



WHITE PAPER · SEPTEMBER 2026

Smart grid

Reliable and secure communications for the energy-transition
power grid

Summary

- Renewables, storage and EV charging require the distribution grid to be observed and controlled in near real time.
- Communications must deliver different latency, synchronisation and availability for protection, automation and metering. Fibre and 5G with slicing cover most needs.
- Security is governed by NIS2 for the energy sector and by the EU network code on cybersecurity (Delegated Regulation (EU) 2024/1366), in force since 13 June 2024 for high-impact entities.
- Meters, inverters and gateways with radio fall under the RED with EN 18031; all products with digital elements under the Cyber Resilience Act.

01

Context

The grid is moving from a few large plants to millions of points that produce and consume. Managing it needs frequent data from secondary substations, fast commands and coordinated protection: communication becomes part of the power system.

Each service class has different requirements. Protection needs tight latency and synchronisation, medium-voltage automation needs high availability, metering needs wide coverage and low power. Designing a single network without distinguishing these classes leads to high costs or poor performance.

02

Regulatory framework

Regulation or standard	What it requires	Dates
Network Code on Cybersecurity (NCCS) – Delegated Regulation (EU) 2024/1366	Risk management, minimum and advanced controls for high- and critical-impact entities	In force from 13/6/2024, phased implementation
NIS2 – Italian Legislative Decree 138/2024	Energy as a highly critical sector: security measures and incident reporting	Baseline measures by October 2026 (entities notified in 2025)
Cyber Resilience Act – Regulation (EU) 2024/2847	Reporting of exploited vulnerabilities to ENISA; product security requirements	Reporting from 11/9/2026; full application from 11/12/2027
RED – Delegated Regulation (EU) 2022/30, EN 18031	Cybersecurity of connected radio equipment	From 1/8/2025
IEC 61850, IEC 62351, IEC 62443	Substation automation, protocol security, industrial security	Technical references

This document is for information only and is not legal advice. Regulatory dates and obligations must be checked against official texts at the time of application.

03

Reference architecture

Grid applications	L5
automation · protection · flexibility · metering	
Platforms	L4
SCADA and ADMS · data and AI forecasting	
Cloud and edge	L3
processing in primary substations	
Communications	L2
fibre · 5G with slices · time synchronisation	
Field	L1
substations · secondary substations · inverters · storage · meters	

Each layer has its own performance, security and management requirements: acceptance testing is done layer by layer and end to end.

04

Use cases

Use case	Technology	KPIs to measure
Medium-voltage automation	5G slice or fibre	Latency, availability
Differential protection	Fibre or low-latency 5G with synchronisation	Latency, jitter
PV and storage integration	5G, NB-IoT	Command time
EV charging	4G/5G	Availability, security
Meters and sensors	NB-IoT, LTE-M	Coverage, power consumption

05

Getting started in 90 days

- 1 Inventory existing communications and weak points.
- 2 Classify services by latency, synchronisation and availability requirements.
- 3 Measure coverage and latency on a sample of substations.
- 4 Align the security plan with NCCS and NIS2, suppliers included.
- 5 Run a 5G pilot on one feeder, with acceptance testing and comparison against fibre.

06

How Conection works

Conexion supports public bodies and companies as independent engineers: we write measurable requirements and specifications, check suppliers' designs, run field acceptance tests and train staff. We do not sell equipment, so we can stay on the side of the people who use the network.

07

Sources

ACER – Network code on cybersecurity for electricity — <https://www.acer.europa.eu/electricity/cybersecurity>

ICT Security Magazine – NIS2, adempimenti fino a ottobre 2026 —

<https://www.ictsecuritymagazine.com/notizie/nis2-adempimenti/>

Commissione europea – CRA reporting obligations — <https://digital-strategy.ec.europa.eu/en/policies/cra-reporting>

CEN-CENELEC – Cybersecurity standards for the RED —

<https://www.cencenelec.eu/news-events/news/2025/newsletter/ots-59-cybersecurity-standards/>