N>>

Issued by: CESI S.p.A. – KEMA Labs

The server product has been shown to be non-conforming to:

IEC 61850 Edition 2 Parts 6, 7-1, 7-2, 7-3, 7-4 and 8-1

Communication networks and systems for power utility automation

The conformance test has been performed according to IEC 61850-10 Edition 2, the UCA International Users Group Edition 2 Server Test Procedures version 2.0.6 with product's protocol, model and technical issue implementation conformance statements: <<PICS>>, <<MICS>>, <<TICS>> <V.xxx document ID> and product's extra information for testing: <<PIXIT>> <V. xxx document ID>.

The following IEC 61850 conformance blocks have been tested with a positive result (number of relevant and executed test cases / total number of test):

1	Basic Exchange (../26)	9a	GOOSE Publish (../13)
2	Data Sets (../7)	9b	GOOSE Subscribe (../21)
2+	Data Set Definition (../24)	12a	Direct Control (../18)
3	Substitution (../3)	12b	SBO Control (../27)
4	Setting Group Selection (../4)	12c	Enhanced Direct Control (../20)
4+	Setting Group Definition (../13)	12d	Enhanced SBO Control (../28)
5	Unbuffered Reporting (../23)	13	Time Synchronization (../7)
6	Buffered Reporting (../33)	14	File Transfer (../8)
		15	Service Tracking (../17)

This certificate includes a summary of the test results as carried out at Milano in Italy with <<CLIENT SIMULATOR> <<VERSION>> with test suite <<VERSION>> and <<ANALYZER> <<VERSION>>. This document has been issued for information purposes only, and the original paper copy of the CESI S.p.A. - KEMA Labs report <<TESTREPORT NUMBER>> will prevail.

The test has been carried out on one single specimen of the product as referred above and submitted to CESI S.p.A. - KEMA Labs by <<TEST INITIATOR>>. The manufacturer's production process has not been assessed. This certificate does not imply that CESI S.p.A. - KEMA Labs has certified or approved any product other than the specimen tested.

Milano, <<DATE>>

Issued by

<<Manager NAME>>
<<JOB TITLE>>

CESI S.p.A
KEMA Labs

<<Tester NAME>>
<<JOB TITLE>>

Level A - Independent Test lab with certified ISO 9001 Quality System
UCA International Users Group, P.O. Box 315, Shell Knob, MO 65747, USA

CESI S.p.A.
Address Rubattino 54
I-20134 Milano - Italy
Tel: +39 02 21251
Fax: +39 02 21255440
e-mail: info@cesi.it
www.cesi.it

Share capital € 8.550.000 fully deposited
VAT ID no. and Registred office in Milan IT00793580150
N. R.E.A. 429222

SGS SGS SGS

IEC 62351 services to accelerate secure IED validation by KEMA Labs

Our service package helps de-risk and streamline the full IED validation journey:

- Verification / Conformance Testing (IEC 62351-3 and others): structured testing to demonstrate compliance with key IEC 62351 cybersecurity requirements while helping teams identify issues early, reduce rework and build confidence before deployment.

- Advisory on IEC 62351 implementation, helping customers apply cybersecurity requirements across development, integration and validation with a practical, reliable approach that supports faster decisions and stronger project outcomes.

Key Benefits for manufactures and utilities

- **Manufactures** prove the security and interoperability of their substation automation products including SCADA systems and components such as RTUs and IEDs, strengthening market access
- **Network operators** can rely on a compliant device that could operate in their network and in particular lab allow de-risks adoption and enables stable long-term operation of utility networks.
- **System integrators** achieve end-to-end interoperability and security from substation automation up to SCADA system

Kema Labs – Customer Mapping for IED Testing

- **OEMs & IED Manufacturers** – ABB, Hitachi Energy, Siemens, Schneider Electric
- **Utilities & Grid Operators** – TSOs, DSOs, and private network operators
- **System Integrators & EPCs** – Grid automation and substation projects
- **Certification & Compliance Stakeholders** – Type testing, interoperability, cybersecurity, and grid code validation

Why customers choose KEMA Labs to simplify the digital validation journey

- **Faster time to market** through a smoother validation process
- **Lower project risk** with dependable guidance at every step
- **A trusted partner** that strengthens confidence with customers and stakeholders
- **Easier access** to **global markets** with broader recognition
- Greater confidence that your products **meet compliance expectations**