

Transformation Journey Towards Software-Defined Power Systems Operations



Executive Summary

Europe's energy infrastructure is at a turning point. Designed for centralised, predictable electricity flows, the power system must absorb over 200 GW of additional renewable capacity and 50 GWh of new storage over the next 5 years, while defending against escalating cyber threats and meeting ambitious decarbonisation targets at the same time.

However, the systems that manage this complexity—Operational Technology (OT)—were built for stability, not agility. Obstacles on legacy protocols, siloed governance, and outdated security models leave critical infrastructure exposed to greater operational risks, costly delays and heightened cyber vulnerabilities.

The future of energy is decentralised, digitised and decarbonised. To achieve this vision by 2035, utilities need to embrace modular, software-defined OT architectures; real-time intelligence powered by digital twins, testbeds and Artificial Intelligence (AI)-driven automation; zero-trust cybersecurity frameworks embedded into

every layer and cross-domain interoperability to integrate legacy, cloud, and edge systems seamlessly.

For executives, the imperative is clear: OT modernisation is not a technology upgrade—it is a strategic lever for competitiveness, resilience, and compliance. By acting now, utilities not only unlock new value from Distributed Energy Resources (DER) and reduce systemic risk from cyberattacks and outages, but more importantly, future-proof their organisations against regulatory and market shifts.

This whitepaper outlines the transformation journey: from diagnosing today's OT challenges to defining architectures, investing in future capabilities, and implementing governance and talent strategies. Finally, we conclude with 10 practical actions to help leaders move decisively from strategy to execution, bringing the vision to life.



01

Introduction

OT combines physical devices with digital software and network infrastructure to monitor and control industrial processes. In the energy sector, OT is crucial for power generation, transmission, and distribution, ensuring a secure and reliable electricity supply.



Downtime in OT systems can lead to immediate and severe consequences, such as blackouts and safety hazards. While Information Technology (IT) system failures typically affect business processes, they can also indirectly impact grid stability in highly digitalised energy systems.

The energy sector is undergoing a significant technological transformation. Originally designed as robust, specialised infrastructure, OT is now influenced by digital trends seen in manufacturing and telecommunications. These sectors have integrated OT and IT more quickly, but the energy sector faces unique challenges due to stringent regulations, long asset lifecycles, and critical security needs. The energy transition, with its focus on decentralised generation, smart grids, and advanced data analytics, is accelerating OT/IT convergence. This integration offers opportunities for more efficient grid operations and intelligent automation but also exposes critical infrastructure to new risks like cyber threats, increased complexity, and regulatory challenges. Decarbonisation targets and the rapid growth of renewable energy further drive this shift. Utilities must uphold compliance, interoperability, and the secure integration of legacy systems.

1.1 Purpose, Scope and Audience

OT refers to the hardware, software, and communications infrastructure that oversee and control industrial processes. In the power sector, it upholds the secure, reliable, and efficient flow of electricity. Unlike traditional IT systems, OT directly interacts with the physical grid, where failures can cause blackouts, safety risks, and significant economic impacts. Utilities face pressure in three key areas, detailed in Chapter 2:

Technical:

Ageing assets (Chapter 2.1) – Legacy systems are difficult to maintain and integrate with modern digital solutions.

Organisational:

Bottlenecks (Chapter 2.2) – Siloed structures, unclear responsibilities, and slow decision-making processes.

Security:

Cyber threats (Chapter 2.3) – Rising cyber-attacks and fragmented governance in a networked world.

These challenges create a gap between what current OT systems deliver and what new energy systems require. Without action, utilities risk falling behind in efficiency, flexibility, and resilience, jeopardizing the energy transition.

This paper addresses and analyses the gap, outlining a strategic roadmap for OT in 2035. It defines the competencies, architectures, and governance methods needed to transform fragmented systems into an integrated, secure, and responsive operational environment. The paper is structured into four parts:

Current State Analysis (Chapter 2):

An overview of today's OT landscape, including legacy technologies, operational and organisational bottlenecks, and growing data fragmentation and cybersecurity risks.

Architecture Change (Chapter 3):

A discussion on modular and reference architectures to modernise OT and provide interoperability.

Future Capabilities (Chapter 4):

An exploration of digital innovations like digital twins, automation, and resilient infrastructure.

Strategic Direction (Chapter 5):

Recommendations for governance, architectural choices, and organisational competencies, along with rapid response mechanisms in an evolving threat landscape.

This document supports strategic planning, cross-disciplinary collaboration, and actionable steps for scalable and sustainable OT transformation. It is designed for a broad audience, including c-suite executives who set strategic direction and approve budgets; IT and OT leaders who manage transformation programmes; enterprise and solution architects who design and validate integrated systems; operations and engineering

teams responsible for implementing and maintaining these systems; regulators and policy makers who shape compliance and alignment; academic and research institutions exploring emerging technologies and best practices; and technology vendors and integrators who provide products and services. These groups will gain valuable insights and practical guidance tailored to their specific roles and needs.



1.2 Vision 2035: Software-Defined, Resilient, and Sustainable Power Systems

By 2035, Europe's energy infrastructure will be transformed into a decentralised, digitised and decarbonised ecosystem—a grid that is intelligent, adaptive and secure by design. The control room will evolve from a static monitoring hub into a dynamic, collaborative nerve center, where human operators and AI agents work side by side to forecast demand, manage renewable variability, and ensure real-time resilience.

This future grid will be powered by:



Cognitive and Collaborative Operations:

Human operators will team up with AI agents that forecast demand, run "what-if" scenarios, and manage grid congestion or renewable energy fluctuations. These AI agents will guide operators to take the necessary actions and execute some tasks autonomously.



Real-Time Testbeds and Digital Twins:

Large-scale digital twins will simulate electrical and cyber-physical systems, enabling predictive and safe testing. Virtual testbeds will allow secure experimentation with new methods before they are deployed in the real world.



Semantic and Technological Interoperability:

Heterogeneous systems will communicate seamlessly using standard data structures and semantic layers. Secure, controlled data exchange between utilities, operators, and partners will become standard.



Cyber-Physical Security and Resilience:

Security will be integrated into all layers, using zero-trust, real-time monitoring, and redundancy to verify that systems can recover from cyberattacks, failures, or disasters without compromising safety.



Smart Infrastructure and Communication:

Ultra-low latency networks will enable secure control of edge devices, local coordination, and efficient management of distributed assets.



Human-Centric and Multi-Party Collaboration:

Operations will leverage immersive visualisations, Augmented Reality (AR), and natural interfaces for simplified control of complex systems. Real-time collaboration between Transmission System Operators (TSOs), Distribution System Operator (DSO), vendors, and researchers will be facilitated through control centers.



Sustainable, Efficient, and Proactive Operations:

OT will move from passive monitoring to proactive energy flow optimisation, reducing the carbon footprint and extending asset lifespan through predictive maintenance and intelligent scheduling.

1.3. Industry Trends

Europe's OT landscape is undergoing a significant transformation driven by digitalisation, decentralisation and heightened cybersecurity needs. As electric systems become more connected and intelligent, operational efficiency improves, but so does the risk of new threats. Regulatory frameworks like the EU's Fit for 55 [1] and NIS2 [2] Directive are accelerating decarbonisation and mandating stronger cybersecurity, while technological advancements in AI, edge computing, digital twins, and 5G are providing the tools for more adaptive and resilient infrastructures.

Economic pressures for efficiency and resilience, along with social and workforce demands for sustainability and digital innovation, are pushing utilities toward next-generation OT systems. OT, which traditionally monitored and controlled industrial processes in isolation, is now evolving into a highly interconnected, data-driven ecosystem.

In the energy sector, this shift is particularly evident. AI-driven process optimisation, predictive maintenance and intelligent automation are becoming crucial for real-time decision-making and operational resilience. Digital twins, virtual representations of physical assets, enable continuous monitoring, simulation and system-level optimisation. Europe's digital twin market, valued at €363 million in 2024, is projected to grow to €981 million by 2032, reflecting a Compound Annual Growth Rate (CAGR) of 13% [3].

Edge computing is gaining momentum as a foundational technology for decentralised energy systems. By processing data closer to the source, edge solutions reduce latency, minimise bandwidth consumption and support localised autonomy—vital for managing the increasing number of IoT (Internet of Things) devices in

distributed grids. Europe's edge computing market, with strong adoption in utilities and infrastructure, is valued at €4 billion in 2024 and is expected to reach €52 billion by 2033 (CAGR: 32%) [4].

Decentralisation is most apparent in the energy sector, where DERs like solar, wind, battery storage and virtual power plants are reshaping traditional grid architectures. Over 200 GW of distributed renewable energy capacity is already installed in Europe, with solar Photovoltaic (PV) leading the way. Germany, France and the UK are at the forefront, and the continent added over 10 GWh of battery storage capacity in 2022 alone [5]. Between 2019 and 2021, 167 GW of distributed PV capacity was deployed globally—more than the combined peak demand of France and the UK—with a significant portion in Europe [6].

The growing interconnectedness and complexity of OT systems have made cybersecurity a top priority. With cyberattacks on critical infrastructure becoming more sophisticated, it's essential to adopt zero-trust security architectures, robust risk mitigation strategies, and resilient defence mechanisms to maintain system reliability. Germany's OT security market, currently valued at \$3.0 billion in 2024, is projected to nearly double by 2033 [7].

These trends are transforming OT environments from isolated, deterministic systems into interconnected, intelligent ecosystems. To thrive, these ecosystems need integrated approaches that balance innovation, security, and operational excellence. In the coming sections of this whitepaper, we will delve into future capabilities such as digital twins, autonomous functions, semantic interoperability, advanced communication infrastructures, and robust cybersecurity frameworks.

02

Diagnostic Overview of the Existing OT Landscape

The current OT landscape is a result of decades of incremental progress, with legacy systems, proprietary protocols, and siloed operations still prevalent. While these technologies have proven reliable, they were not designed to meet today's needs, such as cybersecurity, interoperability, cloud integration, and real-time analytics.



This chapter sets the baseline for understanding our current situation and identifies the key barriers that must be addressed to transform OT into a secure, flexible, and data-driven environment.

The chapter is divided into three sections. Together, these sections provide a comprehensive foundation for the transformation journey.

2.1 Legacy Landscape

Structural Characteristics

Today's power systems are largely built on legacy OT systems that have evolved incrementally over decades. These systems have provided reliable and stable performance, but their outdated design is increasingly incompatible with modern, data-driven, and distributed power systems. Legacy OT environments are often characterised by single-purpose hardware or tightly coupled modules that are difficult to upgrade. This rigidity is exacerbated by vendor-locked proprietary platforms that limit flexibility and make integration with other technologies challenging. Over time, utilities have added systems in silos to meet new demands, leading to a fragmented architecture. This fragmentation results in broken toolsets, sub-optimal data exchange, and reduced coordination across operational domains.

Technology Constraints

The structural rigidity of these systems directly impacts their technological constraints. Critical systems like Supervisory Control and Data Acquisition (SCADA) have been heavily customised for specific networks, resulting in slow upgrade cycles, cumbersome maintenance, and a growing reliance on a shrinking pool of knowledgeable engineers.

Operational and Cultural Barriers

The challenges extend beyond technical issues. Operational practices and cultural factors within utilities also play a significant role. OT experts have adapted to the limitations of past network infrastructure, and operators are often reluctant to adopt new systems. Maintenance remains labour-intensive, and incremental patches often require vendor support. Backup processes still rely on manual logs and USB-based file transfers.

Communication protocols like Profibus, Modbus, DH+, and RS-232 are being phased out, but at a slower pace than in other industries, and are maintained by a dwindling number of experienced engineers.

Security and Resilience Gaps

Security and resilience gaps further complicate the situation. Legacy infrastructure was designed with "security-by-air-gapping" in mind, offering minimal integration with modern security architectures. These systems lack real-time monitoring, sophisticated zero-trust frameworks, and intrusion detection capabilities. Additionally, the integration of third-party services, such as rooftop solar, battery storage, and demand response, introduces new points of entry and complexity, deepening vulnerabilities.

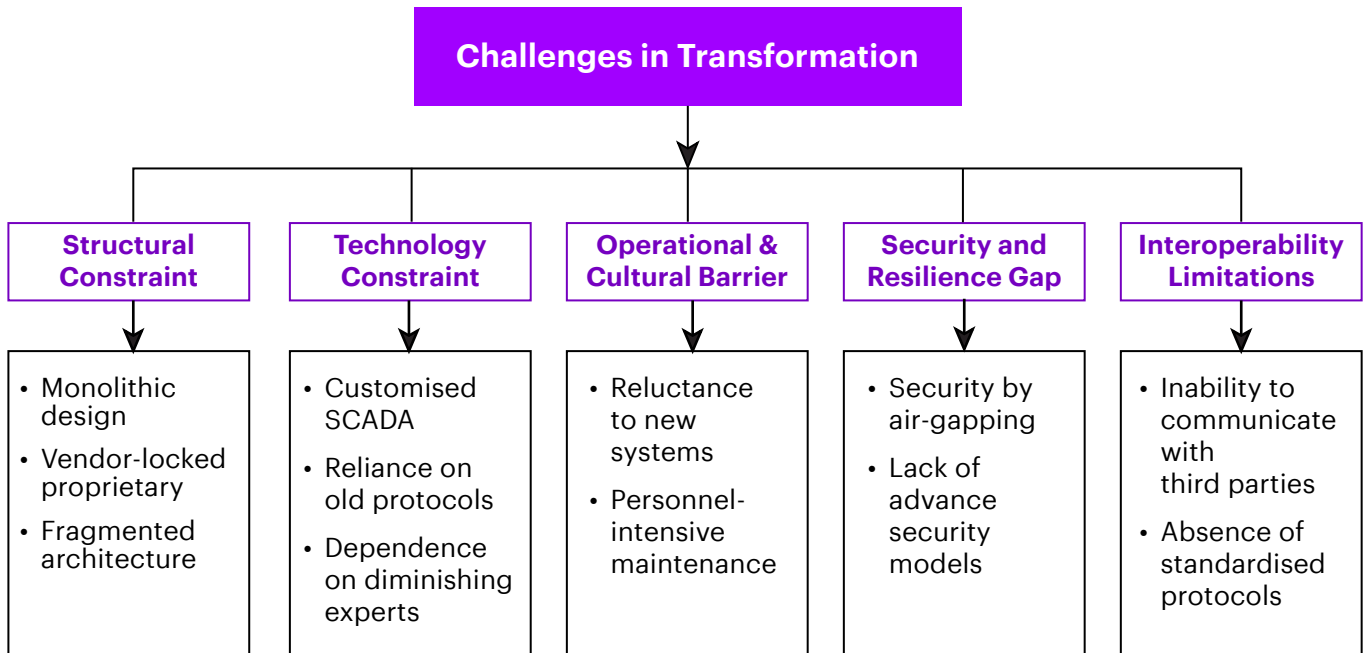
Interoperability Limitations

Interoperability is another significant issue. Legacy OT systems struggle to exchange information or communicate with third-party service providers, aggregators, and other utilities. This challenge is compounded by the lack of universally accepted protocols or harmonised data models, hindering seamless collaboration in the evolving, multi-stakeholder energy ecosystem.

Conclusion

These challenges highlight how legacy OT, once valued for its robustness, has become a roadblock to the transition toward a low-carbon economy. The rigidity, reliance on outdated technology, and incompatibility of legacy OT systems prevent the shift to open, flexible, and secure platforms. Overcoming these obstacles is essential for creating an intelligent, sustainable grid. Figure 1 gives a clear overview of the challenges faced by legacy OT during its transformation.

Fig 1: Challenges of Legacy OT Review



2.2 Organisational & Operational Challenges

Utilities face significant organisational and operational hurdles that hinder their ability to adapt to decentralisation and digitalisation. Siloed structures, fragmented responsibilities, and the gap between IT and OT domains add complexity, reduce responsiveness, and increase risk [11].

Structural and cultural differences among utilities also pose substantial barriers. Departments like operations, asset management, network planning, cybersecurity, and IT infrastructure often operate independently, with few processes for regular coordination. This isolation leads to blind spots in system design, delayed incident responses, and slow adoption of new technologies, especially as the distinction between IT and OT continues to blur.

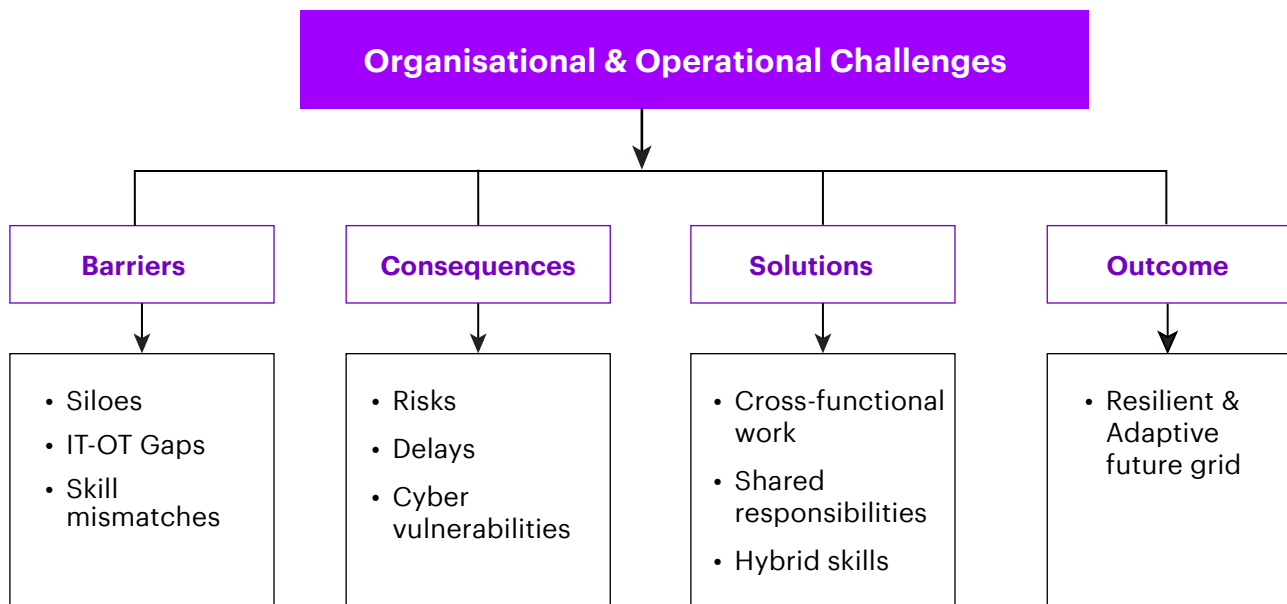
A key issue is the misalignment of skills and responsibilities. For instance, in grid infrastructure, simple, unmanaged switches were once sufficient. Today, the grid uses complex managed switches that require advanced IT expertise to set up and secure against cyber threats. OT teams typically lack these skills, and IT teams are reluctant to handle in-field equipment, leading to gaps in responsibility for critical components.

A similar challenge applies to edge computing. What were once basic field PCs are now high-performance, rack-mounted virtualised servers. These require IT-level support for maintenance, updates, and security, but they are placed in remote, harsh, and unique environments. IT staff may lack the operational knowledge for these settings, while OT staff may not have the technical skills needed for modern virtualisation platforms. This results in inconsistent maintenance, Delayed updates, and heightened vulnerability.

These issues are not just operational; they are systemic organisational gaps. Without shared ownership, hybrid skill sets, and effective cross-domain communication, utilities may struggle to leverage even the most advanced technologies.

Additionally, entrenched organisational cultures often resist change, making teams reluctant to adopt new digital workflows or cross-domain collaboration. Differences in mindset between traditional operations-focused teams and innovation-driven IT functions can further slow transformation and hinder unified progress. Figure 2 represents the overview of organisational and operational challenges.

Fig 2: Organisational and Operational Challenges Overview



To achieve the 2035 Vision,

utilities need to rethink their governance, workflows, and workforce structures. This involves:



Integrating cross-functional operations into daily business practices.



Developing hybrid technical and operational skill sets.



Establishing shared responsibility for critical infrastructure.



Organising teams to support modular, interoperable, and secure OT systems.

Aligning organisational structures with technical capabilities will enable a resilient, adaptive grid—supporting real-time decision-making, embedded cybersecurity, and seamless multi-party collaboration.

2.3 Data & Cybersecurity Concerns

OT environments face increasing pressure to modernise for better security and data integrity. However, many current infrastructures still rely on legacy systems and older protocols. Standards like Modbus, DNP3, and IEC 104, while foundational for industrial control, were not designed with modern cybersecurity best practices in mind. These protocols often lack robust encryption, authentication, and tamper detection, making them vulnerable to attacks such as spoofing, replay attacks, and unauthorised remote access.

Older devices often remain unpatched due to operational limitations or vendor dependencies, leaving them exposed to exploitation. Without regular updates, vulnerabilities accumulate, increasing the risk of sophisticated cyber-attacks on major grid assets.



Data Governance Challenges

OT environments also struggle with data quality, access, and governance. Accessing standardised OT data often requires manual workarounds, leading to inconsistent datasets. Consumers, despite having consumption data, may lack the awareness to handle it effectively. Fragmentation and silos exacerbate this issue, as data is stored in separate systems and captured by different applications with varying transformations and lineage. Manual handling, grey IT, and heavy reliance on spreadsheets or ad-hoc processes introduce human errors, inconsistent calculations, and conflicting reports. The lack of standardisation in data models and governance structures limits the scalability of analytics tools needed for consistent insights. Non-standard tools, fragmented capabilities, and varied datasets increase costs, degrade data quality, and hinder the advanced analytics essential to the 2035 Vision of proactive, data-driven OT.



Poor Access Controls and Network Architecture

Access rights management in OT environments is often sub-optimal, creating multiple attack vectors. Standard or generic passwords are commonly used, and overly broad access rights grant more control than necessary. In some cases, former employees' login credentials remain active, further increasing exposure. Flat network topologies, typical in older systems, worsen the situation: once an attacker breaches the perimeter, they can move laterally without detection, compromising multiple control layers.



Connectivity Risks in Modernisation

As power companies adopt real-time monitoring, DERs, and smart automation, the vulnerabilities of outdated equipment become more pronounced. These older devices often cannot meet the encryption, bandwidth, and oversight requirements of modern systems. Low-bandwidth telemetry channels, including some via dial-up, limit data delivery and reduce situational awareness, constraining grid optimisation opportunities.



Interoperability and Trust Barriers

Effective and trusted data exchange remains a significant challenge. Concerns over confidentiality, ownership, and potential misuse of data often discourage collaboration. Non-compliance with existing standards, or the absence of data standards, creates a lack of semantic interoperability, hindering smooth integration between utilities, market operators, and third-party providers.

These constraints directly oppose the 2035 vision for seamless cross-organisational data exchange and coordinated multi-actor grid management.

03

Architectural Transformation

The energy industry is moving toward decentralised, renewable, and digitally integrated systems. This shift requires a fundamental overhaul of OT architectures.



The 2035 Vision calls for grid control environments that are resilient, adaptive, interoperable, and secure, capable of continuous innovation while tackling legacy dependencies, organisational silos, cybersecurity risks, and fragmented data governance.

In this chapter, we explore three foundational design principles to achieve this vision: modular transition, reference architectures, and architectural enablers.

3.1 Modular Transition

Traditionally, OT systems were tightly integrated and vendor-specific, relying on proprietary protocols, data formats, and upgrade paths. While this model provided stability in the past, it now hinders the agility needed for the 2035 grid vision. The challenges of legacy systems, vendor lock-in, fragmented data, and slow innovation stem from this monolithic architecture.

A modular approach moves OT architecture toward open standards, open-source modules, and API-first (Application Programming Interface) designs. This allows core functionalities like analytics, control logic, and visualisation to be upgraded, replaced, or extended independently. By decoupling components, utilities can quickly adopt new technologies, embrace innovations from various vendors, and avoid costly full-system replacements.

Key enablers for advancing OT data capabilities include:

Standard Data Models:

Common Information Model (CIM) and IEC 61970/61968 ensure uniform semantics.

Interoperable APIs:

REST, gRPC (Remote Procedure Calls) and OPC UA (Open Platform Communications Unified Architecture) enable seamless component interaction.

Digital Twins and Simulation:

These tools allow for testing upgrades before deployment.

Event-Driven Ingestion:

Protocols like Message Queuing Telemetry Transport (MQTT) and Kafka feed a central OT data lake, making data readily available for cross-functional use.

Open Implementations:

Open-source-inspired functions support ongoing advancements

Strategic advantages of modularity:

Faster Innovation:

AI/ML (Machine Learning) applications, predictive maintenance, and DER control can be implemented gradually.

Vendor Neutrality:

Competitive procurement of each module prevents lock-in.

Cost Efficiency:

Reduced integration work and focused upgrades lower lifecycle costs.

Ecosystem Growth:

Open interfaces foster third-party solutions and specialisation.

However, modularity is not the same as fragmentation. Success requires a clear integration strategy, well-defined data agreements, and robust orchestration mechanisms. Strong lifecycle and version control are essential to manage updates across modules, and configuration harmonisation minimises integration risks as the number of modules grows.

A phased migration is often the most practical approach, prioritising upgrades by criticality, readiness, or Return On Investment (ROI). This method gradually integrates legacy systems into the modular environment.

In summary, modular transition is not just a technical choice but a strategic direction for the 2035 vision. It bridges legacy limitations with the flexibility, security, and scalability needed for the new energy system.

3.2 Reference Architecture

While modularity defines how components interact, a reference architecture make sure that the entire system remains coherent, scalable, and interoperable. In the energy transition towards 2035, this distinction is crucial: without a common design, modular solutions can become isolated, rather than forming a resilient, future-ready ecosystem.

Currently, operators lack a widely adopted, future-proof reference architecture for OT. Existing systems are often built on legacy protocols, proprietary technologies, and incremental integration projects. To bridge these gaps and support digitalisation, IT/OT convergence, and cross-industry interoperability, a shared architectural blueprint is essential.

Starting Point: SGAM as the Energy-Specific Foundation

The Smart Grid Architecture Model (SGAM), developed under the European Commission's Mandate M/490, is the most recognised reference framework for smart grid design in Europe (see Figure 3). SGAM serves as a technology-neutral structure, enabling stakeholders to describe, analyse, and compare smart grid systems consistently.

At its core, SGAM is a three-dimensional model, as illustrated in Figure 3, comprising:

Interoperability Layers (Business, Function, Information, Communication and Component):

These layers represent the perspectives needed to achieve interoperability across both technical and organisational aspects.

Domains (Bulk Generation, Transmission, Distribution, DERs and Customer Premises):

These domains cover the entire electrical energy conversion chain, from central generation to end-users.

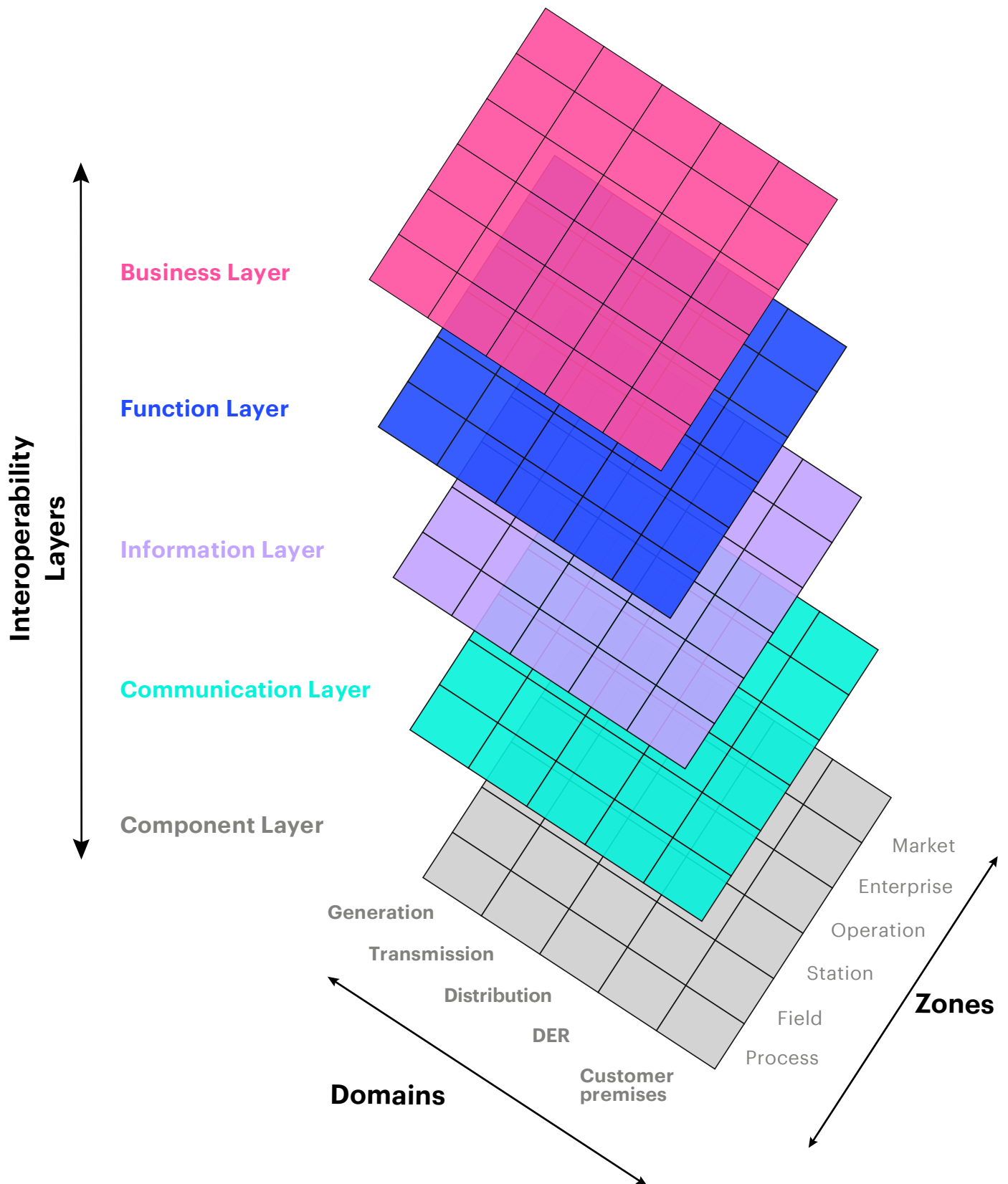
Zones (Process, Field, Station, Operation, Enterprise and Market):

These zones capture the hierarchical management levels of the power system, from real-time process automation to enterprise management and market operations.

By integrating these dimensions, the framework offers a common language for diverse stakeholders, from regulators to utilities and vendors. It enables consistent mapping of use cases across layers, domains, and zones, and a basis for gap analysis, highlighting where standards are missing or insufficient for interoperability. For example, IEC 61850 aligns with the Component, Communication, and Information Layers in the Process, Field, and Station Zones, while the CIM, IEC 61970/61968 primarily resides in the Information Layer at the Operation, Enterprise, and Market Zones. This mapping helps systematically analyse how standards support specific use cases and identify interoperability gaps. [15][16]

However, SGAM has limitations for future-oriented OT architectures. It does not explicitly address digital twins, lifecycle data integration, semantic data sovereignty, cross-industry data spaces, AI-driven operational intelligence, or governance mechanisms needed for secure, multi-party data exchange. These gaps reflect the evolution of the energy system since SGAM's inception. As the grid becomes more distributed, digitalised, and interconnected, additional concepts are needed to complement SGAM. Lifecycle orientation and semantic interoperability, as seen in manufacturing frameworks like RAMI 4.0, offer valuable extensions. Similarly, EU blueprint projects show how SGAM can be enhanced with microservices, edge-cloud coordination, and secure data exchange platforms. The int:net project [18] also emphasises the need to evolve SGAM to address emerging requirements.

Figure 3: SGAM Framework combining the three dimensions [15]



Complementary Perspective – RAMI 4.0

While SGAM is tailored for the energy sector, it lacks certain dimensions crucial for future OT systems. Insights from other industries, such as manufacturing, can provide valuable inspiration. The Reference Architecture Model Industrie 4.0 (RAMI 4.0), introduced in DIN (Deutsches Institut für Normung e.V.) specification 91345 [16] and widely adopted in manufacturing, offers a structured approach to manage interoperability, lifecycle, and semantics in highly diverse environments.

RAMI 4.0 is widely recognised in manufacturing for structuring complex, interconnected systems. It introduces a lifecycle perspective, spanning asset design, engineering, operation, and decommissioning. This dimension is largely missing in SGAM, which focuses more on interoperability at a specific point in time. RAMI 4.0 also emphasises semantic interoperability through the Administration Shell, which provides standardised digital representations of assets, ensuring consistent information across vendors and domains [17]. Additionally, it stresses modularity and hierarchical integration, enabling flexible scaling from local edge devices to enterprise platforms and cross-industry data spaces [17].

For the energy sector, these principles are highly relevant. Lifecycle orientation helps manage long-lived and diverse assets consistently. Semantic asset models are essential for secure and trusted data exchange across operators and industries. Modularity and hierarchy support the integration of edge computing and DERs into broader system architectures. Therefore, RAMI 4.0 is not a replacement for SGAM but a complementary framework. While SGAM maps energy domains, zones, and interoperability layers, RAMI 4.0 adds lifecycle, semantics, and modular integration. Together, they create a more future-proof basis for OT architecture in 2035.

From Framework to Blueprints

Frameworks like SGAM and RAMI 4.0 offer valuable guidance. SGAM Organises the energy value chain across domains, zones, and interoperability layers, while RAMI 4.0 focuses on lifecycle management, semantic asset models,

and modular integration. However, their full potential is realised when these frameworks are translated into concrete design patterns.

In recent years, the European Commission has funded numerous R&D and demonstration projects under the BRIDGE initiative. Many of these projects map their system designs to SGAM and incorporate RAMI-inspired concepts, such as lifecycle data management and semantic interoperability. The most comprehensive result of this work is the European Energy Data Exchange Reference Architecture (DERA 2.0) [18], which builds on SGAM and references RAMI 4.0 for cross-sector data spaces and governance.

The report synthesises the architectures of 20 major EU projects. For example, OneNet and INTERFACE show how distributed balancing and flexibility services can be coordinated between TSO and DSO, demonstrating the practical application of SGAM's functional layering. InterConnect and Platone emphasise semantic interoperability and digital asset representations, aligning with RAMI's concept of the Administration Shell. EU-SysFlex offers insights into cross-border balancing, while BD4NRG and TwinERGY highlight the importance of data spaces and AI-driven analytics, extending SGAM with lifecycle and semantic considerations that mirror RAMI's approach.

DERA demonstrates that interoperability is not just about standards but about the systematic integration of architectural frameworks, semantic governance, and lifecycle principles. SGAM verifies alignment with the energy sector's structure, while RAMI provides the tools to evolve towards cross-sector, data-driven architectures.

Control-Plane and Data-Plane:

A Reference Model for 2035

The combination of SGAM and RAMI 4.0 forms the conceptual foundation for structuring energy system architectures. Projects like OneNet and InterConnect have shown how these frameworks can be applied in practice. Building on this foundation, we can outline a reference model for 2035 that integrates the strengths of both approaches into a coherent target architecture. This target architecture is based on a clear

separation of concerns between the Control-Plane and the Data-Plane:

- The Control-Plane handles deterministic, real-time functions at the process, field, and station levels, ensuring operational safety and protection.
- The Data-Plane enables semantic integration, analytics and cross-operator value creation, supported by cloud-native platforms, APIs and governance mechanisms.
- The Convergence Zone (industrial DMZ and edge) securely connects the two planes, allowing information to flow without compromising latency or safety-critical requirements.

Figure 4 illustrates this future state OT/IT reference architecture. It extends the well-known Purdue Model by incorporating edge computing, industrial DMZs, and cloud-based analytics platforms. It shows how traditional OT layers (physical process, Programmable Logic Controller

(PLC), SCADA, historians) are complemented by IT Enterprise Resource Planning (ERP), asset management) and enhanced by a data platform that includes pipelines, data lakes, time series databases, machine learning engines, and self-service APIs. Security is integrated at multiple levels, with firewalls separating OT and IT, and governance functions ensuring compliance and trust. This model embodies the principles derived from SGAM and RAMI:

From SGAM:

structural orientation across domains, zones, and interoperability layers.

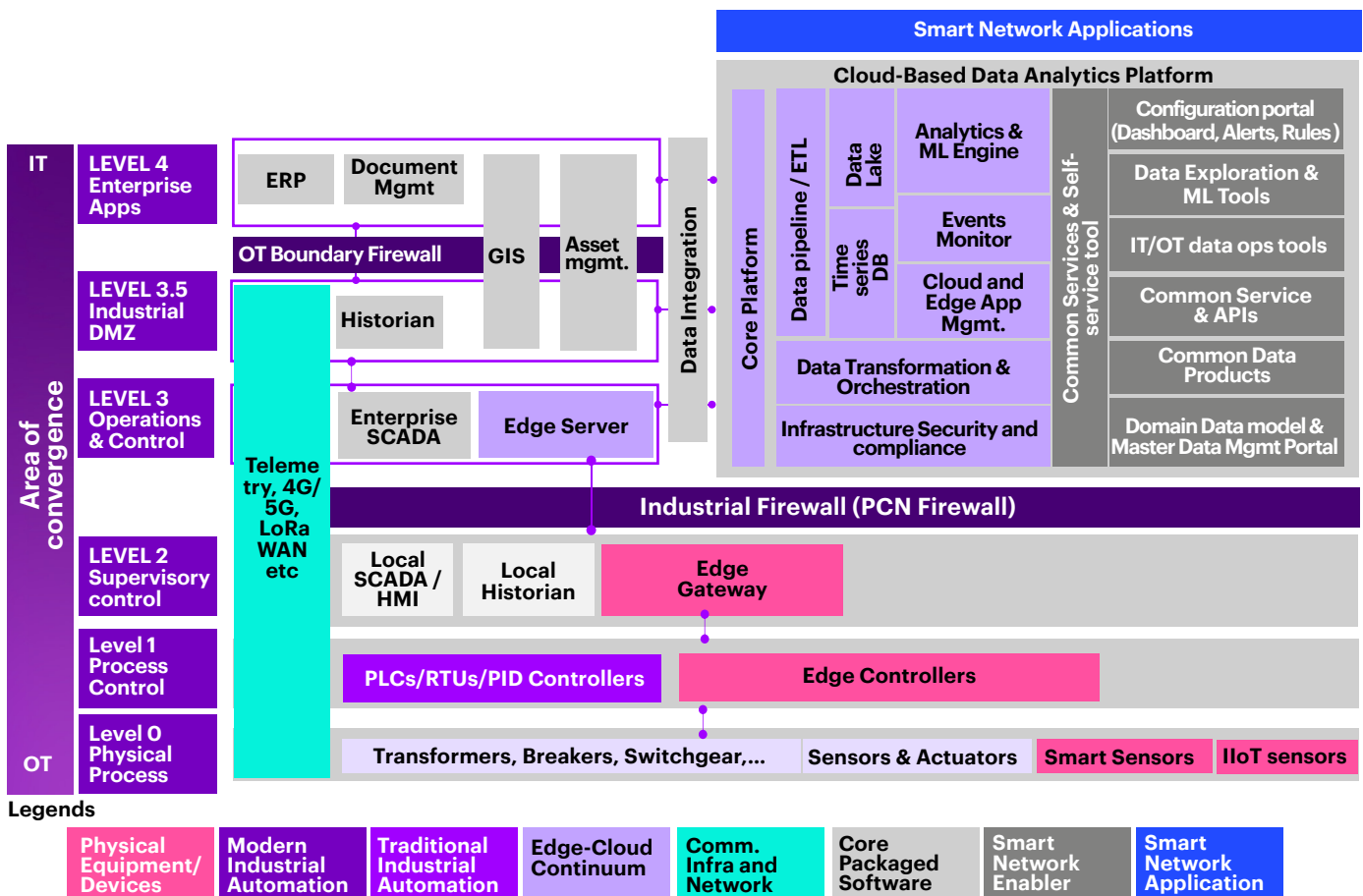
From RAMI 4.0:

lifecycle orientation, semantic digital representations, and modular integration.

From Blueprints:

validated design patterns for flexibility markets, cross-border coordination, and semantic data exchange.

Figure 4: Illustrative IT/OT Reference Architecture



3.3 Architectural Enablers

To achieve modular and future-ready OT architectures, utilities need a set of essential technologies that serve as the operational backbone. These enablers bridge the gap between conceptual frameworks and functional systems, ensuring programmability, scalability, resilience, and secure interoperability across diverse environments.

One key enabler is the integration of cloud and edge computing. Cloud platforms offer flexible capacity for analytics, forecasting and cross-operator coordination, while edge computing provides low-latency intelligence near critical assets like substations, DERs and microgrids. This combination allows utilities to scale uniformly while keeping protection and automation local and deterministic, which is crucial for the reliability of decentralised grids.

Containerisation and virtualisation also play vital roles by separating applications from hardware and promoting vendor independence. Grid services can run in standardised, portable environments, speeding up innovation, simplifying deployment, and reducing reliance on proprietary systems. Open-source initiatives, such as those led by Linux Foundation Energy (LFE), enhance collaboration, transparency, and shared innovation across the energy sector.

Data platforms and event-driven architectures are equally important. They process vast amounts of real-time telemetry for predictive analytics,

situational awareness, and anomaly detection. Event-driven models maintain timely responses to critical system events, minimizing downtime and improving operational decision-making.

Cybersecurity is non-negotiable. As IT and OT converge, traditional perimeter-based protections are no longer sufficient. Adopting zero-trust models ensures continuous verification and identity-driven access, but this must be complemented by OT-specific security patterns. Standards like IEC 62443 for zones and conduits, IEC 62351 for secure communications, and Parallel Redundancy Protocol (PRP)/High-availability Seamless Redundancy (HSR) for resilience are essential. Orchestration and automation frameworks, along with DevSecOps practices, assures consistent deployments, policy-driven operations, and continuous monitoring. In OT, this means continuous validation, controlled release cycles, and regulatory compliance to maintain system resilience and enable rapid service introduction.

Together, these enablers form the foundation of a software-defined power system. They unlock innovation, flexibility, and resilience but also present challenges, such as integrating legacy infrastructures, meeting evolving compliance requirements like NIS2, and addressing the skills gap between traditional OT engineers and IT specialists. Overcoming these hurdles is essential to realising the 2035 vision of adaptive, intelligent, and secure energy systems.

04

Future Capabilities

The future of the energy industry is decentralised, digitised, and decarbonised. To achieve this vision, utilities must develop operational capabilities far beyond traditional control methods.



Today's challenges—legacy infrastructure, fragmented vendor ecosystems, cyber threats, and the high stakes of live operations—pose significant barriers. However, next-generation OT capabilities such as digital twins, testbeds, autonomous control, AI-powered forecasting, and sector-coupled energy management will lay the foundation for this future. These technologies will help utilities predict, simulate, and respond to changes before they impact the physical grid, ensuring operational stability and innovation.

4.1 Digital Twins and Testbeds

As the energy sector rapidly digitises, the ability to predict, simulate, and verify operating scenarios has become essential. Digital twins and testbeds are key enablers of this transformation, shifting utilities from reactive crisis control to proactive, intelligence-guided operations.

A digital twin is more than just a 3D model or static diagram. It is a high-fidelity digital replica of a physical asset, process, or system, enriched with real-time operational data and contextual metadata. In the energy context, this means simulating the behaviour of a substation, modelling grid-wide power flows with different DER scenarios, or assessing the health and ageing of transformers. Digital twins combine:

Static Models:

asset topology, configuration and design parameters

Dynamic Models:

real-time telemetry, control systems and operating conditions

Predictive Models:

AI and machine learning algorithms that forecast, optimise and recommend

Together, these elements allow digital twins to diagnose inefficiencies, predict faults, and support data-driven decisions.

Testbeds, on the other hand, offer a secure, controlled environment for testing real-world changes without disrupting operations. They can be physical, virtual, or hybrid, but their key feature is isolation. Testbeds replicate the live OT environment's behaviour closely enough to test changes while keeping production systems safe. This is crucial for:

- Testing vendor hotfixes, security patches, and software upgrades
- Simulating disaster scenarios to understand network behaviour under stress
- Training operators in realistic, risk-free environments

- Prototyping and validating modifications before live deployment

Without testbeds, utilities are forced to "test in production," risking downtime, cascading failures, and service interruptions.

The applications of testbeds extend beyond change management. They enable:

- Functional testing of new control algorithms
- Protocol compatibility testing across different vendor systems
- Data model alignment validation before integration
- Practice of black start procedures
- Training on DER coordination during peak demand
- Simulation of dangerous or expensive "what if" scenarios

By using testbeds, utilities can verify operational readiness is a quantifiable, reproducible process, not a matter of chance.

When used together, digital twins and testbeds create a powerful feedback loop. Digital twins generate simulated scenarios that testbeds can validate, and the results from testbeds improve the predictive accuracy of the twins. This synergy addresses challenges such as:

- Upgrading legacy infrastructure without risking outages
- Closing security gaps in flat network designs and siloed information
- Managing integration risks with new vendor technologies

In a future-ready OT ecosystem, these capabilities will be integrated into a common data and control architecture. Digital twins will draw from time-synchronised data streams through SCADA, Power Management Unit (PMUs), and IoT sensors,

while testbeds will be managed via modular, API-first platforms that support both edge and cloud execution. Reference models like SGAM and RAMI 4.0 uphold alignment with industry best practices, mapping these capabilities across business, functional, information, communication, and component layers.

The strategic value of digital twins and testbeds lies in their ability to de-risk innovation. Utilities can test new vendor solutions, regulatory compliance scenarios, and cyberattack models without making procurement commitments or risking real-world disruptions. By moving most operational changes to a controlled environment, utilities

can minimise unplanned downtime, extend asset lifecycles, and accelerate the safe adoption of emerging technologies.

For businesses facing the dual pressures of decarbonisation and digitalisation, the question is no longer whether digital twins and testbeds are nice to have, but how soon they can be implemented. Those who integrate these capabilities into their OT strategy will innovate with confidence, knowing that changes have been verified, scenarios practised, and results quantified before reaching the live grid.

4.2 Intelligent and Automated Functions

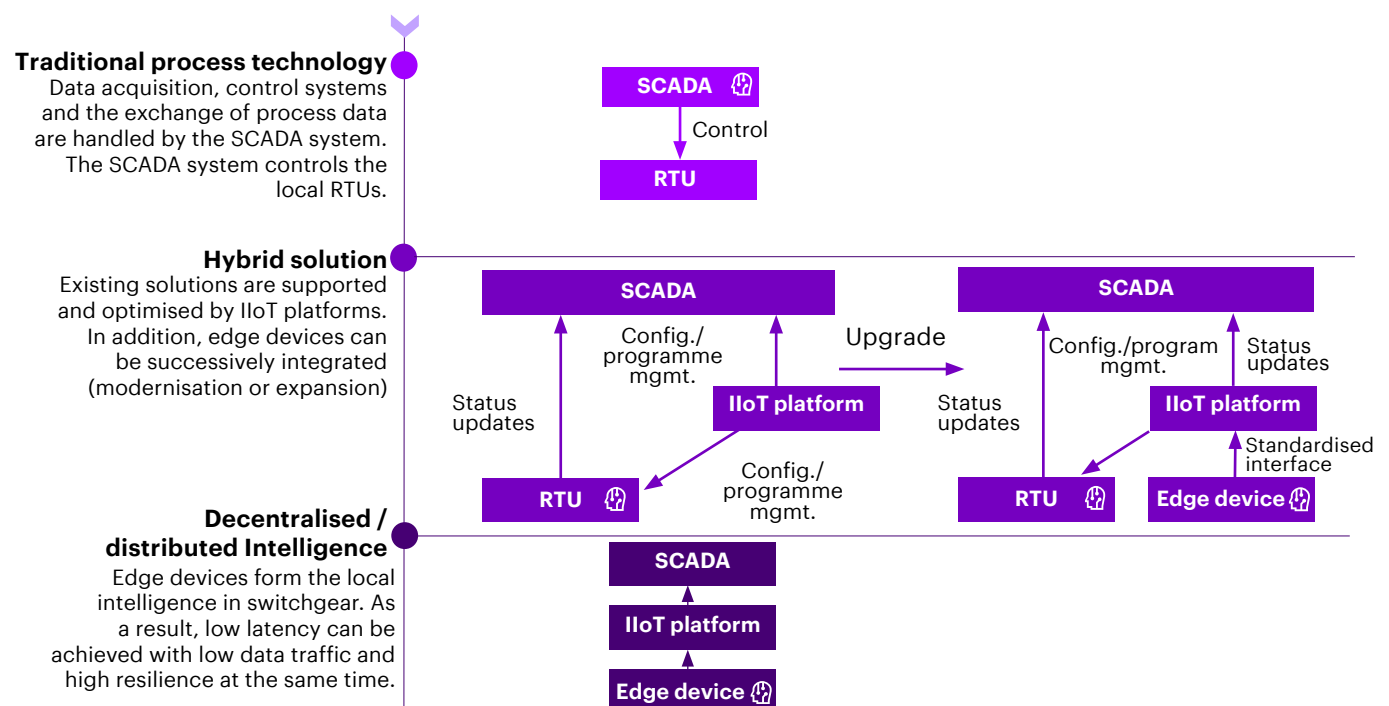
As modern power systems grow more complex due to the rise of DERs, electrification, and advanced digital technologies, utilities are embracing intelligent and autonomous functions to improve efficiency, reduce risks, and support real-time decision-making. These functions leverage AI, ML, and automation to shift from reactive to proactive and predictive operations.

Intelligent functions can analyse vast amounts of real-time data, identify anomalies, predict future conditions, and suggest the best actions. They are designed to augment, not replace, human decision-making. Autonomous functions take this a step

further by executing predefined tasks with minimal intervention, such as detecting faults, restoring services, and enabling self-healing grid mechanisms. Together, these capabilities boost system resilience, reliability, and adaptability.

Transitioning from a traditional SCADA-to-Remote Terminal Unit (RTU) architecture to a modern ecosystem that includes IIoT platforms and edge devices should be a gradual, phased process. This approach maintains cost-effective integration of existing assets. The figure below provides a high-level overview of this transition.

Figure 5: High Level Transition Overview



Deploying these functions goes beyond just technical innovation. Building trust in AI models is just as crucial as creating the models themselves. This requires strong governance and structured frameworks. Organisations need clear guidelines for responsible AI, outlining how trust is built, monitored, and maintained. On the technical side, consistent processes for managing models—from development to deployment, monitoring, retraining, and retirement—are essential to maintain long-term reliability. Automated model management, including "champion-challenger testing", monitoring tolerances, and safely replacing outdated models, is key to preventing drift or failure in live systems.

Agentic AI is emerging as a vital enabler, linking functions across various platforms like enterprise systems, Geographic Information System (GIS), and Advanced Distribution Management System (ADMS). By coordinating processes across different domains, agentic frameworks allow for the design of more complex and adaptive workflows, potentially leading to autonomous actions at scale. However, this evolution underscores the importance of transparency, explainability, and clear accountability to verify safety and compliance in critical operations.

Fig 6: AI Capabilities

Traditionally there have been 4 types of analytics, GenAI enhances this & Agentic combines them


















Agentic				
Descriptive	Diagnostic	Predictive	Prescriptive	Generative
What happened?	Why did this happen?	What might happen in the future?	What should we do next?	How Gen AI can help with the execution?
KPIs 	Analyse 	Pattern 	Simulate 	Advise 
Aggregation 	Scenario 	Forecast 	Optimise 	Create 
Statistics 	Segment 	Model 	Recommend 	Code 
				Automate 
				Protect 

Figure 6 illustrates the evolution of analytics, moving from explaining what happened and why to predicting future outcomes and recommending actions. Generative AI further enhances this by enabling execution, advising, creating, coding, automating, and securing, making analytics smarter and more actionable.

AI is already making a practical impact in OT. Anomaly detection helps operators identify unusual data patterns that could signal equipment faults, cybersecurity threats, or technical errors, allowing them to address issues before they escalate. Large Language Models (LLMs) can interpret operational data, diagnose problems, and offer clear recommendations, improving decision-making speed and quality.

Predictive maintenance, another key area, uses IoT sensors and machine learning to detect early signs of equipment wear. This helps utilities schedule timely interventions, reducing downtime, extending asset life, and enhancing safety while cutting costs.

These technologies are shifting the paradigm from reactive to proactive, data-driven operations. By integrating intelligent analytics, partial automation, and eventually autonomous functions within a trusted governance and technical framework, utilities can create a more efficient, resilient, and adaptive grid. While full autonomy will not happen overnight, the gradual adoption of these capabilities is a practical and essential step toward the future of energy systems.

4.3 Interoperability and Semantics

As energy systems evolve into modular, data-driven, and multi-vendor ecosystems, interoperability is essential, not an afterthought. In next-generation OT architectures, applications will be built and deployed on modular platforms. For these applications to communicate and operate effectively, they must be built upon standardised data models, irrespective of the vendor or underlying system.

Interoperability means different systems, devices, and software can work together seamlessly, exchanging and understanding data without manual intervention or custom integrations. This requires harmony on two levels:

Syntactic Interoperability:

Ensuring systems can technically exchange data using compatible formats and protocols.

Semantic Interoperability:

Making sure all stakeholders interpret the data in the same way.

In the energy industry, the CIM is a key standard for interoperability in Europe and North America. CIM provides a standard semantic model, ensuring data has a uniform meaning across various systems. Building on CIM, ENTSO-E's Common Grid Model Exchange Standard (CGMES) enhances these functions by enabling dynamic real-time models of the power grid, improving operational coordination between TSO and DSO.

Additional IEC standards like IEC 61970, 61968, 62325, and 61850 are widely used in utility companies and substations to support interoperability. Protocol converters and gateway devices are crucial in mixed-protocol systems, translating between different formats to have communication between disparate systems.

However, achieving interoperability isn't just about standardizing modern systems; it also involves integrating legacy devices. These older devices use proprietary protocols that weren't designed for today's cyber-secure,

data-rich environments. A robust IT/OT strategy should outline how to translate, transform, and integrate these devices into common data models. Technologies such as protocol-agnostic middleware—like an OT Message Bus (OTMB)—facilitate real-time, secure, and standardised communications without requiring each application to maintain its own integration layer. When direct upgrades are not feasible, utilities must weigh the costs of modernisation or refurbishment against the risks and inefficiencies of continued operation.

On the semantic front, ontologies are effective in harmonising meaning across domains. The Smart Applications Reference Ontology (SAREF), established by European Telecommunication Standards Institute (ETSI), offers a modular ontology for IoT devices. Its energy extension, SAREF4ENER, focuses on decentralised energy systems and smart homes, covering appliances, loads, distributed generators, and flexibility resources. Complementary approaches, like the Smart Energy Domain Ontology (SARGON) ontology, enhance building automation and energy systems by introducing reasoning support based on OWLlogic, along with smart metres, control schemes, and automation processes.

These standards and ontologies enable cross-domain data understanding. For example, both a smart building management system and a DER aggregator can publish flexibility data, such as demand reduction potential, in a format that a grid operator can understand without custom mappings. This makes it easier to incorporate grid-edge assets into central operations. By leveraging the strengths of CIM, CGMES, SAREF, and SARGON, utilities can develop systems that are interoperable at both the protocol and semantic levels. This dual approach reduces integration costs, breaks down data silos, and accelerates innovation in increasingly complex energy ecosystems. In the long term, interoperability and semantics will be crucial for building resilient, adaptive, and future-proof energy networks.

4.4 Cybersecurity

As energy systems become more digital and connected, cybersecurity is no longer an afterthought but a fundamental part of grid operations. Many OT systems were not designed to withstand today's threats, making them vulnerable as they integrate with IT, cloud, and AI-driven platforms. Real-world incidents, such as cyberattacks on power grids, have demonstrated how quickly disruptions can spread when security gaps are exploited. To safeguard future operations, utilities must move beyond perimeter defences and adopt strategies like zero trust, continuous monitoring, and preparing for emerging risks such as quantum computing. Security must be built into every layer of the system to verify that the grid remains resilient and trustworthy.



Evolving Threat Landscape

The dangers are no longer hypothetical. Disastrous events, like the Ukrainian blackouts caused by malware, highlight the reality of OT attacks in the physical world. Nation-states and cybercrime syndicates are continuously refining their methods to target critical infrastructure, as reported by ENISA. Emerging technologies such as AI and quantum computing will expand this challenge, serving both as powerful defence mechanisms and new offensive tools. In this context, relying solely on perimeter defences is no longer sufficient. Organisations must assume that attackers will penetrate their systems and focus on rapid detection, response, and resilience.



Zero Trust for OT

Zero Trust (ZT) is gaining traction in OT environments. The "never trust, always verify" principle is particularly relevant in infrastructure where implicit trust has been the norm. Instead of relying on traditional flat networks with perimeter firewalls, ZT enforces continuous authentication, rigorous access controls, and micro-segmentation to isolate assets. Trust is dynamic, re-evaluated at every stage, and revoked if abnormal behaviour is detected.

Implementing ZT requires careful planning to avoid disrupting high-priority processes. Over time, ZT best practises will become formalised, requiring continuous validation, least-privilege access, and identity-aware network controls.



Secure Communications and Post-Quantum Readiness

Encryption is essential in increasingly integrated OT systems. Legacy protocols often lack encryption, leaving OT environments particularly exposed. This vulnerability is compounded by the looming threat of quantum computing, which could break widely used cryptographic algorithms within the next decade, undermining secure communications and VPNs.

Given that OT assets often remain in service for decades, crypto-agility—the ability to upgrade encryption in the field—must be embedded in systems now. NIST and EU guidance set clear timelines: quantum-safe standards by 2030–2035, with hybrid cryptography (PQC + PKI) essential during the transition phase.



IT/OT Convergence and Cloud Adoption

The convergence of IT and OT brings significant benefits, including integrated data visibility, predictive analytics, and remote control across the grid. However, it also increases the risk of IT-originating attacks spreading to OT networks. Network segmentation and defensibility are crucial in this context. Unified IT/OT Security Operations Centers (SOCs) are emerging, with about 30% of organisations already adopting them, and this trend is expected to grow. Similarly, the adoption of cloud-hosted OT applications is increasing, requiring risk-aware uptake and secure architectural protection.



AI and Security Analytics

AI and machine learning are beginning to reshape OT security by processing vast amounts of telemetry, threat intelligence, and user behaviour to detect anomalies much faster than humanly possible. While adoption is currently limited (about 10% of companies implement AI tools, typically in pilot phases), maturity will grow. AI must be used responsibly, with clear objectives, robust governance, and thorough testing.

When implemented properly, AI enables a shift from reactive response to proactive prevention. New applications include predictive threat intelligence, digital twin-based anomaly detection and insider-threat prevention through behaviour monitoring.



Autonomous Response and Self-Healing

Cybersecurity in OT is evolving to emphasise resilience by design. Self-healing networks, AI-driven playbooks, and automated orchestration will allow systems to detect, diagnose, and respond to attacks with minimal human intervention. Deception technologies, such as honeypots, decoys, and simulated data streams, will also be increasingly deployed to mislead attackers, providing defenders with more time and reducing the impact of incidents.



Secure by Design and Cyber-Informed Engineering

The security model is shifting from bolting on controls to embedding them from the start. Secure by Design principles, as promoted by UK government frameworks, emphasise integrating security requirements into technology and procurement decisions at the earliest stage. This approach is complemented by Cyber-Informed Engineering (CIE), which integrates security into the engineering lifecycle, infusing risk analysis into requirements, design trade-offs, and safety assessments from the beginning.

As a result, there will be a growing demand for secure out-of-the-box products, lifecycle patching plans, and secure decommissioning processes.

4.5 Communication and Infrastructure

By 2035, energy systems will evolve beyond just physical assets like lines, transformers, and substations. They will become cyber-physical platforms where various distributed resources interact in real time, dynamically balancing supply and demand with security. For this future to be possible, communication must be treated as critical infrastructure, ensuring reliability, low latency, and scalability by design. Utilities are shifting from fragmented, serial, and circuit-switched networks (like IEC 60870-5-101, DNP3-Serial, TDM/SDH) to unified, IP-based standards such as IEC 60870-5-104 and IEC 61850 over Ethernet/MPLS. This common backbone allows substations, DERs, and supervisory systems to exchange information seamlessly, eliminating protocol silos and paving the way for advanced analytics, wide-area protection, and digital twins.

Fundamental Requirements

To turn this vision into reality, future communication infrastructures must meet several key requirements: performance, scalability, resilience, security, and interoperability. These are not just nice-to-have features; they are essential. Without them, even the most advanced technologies cannot deliver their intended value. Establishing these requirements sets the baseline for all technological choices.

Performance, Scalability and Resilience

Future communication infrastructures must be designed for the demands of a high-DER, high-data energy system. Latency is crucial: protection schemes need response times under 10 milliseconds, while monitoring and metering can handle latencies of a few seconds. Redundancy and self-healing mechanisms see to it that when nodes or links fail, traffic is automatically rerouted without compromising real-time performance. Handling massive telemetry streams and simultaneous device transmissions without bottlenecks or service degradation is equally important. To achieve this, architectures must be horizontally scalable and designed without single points of failure. Only then can deterministic performance be maintained in challenging operating conditions.

Interoperability Beyond Physical Connections

True interoperability is more than just physical connectivity. It requires compatibility at both technical and semantic levels. Technical standards like IEC 61850, OPC UA over Time-Sensitive Networking (TSN), and 5G Ultra-Reliable Low-Latency Communications (URLLC) profiles maintain reliable interaction between devices from different vendors. Semantic standards like the CIM and NGSI-LD ensure that information is interpreted consistently across organisations and platforms. Interoperability also depends on governance. Utilities must work with telecom operators, cloud hyperscalers, and regulators to establish service-level agreements, define priority policies for bandwidth allocation, and manage shared infrastructures. Without this alignment, technical advancements can be undermined by fragmentation and inconsistent practices.

Enabling Technologies

While requirements define the "what," technologies define the "how." The principles of latency sensitivity, redundancy, cybersecurity, and interoperability are brought to life through specific communication technologies. Fibre, TSN, mobile networks with edge computing, and software-defined control each address key aspects of these requirements. Together, they form the technological foundation of a communication network that is both future-proof and adaptable.

Fibre: The Backbone of a Digital Grid

Optical fibre is the go-to medium for mission-critical OT communication. Its high bandwidth, low and predictable latency, immunity to electromagnetic interference, and long-distance reach make it essential for real-time monitoring and protection. Applications like synchrophasor networks, sampled values, and digital substations rely on fibre to maintain consistent performance under all conditions. Beyond technical benefits, fibre offers long-term scalability and security, making it ideal for future data-intensive applications such as AI-driven analytics and high-resolution digital twins. While initial deployment costs can be high, the lifecycle economics of fibre are favourable, and hybrid strategies can help manage upfront investments.

Time-Sensitive Networking (TSN)

Fiber does not by itself guarantee deterministic performance, even though it offers the structural underpinnings for high bandwidth and low latency. Because standard Ethernet is non-deterministic, it cannot be used for automation and protection tasks that require responsiveness at the millisecond level. By improving Ethernet with bounded end-to-end latency, low jitter, and congestion-free forwarding, TSN fills this gap. This makes it possible for monitoring, control, and protection traffic to live peacefully on the same network. Process bus architectures that can reliably transmit IEC 61850 GOOSE messages and sampled values are made possible by TSN within substations. In the future, TSN will support coordinated microgrid operations and wide-area protection by lowering dependency on proprietary fieldbus technologies and enabling deterministic communication across dispersed assets. However, TSN is most appropriate for local domains like substations or microgrids because it functions at Layer 2 of the OSI model. By adding traffic engineering, resource reservation, and packet replication to achieve end-to-end guarantees over IP networks, the IETF's Deterministic Networking [42] framework expands on TSN principles to extend deterministic behaviour across Layer 3 routed environments. For future grid protection, distributed energy coordination, and cross-operator interoperability, TSN and DetNet work together to provide dependable, low-latency, and fault-tolerant communication across local and wide-area energy systems.

Mobile Networks, Edge, and Satellite

While fibre and TSN ensure deterministic performance in wired environments, they cannot reach every location economically. Mobile assets, remote substations, and dispersed IoT devices need connectivity

beyond the fibre footprint. Next-generation mobile networks (5G and 6G) bridge this gap by extending low-latency and high-reliability communication to the wireless domain. However, mobility alone isn't enough; the vast number of devices and the data they generate would overwhelm central systems if all processing were backhauled. Edge computing complements mobile networks by enabling local processing, rapid control actions, and continued operation even when wide-area links are degraded.

For extremely remote or offshore locations where terrestrial networks are unavailable, satellite communication solutions (e.g., Starlink, OneWeb) offer a viable alternative. Although latency is typically higher than fibre or 5G, modern low-earth-orbit constellations significantly reduce this gap, ensuring basic connectivity and resilience in otherwise unreachable areas.

Software-Defined Networking (SDN)

Fibre, TSN, and next-generation mobile networks with edge computing provide the essential building blocks of a future-proof communication fabric. However, without a unified control layer, these domains risk becoming isolated silos with inconsistent policies and limited flexibility. SDN provides this orchestration. By separating the control and data planes, SDN offers a centralised view of the network, enabling deterministic path configuration, dynamic traffic steering, automated failover, and QoS enforcement across different domains. It abstracts vendor-specific technologies and unifies them into a programmable environment. For utilities, this means network services can be provisioned, reconfigured, and secured dynamically, with minimal manual intervention. More importantly, SDN forms the programmable foundation for emerging technologies like AI-driven control, blockchain-enabled market platforms, and distributed optimisation.

The Road Ahead

These requirements and technologies will shape the future of energy by 2035, making communication the backbone of a fully digitalised and resilient system. Future communication systems will be modular, easily integrating new technologies without major redesigns. They will be software-defined, allowing for programmable, agile, and policy-driven operations. Additionally, they will be service-oriented, enabling on-

demand provisioning and dynamic scaling.

These systems will connect substations, field devices and the cloud, supporting federated data spaces, distributed control loops and AI-driven operational decisions. Communication will move from the background to the forefront, becoming the critical infrastructure that maintains the observability, coordination, and resilience of the entire energy value chain.

05

Recommendations & Strategic Directions

IT and OT modernisation is not just about new systems and technologies; it's a profound organisational transformation. This change affects decision-making, disrupts traditional roles, and demands a culture of agility, accountability, and resilience.



While technology choices are important, the true differentiator lies in how organisations govern, lead, and manage this change. Effective governance sees that investments align with business strategy, security needs, and regulatory compliance. Strong leadership is crucial for building momentum and overcoming resistance.

5.1 Governance and Leadership

Successful IT/OT transformation hinges on three key pillars: clear governance structures, strong leadership alignment and continuous responsibility with measurable progress. As IT and OT converge, roles such as instrumentation engineers, control system engineers, and IT network administrators are becoming more interconnected. Without clear governance, this overlap can lead to ambiguity, unmanaged risks, duplicated efforts, and overlooked critical tasks.

Leadership Sponsorship and Cross-Departmental Alignment

Successful transformation relies on active support from senior leadership, particularly at the C-suite level. These leaders play a crucial role in removing organisational barriers, scaling initiatives across the enterprise, and safeguarding long-term programmes from short-term pressures. By aligning leaders across departments, we establish collective accountability, ensuring that siloed priorities do not impede overall progress.

Creating Role Clarity: Cross-Company RACI

A draft RACI matrix (Responsible, Accountable, Consulted, Informed) should be part of the change programme. This matrix must be a cross-functional tool that spans IT, OT, engineering, and business functions. Importantly, it should not be static. As workflows and technology stacks evolve, the RACI matrix should be updated regularly—ideally every quarter—to align with new architectural and operational innovations. For example, the transition from unmanaged switches to managed Ethernet shifts responsibilities. Instrumentation engineers once replaced failed hardware, but now configuration management often falls under IT. Clear definitions are essential to avoid security vulnerabilities and performance issues.

Core Governance Bodies

To see to it that effective governance, two formal decision-making bodies are essential:

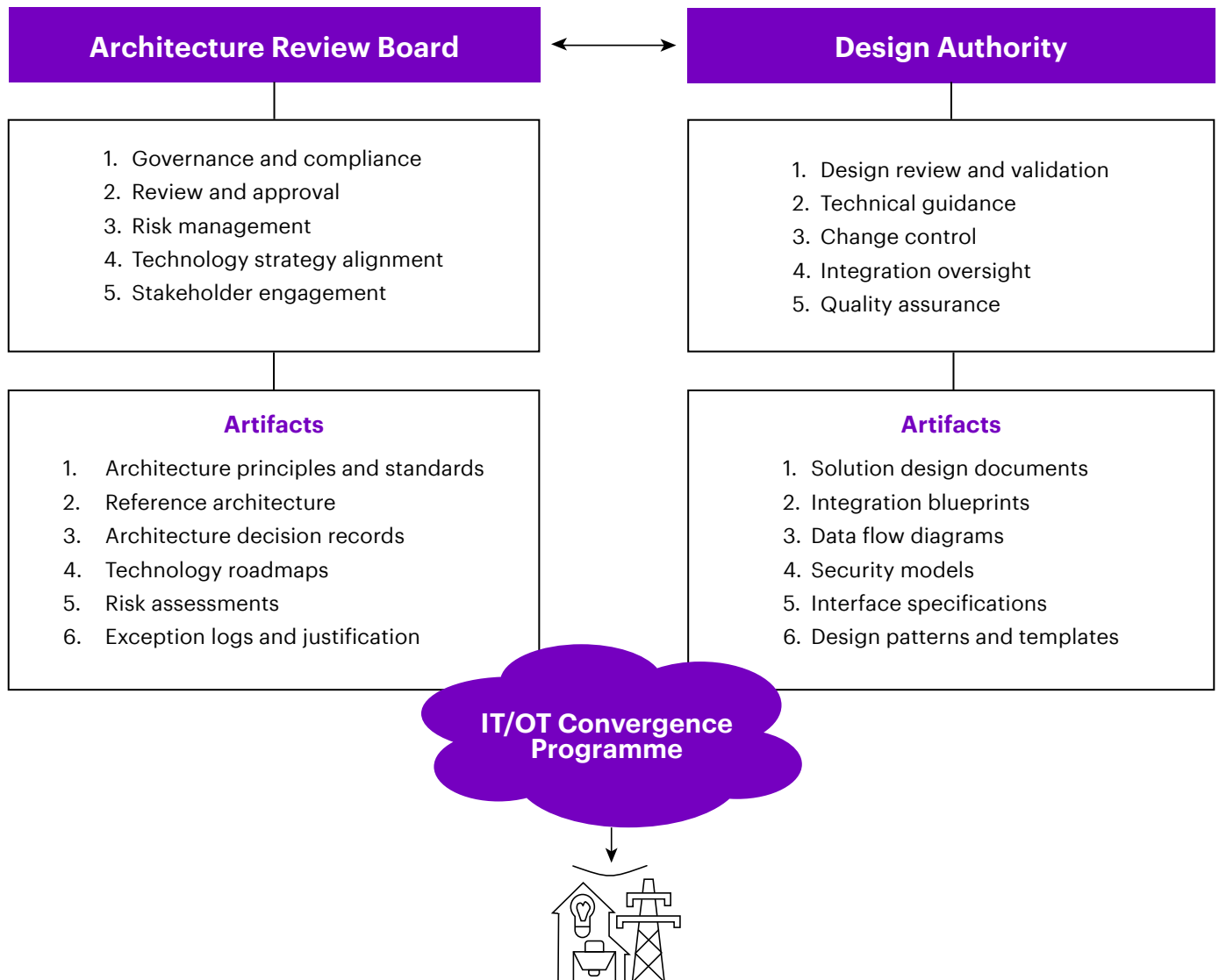
- **Architecture Review Board (ARB):**
The ARB is responsible for approving strategic architectural decisions, ensuring compliance with enterprise standards like TOGAF, cybersecurity frameworks, and regulatory requirements. Its duties include endorsing technology blueprints, defining principles, governing reference architectures and integration designs, and managing architectural risks to align with business goals and long-term resilience.
- **Design Authority (DA):**
The DA, reporting to the ARB, reviews and approves detailed solution designs. Its role is to ensure that solutions are technically sound, feasible, aligned with approved architectural principles, and delivered with strong integration oversight and quality assurance.

Decision-making in these bodies must be timely and efficient. Bureaucratic delays should be avoided, and resubmissions minimised. Shared software can help streamline this process. The following figure illustrates the decision-making functionalities.

Continuous Governance Maturity Assessment

Governance should be an ongoing process, not a one-time task. Regular capability and maturity reviews help identify gaps, drive continuous improvement, and maintain alignment with the long-term transformation vision. Quarterly reviews can track KPIs and governance performance, while annual strategic reviews should address evolving regulations, technologies, and market conditions. This keeps the change process both action-oriented and strategically relevant.

Figure 7: Function of decision-making bodies



5.2 Architecture Choices

The journey toward software-defined power system operations involves more than just adopting new technologies. It also requires making deliberate architecture choices that align with organisational goals, risk tolerance, and long-term sustainability. The examples below highlight some of the key architectural choices teams must navigate when designing complex systems.

Open-Source vs. Commercial Licensing

To determine the desired level of vendor independence while ensuring reliable support, consider the following options:

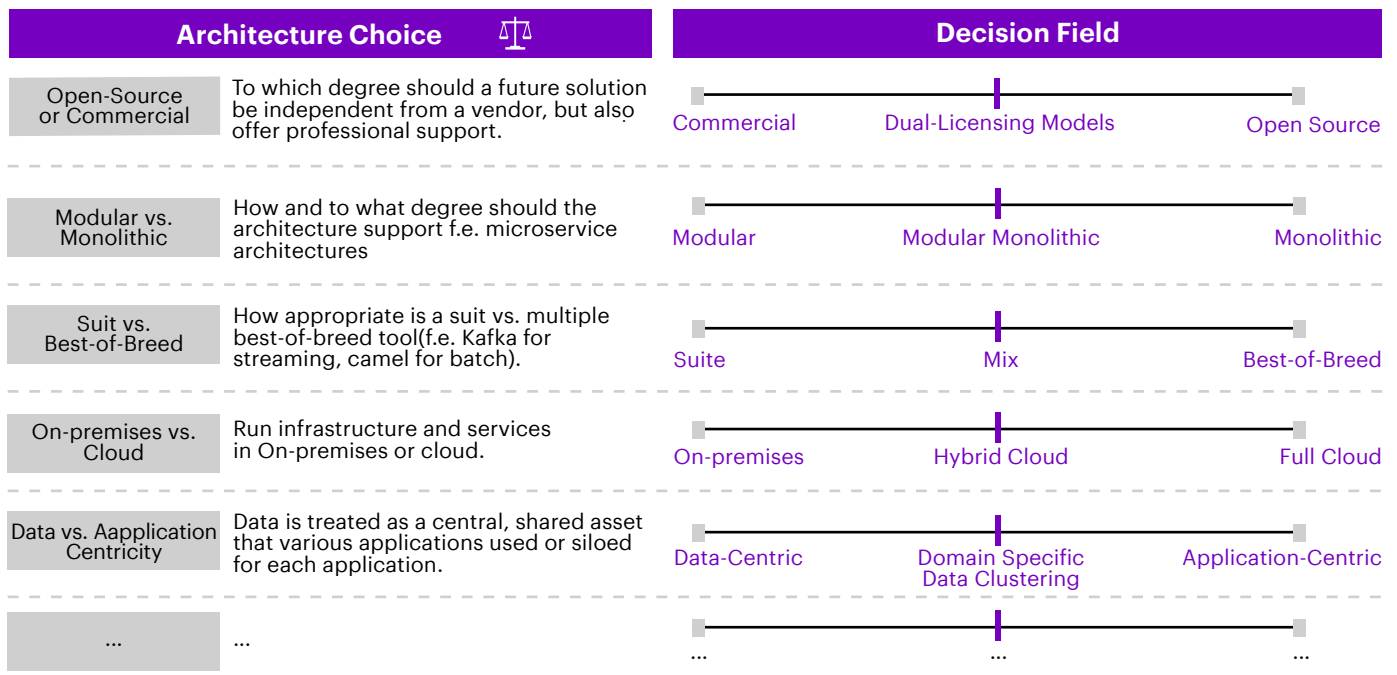
- **Commercial Solutions:** For mission-critical databases, like Microsoft SQL Server, choose

commercial options that offer 24/7 enterprise support.

- **Dual-Licensing Models:** Platforms like MongoDB provide flexibility with both open-source community editions and enterprise-grade features.
- **Open-Source Platforms:** For cost control and vendor independence, opt for open-source solutions like PostgreSQL.

The key is to balance licensing costs, support needs, vendor lock-in risks, and your team's internal expertise.

Fig 8: Architecture principles to further derive selection criteria and to narrow down Solution Options



Modular vs. Monolithic Architecture

When selecting a future architecture, evaluate the benefits of microservices versus consolidated deployments:

- **Modular Approach:**
Break down systems, such as an e-commerce platform, into separate services for user management, inventory, payment processing, and order fulfillment.
- **Modular Monolith:**
Create distinct modules within a single deployable unit, like separate packages for different business domain.
- **Monolithic Approach:**
For small teams that value simplicity, a fully monolithic system, like a content management system, might be the best choice.

Your final decision should consider team structure, deployment complexity, scalability needs, and operational overhead.

Suite vs. best-of-breed solutions

Weigh the advantages of a comprehensive suite against multiple specialised tools:

- **Suite approach:** Implement a suite like Microsoft 365 to cover productivity needs, including email, documents, collaboration and storage.

- **Mixed Strategy:**
Pair a CRM like Salesforce with specialised platforms such as HubSpot for marketing automation and Tableau for analytics.
- **Best-of-Breed Approach:**
Use Kafka for streaming, Elasticsearch for search, Redis for caching, and PostgreSQL for transactional data.

Consider factors like integration complexity, vendor relationships, total cost of ownership, and the need for specialised features.

Data vs. Application Centricity

Determine whether data should be managed as a centralised, shared asset or remain in application-specific silos:

- **Data-Centric Approach:** Use a common data lake with standardised APIs to enable unified data access for CRM, marketing, and support systems.
- **Domain-Specific Clustering:** Organise data into domains such as customer, product, or financial, allowing shared access within each domain while maintaining separation.
- **Application-Centric Approach:** Let each system, such as HR, inventory, or accounting, retain its own database with point-to-point integrations.

Your choice should align with governance requirements, integration complexity, performance demands, and your organisation's data maturity.

On-Premises vs. Cloud Infrastructure

Decide how much to rely on cloud environments versus company-controlled data centers:

- **On-Premises:** Offers complete control over hardware, networks and security but requires significant in-house expertise and resources.
- **Hybrid Cloud:** Balances control and flexibility by keeping sensitive data and legacy systems on-site while moving development and customer-facing applications to the public cloud.
- **Full Cloud Deployment:** Shifts the entire infrastructure to providers like AWS, Azure, or Google Cloud, leveraging native services for compute, storage, and databases.

The right choice depends on regulatory compliance, data sovereignty, operational expertise, cost efficiency, scalability, and disaster recovery needs.

Strategic Architecture Choices

Strategic architecture choices set the guardrails for implementing enabling technologies. Balancing these dimensions will shape the long-term flexibility, cost structure, and resilience of software-defined power system operations. Clear decision-making in these areas see to it that technology adoption aligns with your organisational strategy and operational requirements. These represent only a subset of architectural choices; many additional trade-offs must be evaluated based on context, priorities, and long-term strategy.

5.3 Talent and Skills

The energy sector is undergoing a digital transformation through the integration of IT, OT, and AI. This shift has created significant skill gaps that go beyond technical differences, extending to structural and cultural variations among these domains. Bridging these gaps is crucial for the successful deployment of scalable, secure, and intelligent grid systems using cloud, edge, and real-time technologies.

IT Domain Skill Gaps

While IT professionals excel in systems administration, cloud infrastructure, and cybersecurity, they often struggle in operational environments. Many lack familiarity with OT-specific protocols such as Modbus, DNP3, and IEC 61850, which are vital for SCADA systems and field-level communication. They also have limited experience with real-time, deterministic systems essential for power grid stability. Additionally, IT teams are often unfamiliar with industrial networking technologies, including fieldbus, industrial Ethernet, and the protection of legacy systems, where patching options are limited. Environmental and physical challenges in OT environments, such as extreme temperatures, dust, and restricted remote access, are also unfamiliar territory for IT teams.

OT Domain Skill Gaps

OT professionals, traditionally trained in instrumentation and physical systems, are now expected to adopt digital skills. Many have limited knowledge of modern software practices like CI/CD, DevOps, and programming languages such as Python. Their understanding of distributed and hybrid cloud/edge environments, including virtualisation, containerisation, and orchestration tools like Docker and Kubernetes, is often inadequate. Hands-on experience with AI/ML frameworks like TensorFlow or PyTorch is also limited, despite their importance for predictive maintenance and anomaly detection. Moreover, cybersecurity training is often insufficient, particularly in areas like intrusion detection, secure remote access, and managing threats in legacy or air-gapped systems.

AI Domain Skill Gaps

AI experts often lack the contextual understanding and deployment experience needed for the power sector's constrained operating environments. They may have limited knowledge of power system dynamics, fault modes, and operational constraints, making it difficult to adapt AI models to real grid requirements. They also often lack experience in deploying lightweight models on edge devices, which require strict latency, reliability, and power efficiency. Expertise in embedded systems programming and optimisation for resource-constrained, mission-critical platforms is frequently missing, hindering effective AI integration in field environments.

Cross-Domain and Organisational Gaps

Some skill challenges affect all domains, creating barriers to effective collaboration and integration. Specialists often remain in silos, lacking a shared language or awareness of how their systems and assumptions impact others, which hampers cooperation. A general weakness in systems thinking means that IT, OT, and AI interdependencies are not fully appreciated, leading to gaps in coordination and resilience. There is also limited knowledge of emerging interoperability standards like OPC UA, MQTT, or IEEE 2030.5, which are essential for future-ready architectures. Companies that rely on outdated platforms risk losing talent, as skilled professionals prefer working with cutting-edge technologies that support their long-term growth.

Organisational Realities

OT networking remains one of the most challenging skill areas, with responsibilities often unclear between OT and IT teams. Critical elements such as firewalls, managed switches, and border devices can be overlooked due to this ambiguity. To address this, teams must be intentionally cross-disciplinary, with clearly defined roles that encourage collaboration. Organisations must also decide strategically which technical functions to keep in-house and which to outsource, whether it be server administration, patching, AI design, or SCADA upgrades. Without a structured training plan, companies risk falling behind unless workforce knowledge is continually updated to keep pace with rapidly evolving technologies.

Closing the Skill Gaps

To bridge the skill gaps in IT, OT, and AI, a collaborative effort from industry consortia, academia, and organisations is essential. Here are some practical steps to reskill and upskill personnel:

- **Cross-functional Training Programmes:**
Organisations should create training programmes that introduce IT, OT, and AI professionals to each other's domains. For example, IT staff can attend workshops on OT standards like IEC 61850, while OT personnel can learn about cloud-native platforms such as Kubernetes. AI experts can participate in grid simulation exercises to gain

deeper insights into power system operations.

- **Certifications in Emerging Technologies:**
Industry-specific certifications, such as those from the International Society of Automation (ISA) or industrial cybersecurity training (e.g., IEC 62443), can enhance professionals' domain knowledge. AI experts should consider edge AI or real-time systems certifications to better align with OT requirements.
- **Hackathons and Innovation Labs:**
Cross-disciplinary hackathons can foster collaboration among IT, OT, and AI teams to tackle real-world challenges. For instance, a hackathon could focus on designing a predictive maintenance system for grid assets by integrating AI algorithms with SCADA data and OT protocols.
- **Collaboration with Academia:**
Partnering with universities and research centers can help develop customised curricula for IT/OT/AI convergence in both undergraduate and graduate programmes, as well as post-degree training.
- **On-the-job Training and Mentorship:**
Pairing IT or AI professionals with skilled OT personnel through mentorship programmes can facilitate knowledge transfer. OT engineers can mentor IT staff on the operational constraints of grid systems, while IT professionals can instruct OT personnel in software development practices.
- **Simulation-Based Learning:**
Providing access to simulation platforms or digital twins can help employees build hands-on expertise in integrated IT/OT/AI systems. For example, a digital twin of a smart grid can allow teams to test AI algorithms and cybersecurity measures in a controlled environment.
- **Utilising Open-Source Tools:**
Encouraging the use of open-source platforms like Grafana for monitoring and TensorFlow for machine learning can accelerate skill development. Professional-grade, foundation-governed projects, such as the LFE, can also speed up the adoption of new solutions and paradigms. Open-source tools often have thorough documentation and community support, making them ideal for upskilling.

5.4 Data and Intelligence

Maximizing the benefits of OT transformation relies on interoperable, secure, and valuable data. To achieve this, robust data governance, trusted data-sharing models, and a continuously evolving data strategy are essential, keeping pace with regulatory and technological advancements.

Data governance begins with defining clear roles and standards across the organisation to ensure data quality, integrity, and consistency. Poor data quality can undermine analytics and AI effectiveness. Standardizing OT data is crucial; systems using poorly formatted or uncontextualised data will underperform or fail.

Data spaces are gaining attention for secure and trustworthy data exchange. These federated platforms support sovereign data sharing under predefined rules. In Europe, the Common European Energy Data Space (CEEDS) is being implemented under the Data Governance Act and Data Act to facilitate data sharing among TSOs, DSOs, aggregators, and third parties. Programmes like Gaia-X, Energy Data-X and the INSIEME project are bringing these concepts to life by integrating national and regional energy

platforms. The Data Spaces Business Alliance (DSBA) provides technology and governance roadmaps, including standards, identity systems, and trust frameworks, to ensure secure multi-party data spaces. These efforts help avoid dependency on hyperscale cloud providers and create a cloud-to-edge "digital spine" for AI-driven orchestration, digital twins, and real-time grid operations.

AI use in operational data must be cautious and governed strictly. High-risk AI systems, such as DERMS, grid controls, and trading, are subject to extensive oversight, including explainability, data quality, human-in-the-loop mechanisms, and post-market surveillance. Organisations must understand the data lifecycle in AI pipelines, from storage to processing, to prevent sensitive infrastructure data from being exposed to risks. The data strategy should be dynamic, regularly refreshed to align with rapid innovation and regulatory changes. As circumstances evolve, so should the organisation's approach to data sharing, protection, and intelligence, with trust, interoperability, and agility at its core.

5.5 Ten Quick-Start Actions for Accelerating IT/OT Transformation



Craft an IT/OT Strategy:

Develop a cross-functional plan that aligns technical modernisation with business goals. Assess legacy systems, plan for their retirement and adopt open standards for long-term flexibility



Establish Governance Structures:

Form a joint OT/IT task force to define decision-making roles, responsibilities, and best practices from day one.



Bridge Business and Technology:

Organise formal workshops to bring together business, IT, OT, and engineering teams. Collaborate to create a high-value use case backlog for digital initiatives.



Implement Interoperability Standards:

Map system information and adopt models like CIM or SAREF to have seamless data sharing between devices, platforms, and stakeholders.



Revamp Communications Infrastructure:

Overhaul networks with flexible, future-proof technologies such as IP-based solutions, optics, and secure 5G channels.



Fortify Cybersecurity:

Create an integrated cybersecurity task force to implement zero-trust architectures, real-time threat detection, and continuous assessments throughout the OT lifecycle.



Evolve the Workforce:

Update job profiles, reskill at-risk positions, and partner with academic or training institutions to maintain expertise in OT, AI, and automation.



Prepare for AI Integration:

Develop an operating model that incorporates Responsible AI principles in governance, monitoring, and change management before full-scale AI deployment.



Build Simulation & Testbed Infrastructure:

Set up simulation twin infrastructure to test and validate new solutions in a controlled environment before real-world implementation.



Ensure Ongoing Alignment:

Make all processes iterative, regularly revisiting them during maturity reviews to keep transformation aligned with long-term vision.

By implementing these quick-start actions, organisations can effectively address the identified gaps and accelerate their IT/OT transformation. These steps not only build initial momentum but also uphold a solid foundation for future growth.

References

- [1] European Commission, “Fit for 55: Delivering the EU’s 2030 Climate Target on the way to Climate Neutrality,” COM(2021) 550 final, European Commission, Brussels, Jul. 2021.
- [2] ENISA, “NIS2 Technical Implementation Guidance,” European Union Agency for Cybersecurity (ENISA), Jun. 26, 2025.
- [3] DataM Intelligence 4Market Research LLP, “Europe Electrical Digital Twin Market – 2025-2033,” Europe Electrical Digital Twin Market, 180 pp., Apr. 2025.
- [4] IMARC Group, “Europe Edge Computing Market Size & Outlook, 2024–2033,” IMARC Group, Jan. 2025.
- [5] Business Research Insights, “DERs Market Size, Share, Growth, and Industry Analysis, By Type (Wind DERs & PV DERs), By Application (Commercial, Residential & Others), Regional Insights and Forecast From 2025 To 2033,” Business Research Insights, Jun. 2, 2025.
- [6] IEA (2022), Unlocking the Potential of DERs, IEA, Paris
- [7] Mordor Intelligence, Germany OT Security Market Size, Share, Insights & Strategy Forecast (2026–2033).
- [8] European Commission, “A European Strategy for Data,” European Commission, Brussels, Feb. 2020.
- [9] European Union Agency for Cybersecurity (ENISA), “Threat Landscape for the Energy Sector,” ENISA, Jul. 2021.
- [10] European Commission, “Cybersecurity of Energy Systems,” European Commission, Brussels, Oct. 2023.
- [11] S. M. Halbrügge, Accelerating Sustainability in Electricity Systems through digitalisation: Coping with Complexity in Times of Transition, Ph.D. dissertation, Faculty of Law and Economics, University of Bayreuth, Bayreuth, Germany, Oct. 2023.
- [12] M. Uslar, C. Dänekas, and J. Förster, “Future SCADA challenges and the promising solution: the agent-based SCADA,” Energy Informatics, vol. 2, no. 1, pp. 1–10, 2019.
- [13] International Electrotechnical Commission (IEC), Smart Grid Standards – IEC 61970/61968 CIM, IEC, 2020.
- [14] ENTSO-E, Common Grid Model Exchange Standard (CGMES) Implementation Guide, European Network of Transmission System Operators for Electricity, 2021.
- [15] CEN-CENELEC-ETSI Smart Grid Coordination Group, Smart Grid Reference Architecture (SGAM), Final Technical Report under Mandate M/490. Technical Report, 2012.
- [16] CEN-CENELEC-ETSI Smart Grid Coordination Group, SGAM User Manual. Technical Report, 2014.
- [17] DIN, DIN SPEC 91345:2016-04: Reference Architecture Model Industrie 4.0 (RAMI4.0), Technical Rule, Apr. 2016.
- [18] European Commission, European Energy Data Exchange Reference Architecture 2.0 (DERA 2.0), BRIDGE Report, 2023.
- [19] J.P. Hauet, P. Bock, R. Foley, and R. Françoise, “Ukrainian power grids cyberattack,” InTech, International Society of Automation, Mar.–Apr. 2017.
- [20] European Union Agency for Cybersecurity (ENISA), Cybersecurity Threats for 2030 – Update 2024 – Executive Summary, ENISA, Nov. 2024.
- [21] North American Electric Reliability Corporation (NERC), Zero Trust Security for Electric Operations Technology, White Paper, Jun. 2023.
- [22] Cybersecurity and Infrastructure Security Agency (CISA), Post-Quantum Considerations for Operational Technology, CISA, Oct. 2024.
- [23] Rockwell Automation, “OT Cybersecurity in 2025: 6 Trends to Watch,” Rockwell Automation Blog, Feb. 7, 2025.
- [24] UK National Cyber Security Centre (NCSC), Cloud-hosted SCADA, NCSC, 2024.
- [25] D. Parsons, “ICS/OT Cybersecurity & AI: Considerations for Now and the Future (Part I),”

SANS Institute Blog, May 28, 2024.

[26] Rockwell Automation, "Cyber-Security Trends 2025," Rockwell Automation Blog, Feb. 7, 2025.

[27] Frenos, Continuous OT Security Posture Management (OT-SPM) Platform, Frenos Inc., 2025.

[28] UK Government, Secure by Design, Gov.uk, 2024.

[29] Idaho National Laboratory (INL), Cyber-Informed Engineering (CIE). Idaho Falls, ID: INL, 2025.

[30] Y. Wang, C.-F. Chen, P.-Y. Kong, H. Li and Q. Wen, "A Cyber-Physical-Social Perspective on Future Smart Distribution Systems," *Proceedings of the IEEE*, vol. 111, no. 7, pp. 694-724, July 2023, doi: 10.1109/JPROC.2022.3192535.

[31] T. Sauter and M. Lobashov, "End-to-End Communication Architecture for Smart Grids," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 4, pp. 1218-1228, April 2011, doi: 10.1109/TIE.2010.2070771.

[32] M. F. Rafy, A. K. Srivastava, F. Neto and J. Biasi, "Communication Technologies for DER-Centric Power Distribution Systems: A Comparative Analysis and Cyber-Resilience Guidelines," *IEEE Access*, vol. 12, pp. 80549-80558, 2024, doi: 10.1109/ACCESS.2024.3408164.

[33] International Electrotechnical Commission, "Communication networks and systems for power utility automation – Part 90-13: Deterministic networking technologies," IEC TR 61850-90-13, Feb. 2021.

[34] Ø. Toftegaard, G. Grøtterud and B. Hämmerli, "OT resilience in the 2023 draft delegated act on cybersecurity for the power sector - An EU policy process analysis," *Computer Law & Security Review*, vol. 54, 2024, Art. no. 105952, doi: 10.1016/j.clsr.2024.105952.

[35] H. He et al., "Integrated Sensing and Communication in an Optical Fibre," *Light: Science & Applications*, vol. 12, no. 25, pp. 1-13, Jan. 2023, doi: 10.1038/s41377-022-01067-1.

[36] R. Salazar et al., "Utility Applications of Time Sensitive Networking White Paper," Technical Report, 2018.

[37] X. Fang et al., "5G Embraces Satellites for 6G Ubiquitous IoT: Basic Models for Integrated Satellite Terrestrial Networks," *IEEE Internet of Things Journal*, vol. 8, no. 18, pp. 14399-14417, Sept. 2021, doi: 10.1109/JIOT.2021.3068596.

[38] B. P. Rimal, D. P. Van and M. Maier, "Mobile Edge Computing Empowered Fibre-Wireless Access Networks in the 5G Era," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 56-62, Feb. 2017, doi: 10.1109/MCOM.2017.1600329.

[39] W. Velasquez, G. Z. Moreira-Moreira and M. S. Alvarez-Alvarado, "Smart Grids Empowered by Software-Defined Network: A Comprehensive Review of Advancements and Challenges," *IEEE Access*, vol. 12, pp. 69601-69620, 2024, doi: 10.1109/ACCESS.2024.3396402.

[40] García Castro, R., Lefrançois, M., Poveda Villalón, M., & Daniele, L. (2023). The ETSI SAREF ontology for smart applications: a long path of development and evolution. *Energy Smart Appliances: Applications, Methodologies, and Challenges*, 183-215.

[41] M. Haghighi, I. Sychev, A. Monti, and F. H. P. Fitzek, "SARGON – Smart energy domain ontology," *IET Smart Cities*, 28-Oct-2020.

[42] E. Grossman, "Deterministic Networking Use Cases," RFC 8578, Internet Engineering Task Force (IETF), May 2019.

Lead Authors

Varshitha Chamanahalli Ramanna

Gary Boyle

Nirvana Husadzic

Christian Hille

Advisors

Accenture

Frank Rütten

Gareth Seglenieks

Hamdi Shishtawi

Jannis Kahlen

Maximilian Dietrich

Philip Hinkel

Phil Scott

Paul Gilroy

Rohit Duggal

Shri Kasivajjula

Tim Montag

Fraunhofer FIT

Antonello Monti

Antigona Selimaj

Ahmed Abdelgawad

Beyza Cizmeci

Charukeshi Mayuresh Joglekar

Michael Andres

Nikolaus Wirtz

Pranav Jayant Kulkarni

About Accenture

Accenture is a leading solutions and global professional services company that helps the world's leading enterprises reinvent by building their digital core and unleashing the power of AI to create value at speed across the enterprise, bringing together the talent of our approximately 779,000 people, our proprietary assets and platforms, and deep ecosystem relationships. Our strategy is to be the reinvention partner of choice for our clients and to be the most AI-enabled, client-focused, great place to work in the world. Through our Reinvention Services we bring together our capabilities across strategy, consulting, technology, operations, Song and Industry X with our deep industry expertise to create and deliver solutions and services for our clients. Our purpose is to deliver on the promise of technology and human ingenuity, and we measure our success by the 360° value we create for all our stakeholders.

Visit us at **[accenture.com](https://www.accenture.com)**.

About Fraunhofer FIT

As a partner for digitisation, Industry 4.0 and the Internet of Things, the Fraunhofer Institute for Applied Information Technology FIT has been developing IT solutions tailored to people and seamlessly integrated into business processes for 40 years. As a driving force of innovation, FIT not only provides guidance, but also shapes the digital transformation in business, the environment and society.

FIT's interdisciplinary R&D teams are drawn from our staff of around 400 scientists from computer science, social science, business administration, economics, psychology, and engineering. They bring their expertise in designing and implementing information technology systems to bear on problems and needs from different areas of life.

Our specific strength is our holistic approach to system development – from concept validation to implementation. We strategically evolve our expertise in IT, specific application fields, and our scientific excellence with the aim to be ahead of the market for our customers from industry and administration. We focus on four application domains: Digital Energy, Digital Health, Digital Sustainability and Digital Business – each of outstanding importance for Europe's future.

Link: **www.fit.fraunhofer.de**

Copyright notice (e.g., "Copyright © 2025 Accenture. All rights reserved.")

Trademark disclaimer (e.g., "This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership by Accenture and is not intended to represent or imply association.")

General guidance disclaimer (e.g., "This document is produced by consultants at Accenture as general guidance. It is not intended to provide specific advice on your circumstances. If you require advice or further details on any matters referred to, please contact your Accenture or [Fraunhofer] representatives")