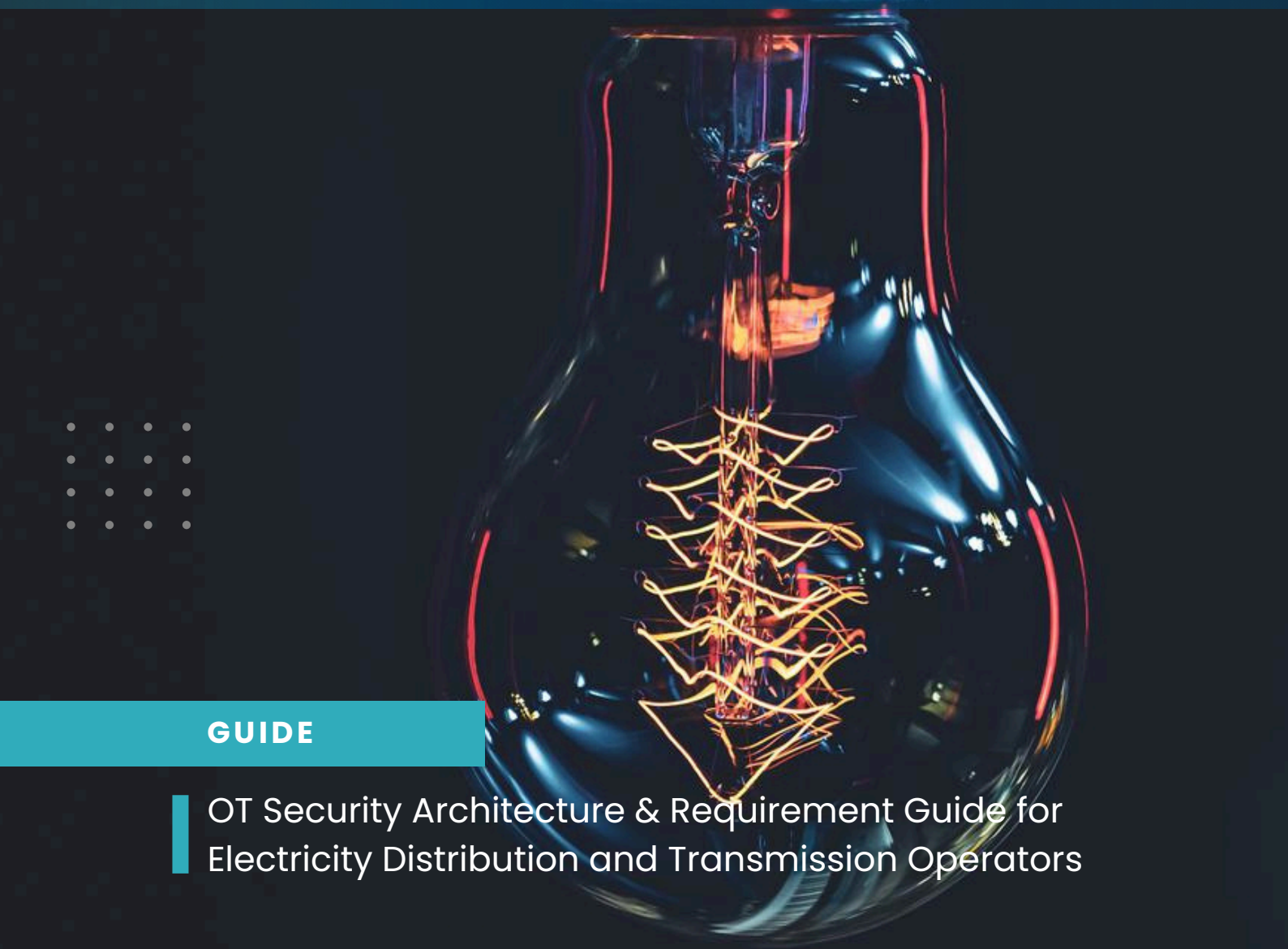
Druid

IEC 62443 Compliance

The Global OT Cybersecurity Standard You Cannot Ignore



GUIDE

OT Security Architecture & Requirement Guide for Electricity Distribution and Transmission Operators

Table of Contents

What is IEC 62443 and why does it matter?	03
Utility 5G Use Cases & Grid OT Classification	06
Utility OT Landscape & IEC 62443 Zone Model	10
References	14
About Druid Software	15

Section 1

What is IEC 62443 and why does it matter?

IEC 62443 is the globally recognized blueprint designed specifically for Operational Technology (OT). It is the only standard that treats cybersecurity as a physical safety issue. The benefits of IEC 62443 compliance for utility companies globally are extensive. Enhanced risk management, stronger operational resilience and bridging the IT/OT gap are just some of the high-level advantages of following these standards.

The electricity grid is the most consequential OT environment on earth. A successful cyberattack on grid infrastructure can cause cascading failures, blackouts affecting millions, and irreversible damage to high-voltage equipment that takes months to replace. At the same time, the grid is undergoing the most significant transformation since electrification: distributed energy resources (DERs) are proliferating at every voltage level, transmission and distribution systems are being automated to handle bidirectional power flows and utilities face mounting pressure to expand capacity while reducing operational costs.

To bridge the gap between legacy limitations and modern operational requirements while adhering to IEC 62443, Utility and Energy companies should consider Private 5G. Accordingly, this document outlines:

- the case for Private 5G in utilities
- specific grid use cases and establishment of an OT classification system
- a network slicing strategy mapped directly to distinct operational tiers and security zones
- the IEC 62443 Zone Model for Utility 5G
- mapping of how Private 5G architecture satisfies NERC CIP standards

Private 5G is already deployed at scale in utility operations

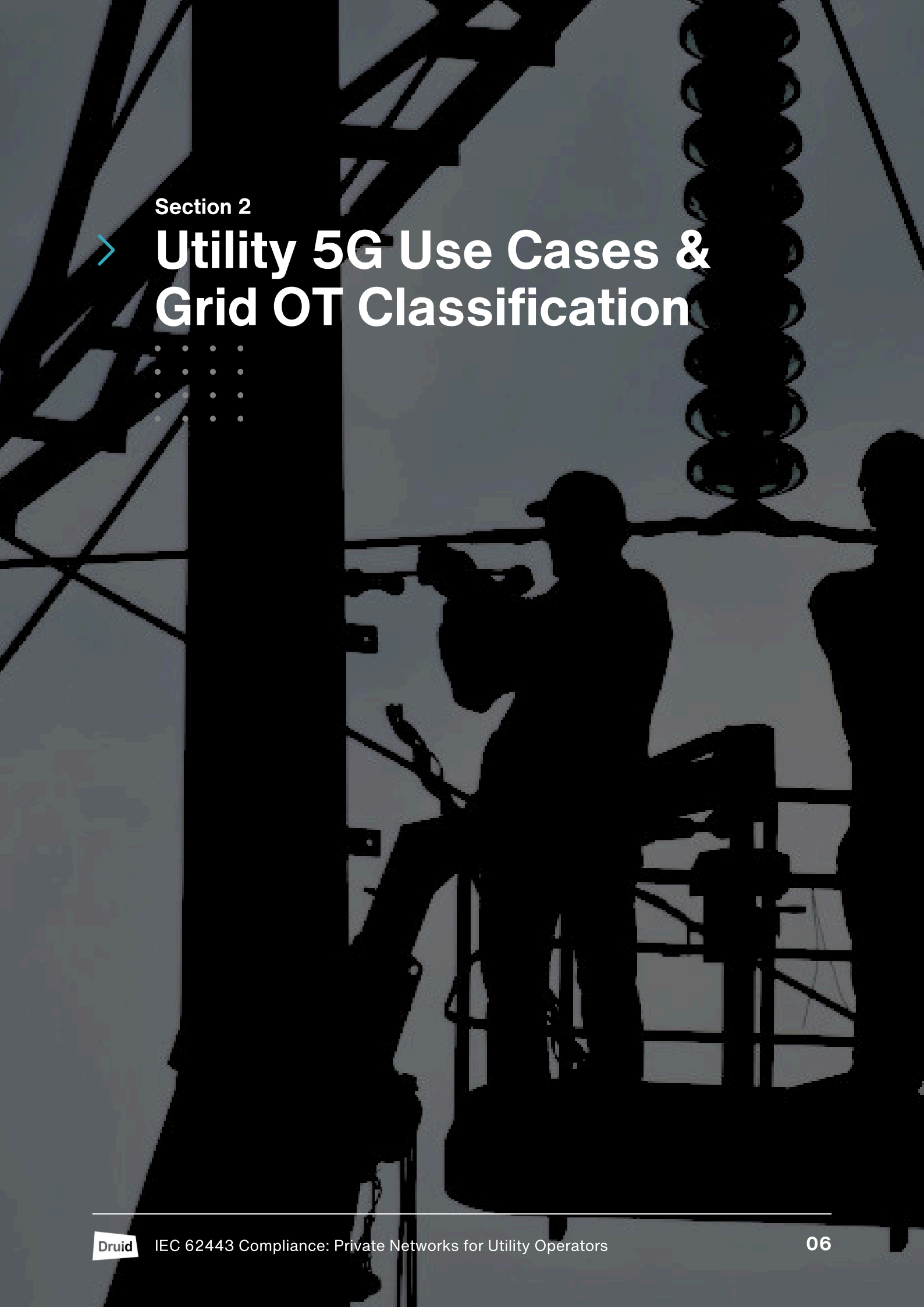
Private 5G is already deployed at scale in utility operations globally, supporting grid modernization and automation. The technology has moved from proof-of-concept to operational deployment.

1.1 Why Private 5G Outperforms Legacy Grid Communication Technologies

Dimension	Legacy SCADA Radio	Leased Line / PLC	Public LTE	Private 5G
Latency for protection	200–500ms — too slow for distance and differential protection requiring <100ms	Low latency when available but geographically limited	50–100ms typical — insufficient for time-critical protection	URLLC: <10ms achievable — sufficient for teleprotection, differential protection, and GOOSE over 5G (3GPP TS 33.501 R-GOOSE framework)
Connection density	Low — point-to-point or small broadcast groups	One-to-one — not scalable for AMI or DER telemetry	Limited by shared spectrum congestion at scale	mMTC/RedCap: 1M+ devices/km² — supports full AMI fleet, DER inverter telemetry, and field sensor networks simultaneously
Security architecture	RF security poor; proprietary encryption or none; no device authentication	Physical security of circuits; limited cyber security	Public network — shared exposure; operator has no control over security policy	SIM/5G-AKA per-device authentication; mandatory air interface encryption; network slicing isolation; operator controls full security stack
Spectrum control	Licensed bands but shared with legacy systems; interference common in dense areas	Not radio — physical circuits	Shared public spectrum — operator cannot guarantee QoS for critical OT	Many options for licensed dedicated spectrum are available now; interference managed; guaranteed OT QoS via GBR slices.
OT protocol support	SCADA-specific radio modems; DNP3/Modbus over serial	Native support for legacy OT protocols	Limited OT protocol awareness	5G Ethernet PDU sessions carry IEC 61850 MMS, GOOSE (via R-GOOSE), sampled values, and DNP3 natively; TSN (Time-Sensitive Networking) integration roadmap
Field crew connectivity	Separate radio systems (P25/DMR) for voice	Not applicable	Available but shared with public users; no priority	MCPTT on 5G delivers priority voice and data; field crew AR applications for live-line working; single device for OT telemetry + crew comms
Regulatory security posture	No dedicated cybersecurity framework	Limited — physical security dominant	MVNO arrangements with limited control	NERC CIP alignment achievable via 5G security controls

1.2 How Private 5G Addresses Grid and OT Requirements

Grid / OT Requirement	How Private 5G Addresses It
IEC 62443-3-3 FR1 — Device authentication	SIM/eSIM provides per-device cryptographic identity for every IED, RTU, smart meter, and field device. Hardware-rooted identity cannot be spoofed — stronger than MAC-based or preshared key alternatives common in SCADA radio environments.
IEC 62443-3-3 FR5 — Zone isolation (SR 5.1)	Network slicing maps directly to IEC 62443 security zones: substation protection traffic on a dedicated URLLC slice, AMI telemetry on a separate mMTC slice, field crew comms on a third — cryptographic isolation enforced at the 5GC level, not just at the firewall.
IEC 61850 — Substation communication	3GPP has defined R-GOOSE (Routable GOOSE) and R-SV (Routable Sampled Values) allowing IEC 61850 protection messages to traverse 5G networks with appropriate latency and integrity controls. 5G is the first wireless technology for which a standards path to IEC 61850 support exists.
IEC 62351 — Grid cybersecurity	IEC 62351 (cybersecurity for power systems communication) and 3GPP TS 33.501 are complementary frameworks. 5G air interface security (encryption, integrity) satisfies IEC 62351 Part 8 transport-layer security requirements for grid communication.
NERC CIP — Electronic Security Perimeter	5G's network slicing and zone architecture, with an on-premise UPF, creates a definable Electronic Security Perimeter (ESP) for CIP-005 compliance. The 5G management plane provides auditable access control logs required for CIP-007 system security management.
NIS2 Art. 21 (EU Directive) — Risk management (energy sector)	5G's mandatory security controls — mutual authentication, encrypted air interface, slice isolation — reduce the residual OT risk that NIS2 demands management. Fewer compensating controls are needed for wireless grid communication than with legacy radio or public LTE.



Section 2

Utility 5G Use Cases & Grid OT Classification

2.1 Grid Use Case Inventory

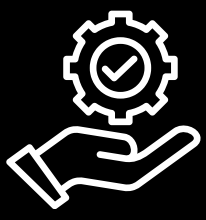
Use Case	5G Service	Latency	IEC 62443 Zone	Why Private 5G Is the Right Choice
Substation automation (IEC 61850)	URLLC (5QI 82/84	<10ms	Zone 1/2	5G carries IED-to-IED communication, GOOSE (R-GOOSE), and MMS between primary and backup substations. Enables process bus extension over 5G — connecting merging units and protection IEDs across buildings without additional fibre
Teleprotection / line differential	URLLC (5QI 84)	<10ms end-to-end	Zone 1	Line differential protection requires symmetric latency <10ms between line ends. 5G URLLC with precise timing (IEEE 1588 / PTP over 5G) is the first wireless technology capable of meeting this requirement without dedicated fibre
Wide-Area Monitoring System (WAMS / PMU)	URLLC (5QI 82)	<20ms	Zone 2	Phasor Measurement Unit telemetry requires precise time-stamped, high-rate (30–120 samples/sec) data delivery across the transmission network. 5G provides timing accuracy and bandwidth for multi-PMU WAMS without leased line cost.
Distribution automation (FLIR / FLISR)	URLLC (5QI 82)	<50ms	Zone 1/2	Fault Location, Isolation, and Service Restoration requires near-real-time communication with remote reclosers, sectionalising switches, and capacitor banks. 5G URLLC enables automated feeder reconfiguration that reduces SAIDI and SAIFI.
DERMS — DER telemetry and dispatch	mMTC / URLLC	<200ms	Zone 2	Tens of thousands of rooftop solar inverters, battery storage systems, and EV chargers reporting to DERMS. 5G mMTC provides the connection density; URLLC delivers dispatch commands to DERs for demand response and grid balancing.
Advanced Metering Infrastructure (AMI 2.0)	mMTC / RedCap	<1s	Zone 2/3	Next-generation smart meters reporting every 5 minutes for time-of-use tariffs, outage detection, and power quality monitoring. 5G RedCap provides cellulargrade security and connection density for AMI without proprietary RF mesh networks.

Use Case	5G Service	Latency	IEC 62443 Zone	Why Private 5G Is the Right Choice
Field crew mobility and dispatch	eMBB + MCPTT	<200ms	Zone 3/4	Technicians performing switching operations access live single-line diagrams, switching schedules, and SCADA state on 5G-connected tablets. MCPTT integrates with the P25 emergency communication platform though standardized interworking gateways.
Overhead line monitoring (sensors, drones)	eMBB / mMTC	<1s	Zone 2/3	Conductor temperature sensors, sag monitors, vibration sensors, and drone-based line inspection video. 5G provides the backhaul for line-mounted IoT without point-to-point radio repeaters.
Power plant / generation monitoring	URLLC / eMBB	<100ms	Zone 2	Gas turbine, hydro, and wind plant telemetry, auxiliary systems monitoring, and DCS interface. 5G extends the plant OT network to remote assets without dedicated fibre backhaul.
Electric vehicle (EV) grid integration	mMTC / URLLC	<500ms	Zone 2/3	Smart charging command and control (OCPP 2.0.1, ISO 15118) for grid-responsive EV charging. 5G provides the communication layer for V2G (vehicle-togrid) applications and demand response dispatch to EV charging infrastructure.
Emergency / mutual aid comms	MCPTT (5QI 65)	<300ms priority	Zone 3	Priority-preempted voice for grid restoration crews during major incidents. 5G MCPTT replaces P25 with a standards-based, data-integrated emergency communication platform that remains operational during major grid events.

2.2 Network Slicing Strategy for Utility Operations

Utility 5G network slicing must reflect both the IEC 62443 zone model and the grid's operational service tiers — from time-critical protection communications to bulk IoT metering. Each slice carries distinct security, QoS, and data sovereignty requirements.

Slice ID	Slice Name	5G Service	IEC 62443 Zone	Replaces / Consolidates
Slice-G1	Grid Protection	URLLC (5QI 84/82)	Zone 1	Teleprotection pilot channels (leased line); IEC 61850 R-GOOSE; line differential protection
Slice-G2	SCADA / Distribution Automation	URLLC (5QI 82)	Zone 1/2	SCADA radio; DNP3 modem links; FLIR/FLISR automation; substation RTU comms
Slice-G3	DERMS / DER Telemetry	URLLC / mMTC	Zone 2	DER inverter monitoring; DERMS dispatch; V2G communication; demand response signallin
Slice-G4	AMI / Smart Metering	mMTC / RedCap	Zone 2/3	Proprietary AMI RF mesh (Silver Spring, Itron, Landis+Gyr); meter data collectors
Slice-G5	Field Crew / Workforce	eMBB + MCPTT	Zone 3/4	P25/DMR field radios; separate crew data tablets; switching schedule PDFs
Slice-G6	Substation Security / OHL Monitoring	eMBB / mMTC	Zone 3	Substation CCTV; access control; overhead line IoT sensors; drone video backhaul
Slice-G7	Corporate / MVNO Fallback	eMBB (5QI 9)	Zone 4/5	Office Wi-Fi; public LTE fallback for remote areas outside private 5G coverage



A single private 5G network with dedicated slices for grid protection, SCADA, AMI, field crew and emergency communications consolidates the utility's legacy technology stack: SCADA radio, protection pilot channel leased lines, P25/DMR, proprietary AMI RF mesh, and point-to-point modem links — all with a single compliance framework and a single supply chain to manage.

Section 3

Utility OT Landscape & IEC 62443 Zone Model

3.1 How Private 5G Addresses Grid and OT Requirements

System Category	Examples	5G Connectivity Role
Protection relays and IEDs	ABB REL650, Siemens SIPROTEC 5, GE Multilin, SEL-311C — line distance, differential, and busbar protection	Slice-G1 URLLC. 5G R-GOOSE and R-SV enable protection relay inter-trip and differential protection across geographically separated substations without leased line dependency.
Substation SCADA / RTUs	ABB MicroSCADA Pro, Siemens Spectrum Power, GE ENMAC, OSIsoft PI; RTUs: ABB RTU560, Schneider Quantum	Slice-G2. 5G replaces SCADA radio and modem links for RTU polling and supervisory control. DNP3/IEC 60870-5-104 over 5G with authentication (IEC 62351 Part 5).
Distribution automation devices	Reclosers (S&C, Eaton, Noja Power), LBS (load break switches), capacitor banks, voltage regulators — all with IED or RTU	Slice-G2 URLLC. Real-time command and telemetry for FLISR. 5G provides the <50ms latency required for automated feeder reconfiguration.
Phasor Measurement Units (PMUs)	Schweitzer SEL-421, GE M60, Doble/Lemke MiCOM P746 — GPS-synchronised time-stamped measurements	Slice-G1 URLLC. PMU data requires precise timing and highthroughput delivery. 5G with IEEE 1588/PTP provides timing accuracy; URLLC provides reliable delivery for wide-area monitoring.
DERMS platform and DER devices	AutoGrid, Enbala, GE DERMS, Schneider EcoStruxure DERMS; inverters: SMA, Fronius, Enphase, SolarEdge	Slice-G3. 5G mMTC handles large DER fleet telemetry. URLLC delivers curtailment and dispatch commands to DER devices for grid stability actions. IEEE 2030.5 / IEEE 1547.1 over 5G.
Advanced Metering Infrastructure (AMI)	Itron OpenWay Riva, Landis+Gyr FOCUS, Honeywell (Elster) AMI, Aclara — smart electricity, gas, and water meters	Slice-G4 mMTC/RedCap. 5G provides cellular-grade security for meter data without proprietary RF mesh infrastructure. DLMS/ COSEM protocol over 5G.
Energy Management System (EMS / ADMS)	GE EMS, Siemens ADMS, Oracle Utilities, ABB Network Manager — transmission and distribution control centres	Zone 4. EMS receives aggregated data from 5G-connected substations, DERs, and AMI — with the on-premise UPF ensuring grid OT data stays within the utility's security perimeter.

Field workforce tools	Esri ArcGIS Field Maps, IBM Maximo Mobile, Trimble Unity, ABB Ability Network Manager Mobile — switching, inspection, and maintenance apps	Slice-G5 eMBB + MCPTT. Field technicians access live GIS, single-line diagrams, and SCADA state on 5G-connected rugged tablets.
Overhead line and asset monitoring	Sensors: PLP LINE·IQ, Ampacimon, Lindsey Manufacturing; CCTV: Axis/Bosch for substation; drones: Teledyne /Inspired/ Percepto for line inspection	Slice-G6 eMBB/mMTC. 5G provides backhaul for line-mounted sensors without radio repeaters and drone video uplink for LiDAR survey and vegetation management.

3.2 IEC 62443 Zone Model for Utility 5G

Zone ID	Zone Name	Target SL	Utility Assets + 5G Components
Zone 0	Process / Field Devices	SL 1–2	Protection relay CT/VT inputs, merging units, instrument transformers, distribution sensors, overhead line monitors — 5G RedCap/mMTC UEs
Zone 1	Substation / Device Control	SL 2–3	Protection IEDs, substation RTUs, reclosers, sectionalising switches, capacitor banks, PMUs — 5G URLLC UEs on Slice-G1/ G2
Zone 2	Supervisory / SCADA	SL 2–3	SCADA servers, ADMS/EMS clients at substations, DERMS edge nodes, AMI data concentrators, distribution management workstations
Zone 3	OT Management / Grid DMZ	SL 2–3	5G Core (AMF, SMF, on-premise UPF), OT firewall, NMS/SMO, OT security monitoring, patch management — this zone is the IEC 62443 Electronic Security Perimeter for NERC CIP purposes
Zone 4	Control Centre IT	SL 2	EMS/ADMS control centre servers, SCADA master stations, GIS, historian (OSIsoft PI, AVEVA), utility enterprise IT
Zone 5	External / Internet / MVNO	SL 1	Public 5G fallback for remote areas (MVNO), internet-facing AMI portals, customer portal — isolated from all OT slices by UPF and zone firewall
Zone 6	Remote Access DMZ	SL 3	OEM/vendor remote access (ABB, Siemens, GE, SEL, Itron), 5G management remote access, field tablet VPN termination — all third-party access terminates here before entering Zone 2/3

3.3 NERC CIP Alignment

For utilities operating under NERC CIP (primarily US and Canadian operators, but increasingly referenced internationally), the private 5G architecture provides a natural alignment with key CIP standards

NERC CIP-002

BES Cyber System identification

5G-connected IEDs, RTUs and protection relays meeting the BES Cyber Asset definition shall be registered in the utility's NERC CIP asset register and linked to the 5G subscriber database entry (SIM/IMSI).

NERC CIP-005

Electronic Security Perimeter (ESP)

The on-premise UPF (Zone 3) defines the ESP boundary for 5G-connected OT systems. Inter-zone comms traverse the 5G conduit (Slice-G1/G2) and terminate at the UPF N6 interface within the ESP — satisfying ESP boundary definition requirements.

NERC CIP-006

Physical Security of BES Cyber Systems

gNBs at primary substations within the Physical Security Perimeter (PSP) are in scope. Remote gNBs at distribution substations require physical security measures consistent with CIP-006.

NERC CIP-007

Systems Security Management

5G NMS provides centralised audit logging for all OT slice access events. Ports and services on 5G-connected devices shall be restricted per CIP-007. Patch management (CIP-007 R2) applies to gNB and 5GC software.

NERC CIP-010

Configuration Change Management

5G slice parameter changes, gNB firmware updates, and device on-boarding shall follow the CIP-010 baseline configuration change management process. The NMS provides the audit trail.

NERC CIP-013

Supply Chain Risk Management

5G equipment vendor assessment (NESAS, IEC 62443-4-1) satisfies CIP-013 vendor risk management requirements. The 5G supply chain is assessed using the same SCRM process as protection relay and RTU vendors.

References

Zone ID	Zone Name
IEC 62443-3-3	System security requirements and security levels (IEC, 2013/2024)
IEC 62443-4-1	Product security development lifecycle requirements (IEC, 2018)
IEC 62443-4-2	Technical security requirements for IACS components (IEC, 2019)
IEC 62443-2-4	Security program requirements for IACS service providers (IEC, 2015)
3GPP TS 33.501	Security architecture and procedures for 5G system (Release 15–18)
3GPP TS 23.501	5G system architecture — network slicing, QoS, UPF placement
3GPP TS 22.179	Mission-Critical Push to Talk (MCPTT) — field crew emergency comms
IEC 61850	Communication networks and systems in substations (all parts)
IEC 61850-8-2	Routable GOOSE (R-GOOSE) and Routable Sampled Values (R-SV) over TCP/IP
IEC 62351	Security for power system communication (all parts, esp. Parts 3, 5, 6, 8)
IEEE 1588	IEEE Standard for a Precision Clock Synchronisation Protocol (PTP)
IEEE 2030.5	IEEE Standard for Smart Energy Profile Application Protocol (DER/CSIP)
ENISA 5G Security	Security in 5G Specifications — Controls in 3GPP (ENISA, 2021)
GSMA NESAS	Network Equipment Security Assurance Scheme (GSMA, current edition)
GSMA SGP.02	M2M Embedded SIM Remote Provisioning Architecture (GSMA)
DLMS/COSEM	Device Language Message Specification — IEC 62056 metering communication
NERC CIP-002–013	North American Electric Reliability Corporation Critical Infrastructure Protection Standards
Ericsson Utility 5G	Journey to the next-gen smart grid supported by 5G MCN (Ericsson, 2025)
Hitachi Energy 5G Grid	Hitachi Energy private 5G for utility and industrial customers — product documentation

About Druid Software

Druid software is a core cellular network software company based in Ireland. Druid was established in 2000 and has evolved to become one of the global leaders in Private Cellular Solutions.

Druid's **Raemis™** technology is extensively deployed around the world to deliver dedicated, resilient, secure wireless infrastructure for the exclusive use of utilities and energy providers. Druid's private 5G and 4G LTE solutions implement high-quality networks that connect applications to devices, and provide voice, messaging and high-speed data services to field engineers and other utilities personnel.

For more information:
email: enquiries@druidsoftware.com
visit: www.druidsoftware.com