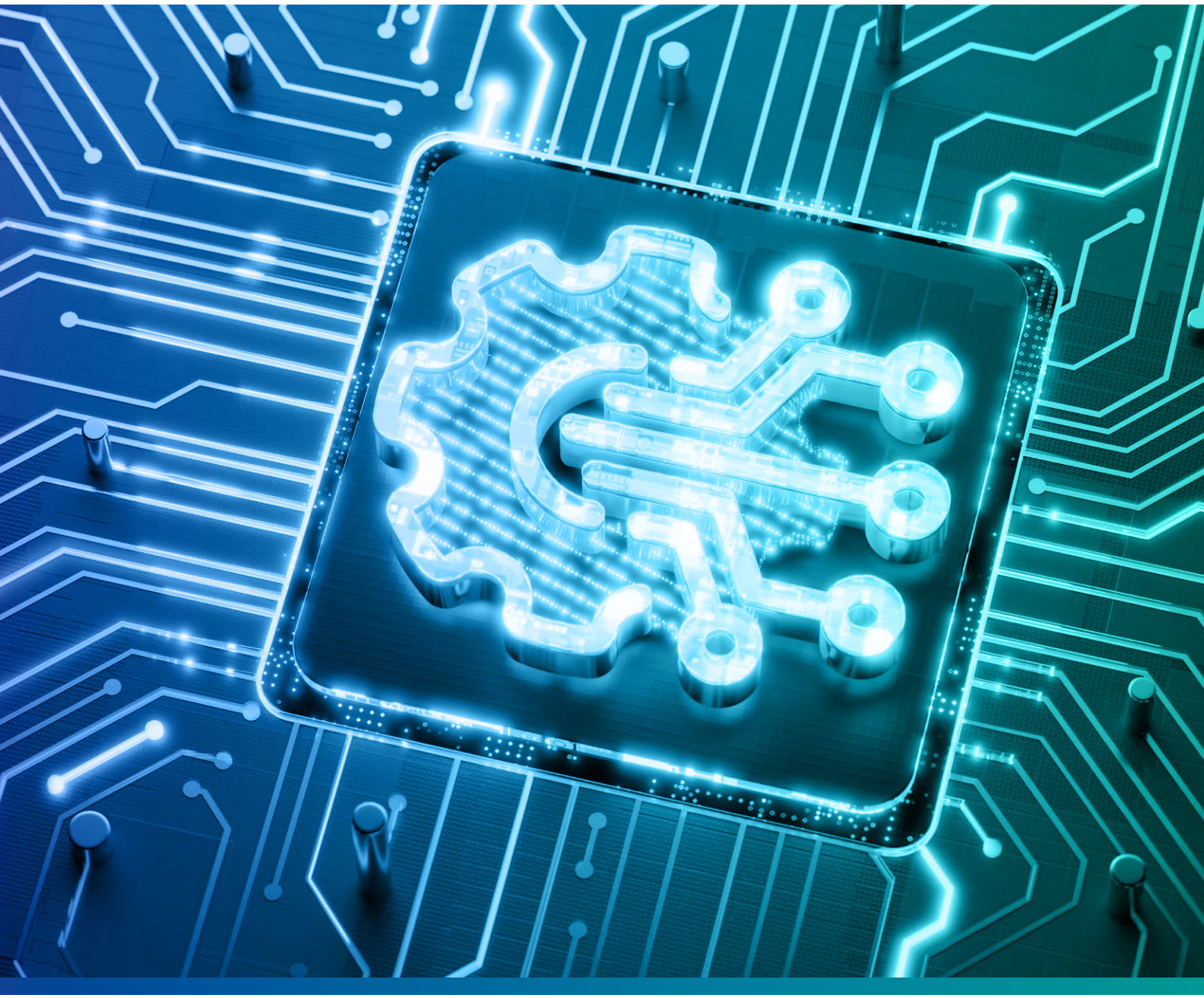
ENTSO-E Position Paper

Vendor Agnostic Solutions for Next-Generation Control Room Eco-Systems

May 2025



entsoe

ENTSO-E Mission Statement

Who we are

ENTSO-E, the European Network of Transmission System Operators for Electricity, is the **association for the cooperation of the European transmission system operators (TSOs)**. The **40 member TSOs**, representing 36 countries, are responsible for the **secure and coordinated operation** of Europe's electricity system, the largest interconnected electrical grid in the world. In addition to its core, historical role in technical cooperation, ENTSO-E is also the common voice of TSOs.

ENTSO-E **brings together the unique expertise of TSOs for the benefit of European citizens** by keeping the lights on, enabling the energy transition, and promoting the completion and optimal functioning of the internal electricity market, including via the fulfilment of the mandates given to ENTSO-E based on EU legislation.

Our mission

ENTSO-E and its members, as the European TSO community, fulfil a common mission: Ensuring the **security of the interconnected power system in all time frames at pan-European level** and the **optimal functioning and development of the European interconnected electricity markets**, while enabling the integration of electricity generated from renewable energy sources and of emerging technologies.

Our vision

ENTSO-E plays a central role in enabling Europe to become the first **climate-neutral continent by 2050** by creating a system that is secure, sustainable and affordable, and that integrates the expected amount of renewable energy, thereby offering an essential contribution to the European Green Deal. This endeavour requires **sector integration** and close cooperation among all actors.

Europe is moving towards a sustainable, digitalised, integrated and electrified energy system with a combination of centralised and distributed resources.

ENTSO-E acts to ensure that this energy system **keeps consumers at its centre** and is operated and developed with **climate objectives** and **social welfare** in mind.

ENTSO-E is committed to using its unique expertise and system-wide view – supported by a responsibility to maintain the system's security – to deliver a comprehensive roadmap of how a climate-neutral Europe looks.

Our values

ENTSO-E acts in **solidarity** as a community of TSOs united by a shared **responsibility**.

As the professional association of independent and neutral regulated entities acting under a clear legal mandate, ENTSO-E serves the interests of society by **optimising social welfare** in its dimensions of safety, economy, environment and performance.

ENTSO-E is committed to working with the highest technical rigour as well as developing sustainable and **innovative responses to prepare for the future** and overcoming the challenges of keeping the power system secure in a climate-neutral Europe. In all its activities, ENTSO-E acts with **transparency** and in a trustworthy dialogue with legislative and regulatory decision makers and stakeholders.

Our contributions

ENTSO-E supports the cooperation among its members at European and regional levels. Over the past decades, TSOs have undertaken initiatives to increase their cooperation in network planning, operation and market integration, thereby successfully contributing to meeting EU climate and energy targets.

To carry out its **legally mandated tasks**, ENTSO-E's key responsibilities include the following:

- Development and implementation of standards, Network Codes, platforms and tools to ensure secure system and market operation as well as integration of renewable energy;
- Assessment of the adequacy of the system in different timeframes;
- Coordination of the planning and development of infrastructures at the European level (**Ten-Year Network Development Plans, TYNDPs**);
- Coordination of research, development and innovation activities of TSOs;
- Development of platforms to enable the transparent sharing of data with market participants.

ENTSO-E supports its members in the **implementation and monitoring** of the agreed common rules.

ENTSO-E is the common voice of European TSOs and provides expert contributions and a constructive view to energy debates to support policymakers in making informed decisions.

Contents

Executive Summary

The vendor agnostic system (VAS) task force is a group of modern, forward-thinking transmission systems operators (TSOs), organised through the European Network of Transmission System Operators for Electricity (ENTSO-E) that recognise the need to move beyond existing tools, addressing their dependencies and missing functions.

TSOs have reached an inflexion point, where grid operation requirements and the capabilities of supervisory control and data acquisition (SCADA)/ energy management system (EMS) have surpassed the capabilities of traditional vendors. Power systems are also becoming increasingly complex, requiring control centre systems to become more advanced and capable of changing more rapidly.

The new eco-system includes everything a TSO needs to operate the electricity grid, including existing legacy systems, current or future expansions in real time or pre-real time, and planning and ex post capabilities. Emerging challenges, such as new grid technologies (photovoltaics, wind, HVDC, microgrids, storage) among other requirements, require adjustments and flexibility in control centre systems.

Therefore, pan-European grid security processes must leverage digitalisation and automation to cope with cyber threats. This requires developing customised enhancements to ensure resilient functionalities to effectively monitor, protect and control the power system.

The responsibilities of TSOs are growing, leading to changes in their profiles as new roles, mindsets and new ways of working arise and must be addressed. No single provider can provide all the required functionalities in sufficient quality and update systems at the required speed. Historically, SCADA/ EMS were all-in-one, non-modular solutions. Each comes with its own operator interface, central communication architecture and databases, which are locked and solely driven by single vendors.

The VAS task force has identified the following core tenets for a new modular eco-system:

I. Transparency

The new eco-system aims to secure transparency for the TSO community, potential providers and even distribution system operators (DSOs).

II. Modularity

The new eco-system shall be modular, with implemented services that are vendor-independent and, ideally, provider-interoperable.

III. Standardisation

The new ecosystem encompasses several domain areas and aspects that will need to be described and standardised for integration, operation and other relevant processes.

IV. Integration

- **The new eco-system must be integrable with and/or connected to existing systems, notwithstanding potential upgrades and/or updates to the existing systems.**
- **The new eco-system shall be agnostic towards underlying infrastructure like private cloud, public cloud or on-premise, as long as technology requirements are fulfilled and scalability is secured.**

V. Digital and Cyber Resilience

- **The new eco-system, its modules and its operation shall be resilient by design, applying zero-trust principles. Information and processes must have a high level of integrity, identifiable entities and verifiable and secure information exchange on and into the eco-system platform.**

VI. Separation of Concerns

- **The new eco-system shall have "separation of concerns" as a guiding principle of its architecture.**

VII. New Ways of Working

- **The new eco-system is not limited to software; it also includes development, operation and maintenance models.**
- **The new eco-system will require a legal framework to support its implementation.**
- **The new eco-system can accommodate a combination of parts/modules that are open-source, proprietary and/or commercial.**
- **The new eco-system will embrace a new collaboration with providers and facilitate new market models.**

According to the ENTSO-E RDI Roadmap 2024–2034, one of the missions of the TSO community is to enhance control and interoperability through digitalisation. Vendor-agnostic modules and tools for system control applications will improve the management of increasing grid complexity, enabling more coordinated and efficient system operations. Furthermore, future control centres will feature additional functionalities.

This position paper is structured to provide an overview of the core tenets behind next-generation modular systems for control centres. The paper will be continuously expanded through the addition of appendices elaborating on topics such as architectural details and recommended standards. Additionally, the VAS task force has developed a list of follow-up activities to undertake in working towards an open eco-system.

Elaboration of the Tenets

I. Transparency

"The new eco-system aims to secure transparency for the TSO community, potential providers and even DSOs."

The concept of transparency varies depending on the context and discipline in which it is used. In organisations, transparency is a commonly used term to prevent siloing. However, it also carries a deeper meaning – making information visible to others – and is commonly referred to as the act of "being open". Transparency is a multifaceted concept that is also widely used in software engineering.[1,2]

In software development, transparency involves establishing agreed-upon communication channels to ensure all parties are involved in decision-making processes regarding:

- Software design
- Architecture
- Technologies used
- Project structure
- Feedback included in the software development and life cycle

Consequently, transparency empowers all stakeholders to voice their opinions, fostering more creative solutions through collective problem-solving and decision-making. Making information equally accessible to all stakeholders reduces barriers to entry for collaboration.

In software development, transparency has been conceptualised in terms of information or process disclosure.[3] Information transparency means making information about software transparent. This includes software artefacts such as requirement documents, design documents and (optionally) code alongside commercial products. Software transparency also refers to the need for buyers or users to conduct code security and quality scanning and verification.

We respect the intellectual property (IP) rights of all provided software. We aim to identify and propose solutions that allow operators to maintain operations while performing necessary patching whenever required.

Process transparency, on the other hand, refers to the software's ability to reveal how it works, what it does and how it does it. This can be categorised into automated (i. e. software) and unautomated (i. e. organisational or business operation) processes. Distinguishing between the two requires defining corresponding factors to measure transparency.

More than 100 definitions of transparency factors exist in the literature, with measures of information and process transparency defined as follows:

- Information transparency:
  - **Accessibility** – Degree to which stakeholders can obtain information they consider necessary
  - **Usefulness** – Enables stakeholders to make decisions and take action based on the information provided
  - **Availability** – Information providers must disclose relevant data to the information receivers
  - **Interpretation** – The provided information must be clear and easily usable by the receivers
  - **Clarity** – The information provided to stakeholders must support effective decision-making based on data quality, accuracy, relevance and comprehensibility
- Processes transparency: Defines how processes are performed in the context of transparency

1 Yu-Cheng Tu, *Transparency in Software Engineering*, University of Auckland (2014).

2 P. Ofem, B. Isong and F. Lugayizi, "On the Concept of Transparency: A Systematic Literature Review," *IEEE Access*, vol. 10, pp. 89887–89914, 2022, doi: 10.1109/ACCESS.2022.3200487.

3 J. C. S. D. P. Leite and C. Cappelli, "Software transparency," Bus. Inf. Syst. Eng., vol. 2, no. 3, pp. 127–139, Jun. 2010

Within the TSO community, additional layers must be taken into account:

- Processes transparency is based on:
  - European Commission Regulation (EU) 2017/1485 of 2 August 2017, establishing a guideline on electricity transmission system operation
  - ACER methodology for coordinating operational security analysis in accordance with Article 75 of Commission Regulation (EU) 2017/1485 of 2 August 2017, establishing a guideline on electricity transmission system operation
- Information transparency is based on:
  - Regulation (EU) No 5 43/2013 of 14 June 2013 on the submission and publication of data in electricity markets

The overall goal is to develop a framework for transparent cooperation among TSOs for solutions in control centre ecosystems that will align with TSO governance to:

- Enhance data exchange via standardised interfaces
- Support transparent information sharing to ensure accessibility and usefulness of software requirements, design and documentation
- Support cooperation among TSOs on the design and deployment of new ecosystem architecture
- Facilitate new business models to share software and/or modules among TSOs
- Improve knowledge sharing of business capabilities and processes, e. g. operating security standards (OSS) stemming from common European regulations.

The purpose of the transparency framework envisioned by WG5 TF VAS is to promote the idea of transparent information, processes and software sharing within the TSO community, with the ultimate goal of sharing this vision with software providers.

II. Modularity

"The new eco-system shall be modular, with implemented services that are vendor-independent and, ideally, provider-interoperable."

Modularity is a principle of system design describing the degree to which a system's components can be separated and recombined. Modular architecture refers to a system made of separate components (modules) that are connected but not dependent on each other. A software module is a deployable, manageable, natively reusable, composable, stateless unit of software that provides a concise interface to consumers. The overall objective is to develop a framework for modules in control centre eco-systems that align with TSO governance.

The modularity description in this document addresses all layers from a business perspective, including business capabilities. This, however, requires that the data products be standardised.

The aim of the modularity description is to share the concept within the TSO community and promote the benefits of a modular approach, particularly when modules are positioned next to each other, overlapping or built on one another.

A modular control room eco-system aims to:

- Unlock the potential of growing operational and non-operational data
- Enable the use of event-based and streaming technologies in designing new applications
- Facilitate seamless information exchange via standardised interfaces
- Enable unrestricted flexibility for maintainability and further functional improvements

In terms of architecture frameworks, like TOGAF®, modularity is addressed in several layers to maintain a holistic view:

- Business architecture (business view)
- Data architecture (data structure)
- Application architecture (tool landscape)
- Technology architecture (IT-technology)

High-level architectural principles for new modules:

- Modules shall be as reusable as possible.
- Modules shall be configurable to accommodate the varying requirements of different TSOs.
- Modules shall work with well-defined input and output data products.
- Modules shall facilitate the separation of concerns principle by encapsulating their functionality and data.
- Modules shall have a clear purpose specific to a business or enabler capability.
- Modules shall be independently deployable and operable.
- Modules may have logical relationships, but no technical dependencies on each other.
- Modules shall be independent of the runtime environment/container.
- Modules shall be externally configurable (e.g. external master data).
- Modules shall expose all the relevant data via common interface standards.
- Module health and processes shall be observable via interfaces.

Modular Contract

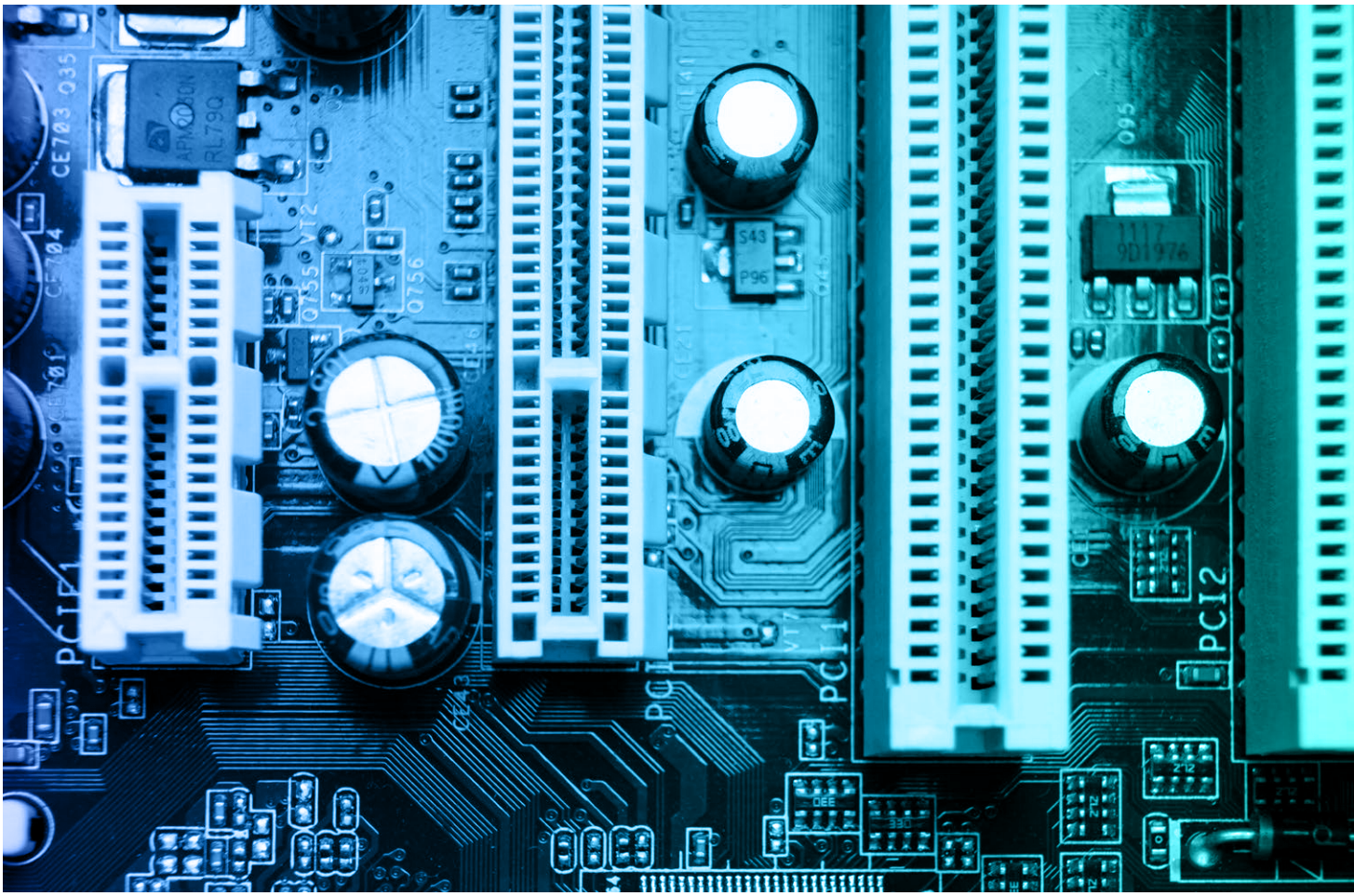
To enable modularity from a practical perspective, documentation must be created to define the terms, expectations and responsibilities between the parties involved in using or providing a module. A modular contract is the interface description for a module, its capabilities and how it will be used. Modular contracts, when standardised across providers and TSOs, enable plug-and-play functionality, which allows quick turnover times for replacing or upgrading modules.

Each module will have a modular contract with both the application platform and the technology platform to which it connects. A modular contract includes the definition of the interfaces, data requirements, application platform services and technology platform services required to run in a standardised format. This standard format will be set by an open, international industry standard.

A modular contract includes but is not limited to:

- Designated capability
- Module function
- Definition of interfaces
- Dependencies on other modules
- Input data requirements
- Output data specifications
- Application platform services
- Technology platform services
- Version
- Support plan
- Support level availability

Each of these criteria will have non-functional requirements as part of a full modular contract. Additionally, each of these characteristics will be described in more detail in further work.



III. Standardisation

"The new ecosystem encompasses several domain areas and aspects that will need to be described and standardised for integration, operation and other relevant processes."

Larger utilities, including TSOs and large DSOs, typically must comply with various externally imposed standards (CEN/CENELEC/ETSI, ISO/IEC/ITU, other international standards,[4] EU utility directives, ENTSO-E standards, etc.) to ensure interoperability, reliability and efficiency in managing the transmission grid. When operating outside these cooperative and regulatory standards, TSOs must consider which standards to use when building their eco-system. The task force recommends the use of established international, open and – if no other standards are available – industry standards as a first priority, followed by commonly agreed standards.

The task force has identified several specific domains where standards are necessary for a modular eco-system to function:

- **Internal interface standards:** Internal interface standards define the communication protocols and data exchange formats that enable different modules or components within a modular control system to interact with each other. These interfaces allow for seamless interaction between various elements, such as operator workstations, EMS and SCADA systems.

- **Interfaces between modules and application platform:** These standards define how the different modules (such as monitoring systems, analytics or control modules) interface with the application platform. It is imperative that these standards be open to third-party providers, enabling them to integrate their solutions or services. Open interfaces promote flexibility and innovation, allowing external developers to contribute new functionalities to the system.

- **External interface standards:** External interface standards specify the protocols and data formats used to exchange information between the TSO's modular control system and external systems, such as other TSOs, market operators or grid regulators. These interfaces are crucial for coordinating activities across national borders and ensuring cross-border grid stability.

- **Platform standards:** Platform standards ensure the underlying infrastructure (such as operating systems, database technologies and communication networks) of the modular eco-system is compatible and standardised, allowing different modules and systems to work on a common platform.

- **Data standards:** Data standards define the structure, format and semantics of the data exchanged within the control system and between external systems. They ensure data consistency and interoperability across different components and systems.

- **Security standards:** Security standards are essential to protect control centre systems from cyber threats. These standards define the security measures to be implemented across the modular eco-system, such as encryption, authentication, access control and intrusion detection.

- **GUI standards:** GUI standards include, but are not limited to, enabling technology, style and usability guidelines to provide the same look and feel across different modules, including their behaviour. The overarching goal is to provide a design catalogue that includes colour code, typography, alarming concept, etc. This will evolve through various maturity levels, ultimately leading to a centralised GUI for displaying module results and configuring modules via the main (centralised) UI module as a single cockpit for end users.

- **System modelling standards:** System modelling standards provide guidelines for creating digital representations of the power grid, including network topology, power flows and load distribution. These standards help ensure that the grid's behaviour is accurately modelled across different platforms and simulation tools.

Once in place, a list of these standards requires governance, which should be maintained by a body independent of any individual TSO. The standards must also be forward-looking, anticipating emerging technologies, as the modular nature of the eco-system will allow TSOs to upgrade/exchange modules at a faster rate than in the previous paradigm. In a subsequent step, a body could also develop tools to confirm that modules comply with the agreed-upon standards. Additionally, it could register compliant modules to a common database for TSOs for easy access to market offerings.

4 Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors

IV. Integration

Integration with Existing Systems

"The new eco-system must be integrable with and/or connected to existing systems, despite potential upgrades and/or updates to the existing systems."

The migration to an eco-system approach for the IT landscape may result in some (specialist) functions of the TSOs not being provided by newly developed modules. TSOs may have a variety of reasons for wanting to retain parts of their existing systems without violating the basic principle of the modular eco-system concept. Seamless integration of new modules with existing systems is therefore of great importance. This applies not only to the transition phase as the TSO shifts to the new eco-system but can also be valid as a permanent solution.

Whether a TSO wishes to continue using existing systems on a permanent basis can only be decided on a case-by-case basis for each TSO and system. The following reasons could be considered in such decisions:

- The existing system or further development of the system has just been commissioned or implemented, making system replacement financially unreasonable.
- The system is used by a TSO community rather than a single TSO, so system replacement requires joint coordination and agreement.
- The system is highly complex, and no comparable system on the market currently meets both the same quality of results and the modular principles.
- The system is a data-supplying system from a third-party provider outside the TSO's sphere of influence.
- The existing system provider agrees to adapt the existing system in accordance with the principles of modularity, eliminating the need for a full replacement.

The seamless integration of new eco-system modules with existing systems is crucial. Since TSOs are unlikely to have a reasonable interest in completely converting their IT systems to new modules, the eco-system concept should focus on the interaction between new modular systems and existing systems.

While new modules can be developed flexibly with customisable interfaces to other systems, existing systems typically lack this openness. It is therefore necessary to evaluate what type of interfaces are required. A distinction must be made regarding whether other modules in the eco-system must supply input data to the existing systems or consume output data from them, or whether both data-supplying and data-consuming interfaces are required.

Due to the black-box nature of many existing systems, interfaces may need to be developed jointly with the provider of the existing system. This becomes particularly relevant if modules must be connected to the existing system as data-providing systems, as these can often only be viewed and adapted by the providers. It is important to ensure that interfaces are created according to the rules of the modular systems, allowing them to be understood by other developers and the TSO. This enables further development, if necessary, without being reliant on the vendor.

If the new module requires output data from existing systems, developing an interface may be unnecessary if the relevant data is already extracted (e.g. a file in a folder). In this case, developing an interface for the new module to the relevant folder and configuring the data model of the new module to read the dataset would be sufficient. However, as the creation, storage and subsequent import of data records in files is often relatively time-consuming, this type of interface is only a reasonable solution for processes that are not time-critical.

Well-developed integration capabilities, including into domain-specific legacy systems, are therefore crucial for the practical feasibility of a modular eco system.

Infrastructure Agnosticism

"The new eco-system shall be agnostic towards underlying infrastructure like private cloud, public cloud or on-premise as long as technology requirements are fulfilled and scalability is secured."

The new eco-system should be flexible, adaptable to any situation or technological environment and compatible with any infrastructure. Agnosticism towards the underlying infrastructure is therefore of great importance, as it ensures the vendor-independency of the system. This means the solution is designed to be usable on different platforms, in different environments or with different infrastructure components without needing major adjustments or changes. In addition to infrastructure agnosticism, it is crucial for the new eco-system to maintain core characteristics like scalability and integrability.

A prerequisite for a modular eco-system is that the infrastructure be cloud-native compliant. Cloud-native practices empower organisations to develop, build and deploy workloads in computing environments (public, private, hybrid cloud) to meet their organisational needs at scale in a programmatic and repeatable manner. It is characterised by loosely coupled systems that interoperate in a manner that is secure, resilient, manageable, sustainable and observable.

Key properties of an infrastructure-agnostic eco-system include:

- **Flexibility:** Operation is not tied to a specific hardware, virtualisation platform or cloud provider.
- **Portability:** Applications or systems can be easily migrated from one infrastructure to another without major changes.
- **Scalability and future-proofing:** Companies can change, expand or update their infrastructure without redeveloping or adapting existing application functions.

For modular, vendor-agnostic systems, the independence of functionality from its technological basis is of great importance, ensuring the successful and flexible use of modules in the planned manner.

V. Digital and Cyber Resilience

"The new eco-system, its modules and its operation shall be resilient by design, applying zero-trust principles. Information and processes must have a high level of integrity, identifiable entities and verifiable and secure information exchange on and into the eco-system platform."

Motivation for Digital and Cyber Resilience

Transmission system operators have clear resilience and security priorities when operating the power system:

1. Functional safety – first personnel safety, then minimising equipment damage
2. Security of supply as the primary goal for society
3. Fair competition across power markets

Hence, overall power system resilience is a key performance indicator.

Resilience for critical entities is defined in the CER Directive as a critical entity's ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident.

Resilience is a multidimensional challenge, which in this position paper is seen from a digital and cyber resilience perspective, where digital and cyber resilience is a critical and important pillar for a future control room eco system. The future control room eco-system is required to function in any power system operational state, whether normal, alert, emergency, blackout or power system restoration.

A future ecosystem shall incorporate an overall resilience concept, covering any type of incidents, securing operational continuity and providing fast recovery if any function should fail.

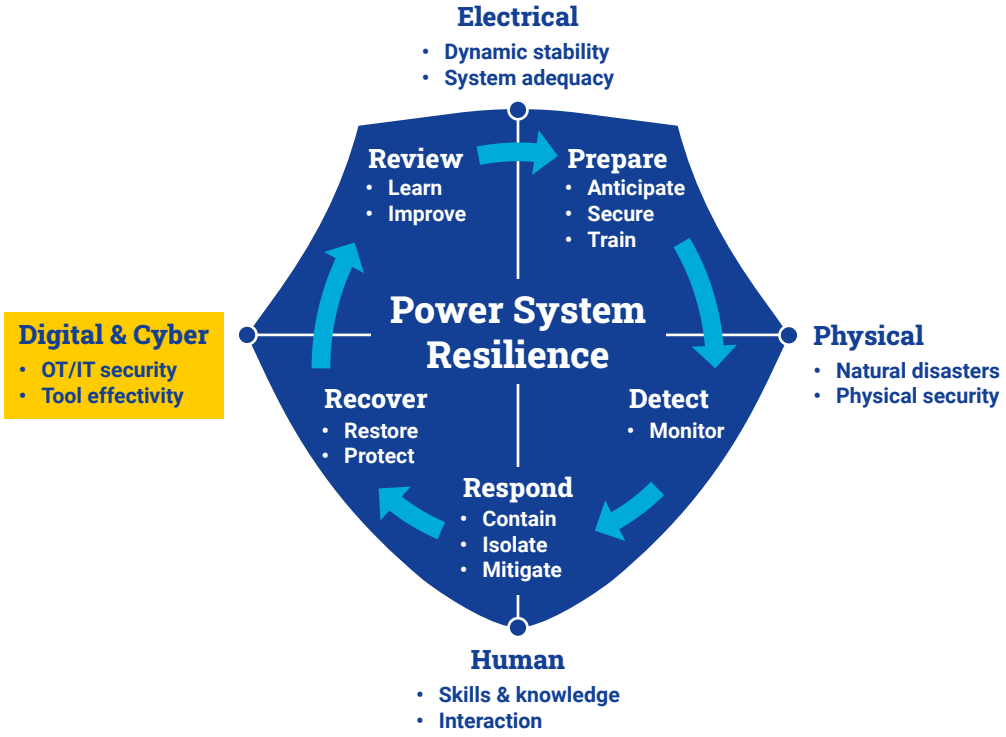


Figure 1: Power System Resilience Life Cycle for the Continuous Improvement of Digital and Cyber Resilience Capabilities

Digital and Cyber Resilience Capabilities and Principles

The future control room eco-system requires new IT business capabilities that ensure a high level of digital and cyber resilience, matching the resilience expected for the power system it operates. To maintain this high degree of resilience, we expect TSO control centres to have IT operations capabilities as an integrated part of the power system control in the future.

IT resilience capabilities are primarily, although not exclusively, derived from present and expected cyber threats.

The most important ones are shown in Figure 2:

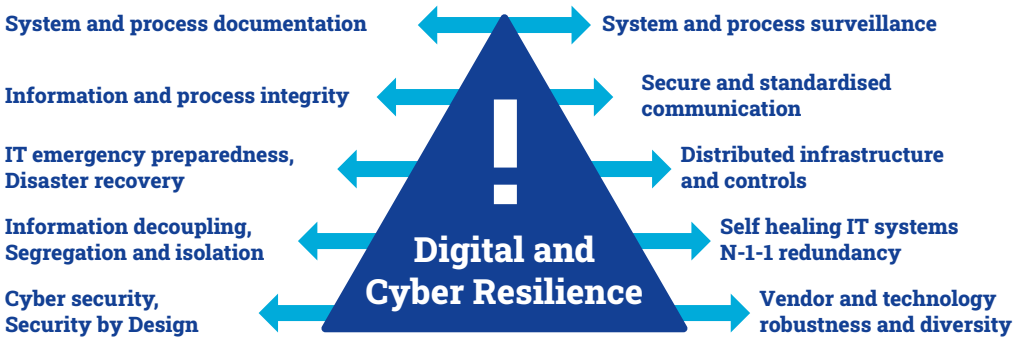


Figure 2: Digital and Cyber Resilience Capabilities – More Than Just Cybersecurity

A future control room eco system must implement a resilience culture that embraces possible incidents in every aspect.

To prepare, detect, respond, recover and review every aspect of digital and cyber resilience, the following key principles shall serve as a guideline for a future control room ecosystem:

- **System and process documentation:** Resilience to loss of personnel, as well as effective onboarding of new personnel and continuous improvements are essential. Documentation plays a crucial role in knowledge management, ensuring smooth onboarding of new personnel and quality maintenance of the digital and cybersecurity eco-system.

- **Information and process integrity:** Information and process integrity, which includes contract-based configuration and information model schema validations where information is verified against known information models, is a key resilience aspect to secure the power system operator's trust in the ICT (Information and Communication Technology) digital services they use. Contract-based configuration and process integrity utilises zero-trust principles by locking all code and configurations as contracts in a "trusted execution environment' using encrypted digital signatures. Codes and configurations should be signed by both people and security scans for approval before deployment. Zero-trust architecture must also ensure full traceability, with digital signatures for approvals on code and configurations in operational environments.

- **Secure and standardised communication:** This technical aspect ensures the integrity of integration and information exchange. Standards maintain integrity between system and system actors, while the use of international standards enhances concept and implementation robustness, as well as resilience to personnel loss and onboarding.

- **System and process surveillance:** It is essential to react to incidents early enough to prevent loss of power system operations. System and process surveillance must be active across every layer of the ICT stack, from information flows through applications to hardware health and performance.

- **Cybersecurity:** Often associated with the use and implementation of ISO 27001, a standard that secures robust processes to detect and react to risks and incidents, this standard must be supplemented with technical standards for implementing ICT-supported mechanisms within cybersecurity processes.

- **IT emergency preparedness:** This involves the response process, organisation and tooling necessary to recover from an abnormal large-scale incident. In IT resilience, this is part of fast recovery in case automated and known procedures are insufficient to recover from an incident.

- **Disaster recovery:** This is the process of recovering from extreme incidents, like malicious cyberattacks or a burnt-down data centre.

- **Self-healing IT systems and N-1-1 redundancy:** Supply-critical systems must be fully redundant, meaning every function, service or asset must be resilient to a single process failure with little to no control centre or function downtime during any hardware or software maintenance. All first-line failover processes shall be automatic where possible. It is part of every OT (Operational Technology)-oriented ICT environment; however, it must be thought through for failures across every layer of the ICT stack.

- **Information decoupling:** This ensures that only information allowed and verified may propagate through the system. This concept also enables the modular concept across security zones in the control room of the future eco-system. Information decoupling is a key feature of the zero-trust architecture.

- **Vendor and technology robustness and diversity:** In the event of supply chain issues that are not easily mitigated, there must be an alternative where existing hardware or software components can be easily and rapidly replaced or switched to minimise operational disturbances.

- **Segregation and isolation:** Isolated operation requires segregation of power supply critical functions from unsafe or infected segments in the IT systems. Operational platforms must be capable of continuous operation in isolated mode, which requires a clear separation between the enterprise environment and power supply–critical functions. Zone segregation with information decoupling between zones enables zone isolation in response to cybersecurity incidents.

- **Security by design:** Security must be embedded in system and solution design from the outset, not added after the fact. It must be integral and implemented with security in depth. The system design must account for robust and secure data transfer (in transit), storage (at rest) and processing (in process), while also incorporating alternative processes if the primary function is unavailable (fallback). Built-in quality is also a key part of security by design.

- **Distributed infrastructure and controls:** Distributing helps spread both physical and control risks, mitigating the impact of physical incidents, such as warlike physical attacks or natural disasters.

VI. Separation of Concerns

"The new eco-system shall have 'separation of concerns' as a guiding principle of its architecture."

Currently, the majority of European TSOs operate a non-modular system for their control centres, relying on one or a few vendors to provide a core system with all the necessary functionalities. This results in vendor lock-in and limits adaptability to new circumstances or technologies, requiring costly, multiyear projects to replace the entire system with a new non-modular system. Non-modular systems can also be integrated into a modular system. Multiple functionalities may be bundled and sold together with a single point of contact with the eco-system. This can devolve into a new rigid system over time.

To prevent non-modular systems from establishing themselves, adherence to a design principle from the software engineering world is recommended. "Separation of concerns" is a design principle that advocates for dividing a software system into distinct sections, each addressing a separate concern or functionality.

This approach enhances modularity, making the system easier to understand, develop and maintain. By isolating different aspects of the system, such as data management, user interface and business logic, providers can work on and implement individual components independently without affecting others. This separation not only simplifies debugging and testing but also promotes code reuse and scalability.

Note: In the case of multi-vendor delivery (one of the main drivers of modularisation), 100% avoidance of redundancy is infeasible, as it would create numerous interdependencies, making delivery and operation contracts overly complex.

The new ecosystem will consist of three layers:

- **Modules:** Modules are the building blocks of a modular system. Each module encapsulates a specific functionality or a set of related functionalities. Modules are designed to be self-contained, meaning they can be developed, tested and maintained independently. This modularity allows for easier updates and scalability, as changes in one module do not directly impact others.

  Each module will have a module contract with both the application platform and the technology platform to which it is to be connected. A module contract includes the definition of the interfaces, data requirements, application platform services and technology platform services required to run.

- **Application Platform:** The application platform serves as the foundation upon which modules are deployed and interact. It provides the necessary infrastructure and services to support the execution of modules. This includes runtime environments, middleware and APIs that facilitate communication between modules. The application platform ensures that modules can work together seamlessly, manage dependencies and handle shared services such as security, logging and data storage. A standardised set of shared services (both minimum and optional) should be defined to ensure module compatibility between TSOs.

  An application platform itself should be made of loosely coupled components, all of which should be exchangeable, replaceable and in some cases, optional.

- **Technology Platform:** The technology platform underpins the entire system, providing the core technologies, tools and environment needed for the application platform to function effectively. It ensures that the system is robust, scalable and capable of supporting the various modules and their interactions. It includes hardware, operating systems, databases and network infrastructure and covers functions such as storage and security and will dictate which standards are used to connect the other layers.

To enable a smooth transition to the new eco-system, the task force proposes scaling ambition levels, which can range from the current paradigm of existing non-modular systems to a fully modular system with fully separated functionalities.

To facilitate a transition, parts of the former modular system will need to be connected to the novel modular architecture to ensure continuity as individual modules take on functions with time. Although this initially results in additional complexity and redundancy, it is the initial step towards modularising the entire system.

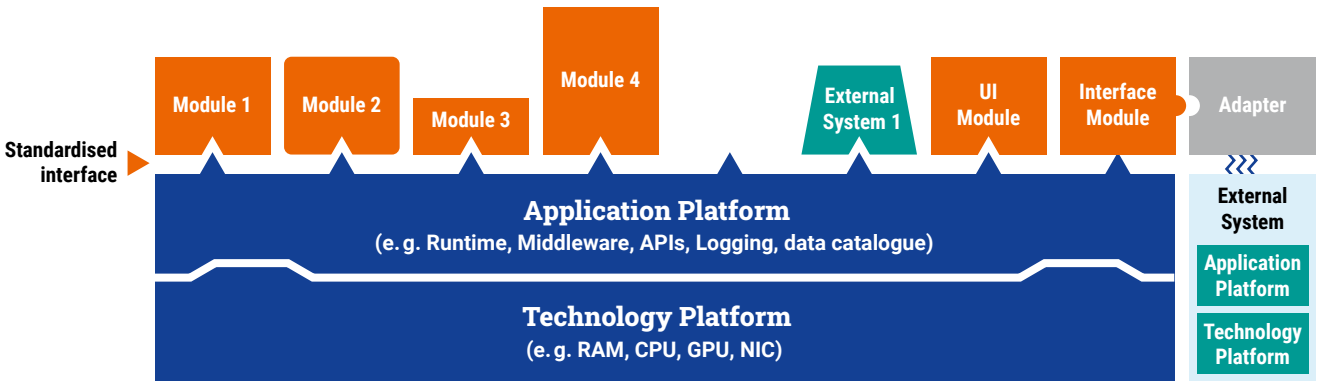


Figure 3: High-Level Illustration of the Proposed Architecture, Including Provisions for Different Module Functions and Integration with Other Surrounding Systems

VII. New Ways of Working

Development and Maintenance

"The new eco-system is not limited to software; it also includes development, operation and maintenance models."

To assume that the new eco-system only describes guidelines and guidance for the development of modular, vendor-agnostic software products is too short-sighted. TSOs operate in a very complex, increasingly changing world, are subject to strict regulations and require highly available and reliable systems. Deployment, software operation and the continuous further development of the modules (updates, upgrades, security patches, etc.) are therefore just as important for the success of the new eco-system as the development of the modules themselves. For this reason, the new eco-system must also provide guidelines and guidance for these areas of the software life cycle. This ensures that all aspects – from development to operation and maintenance – are integrated and coordinated to guarantee a sustainable and effective IT infrastructure.

- **Continuous Integration/Continuous Deployment (CI/CD):** One of the advantages of flexible, modular systems over existing non-modular systems is the ability to continuously release small software increments in an agile, short-cycle development and, after extensive testing, regularly deploy them. The freedom to choose providers at the modular level enables development that is closely aligned with user needs through regular feedback. This ensures that only the necessary functions are delivered, whether by the original provider or an alternate. Providers and TSOs can also work together dynamically on project progress, ensuring that knowledge remains internal to the TSOs and is not lost through externalisation. Building, testing and deployment can be largely automated. In the area of testing, manual testing, in addition to automated testing, is highly relevant. Particularly in critical infrastructures like the energy industry, the systems developed must ensure a high level of availability and reliability. In addition to testing the functionalities, testing these criteria is of great importance for safe software and therefore grid operation.

- **Software operation:** Thanks to flexible, infrastructure-agnostic modules, software can be operated in an environment of the respective TSO's choice, such as public or private cloud. Due to the high criticality of the system environment, an on-premise operation may be the most suitable environment, allowing the TSO itself to manage system operations.

- **24/7 maintenance:** Reliable operation of the power grid is a continuous, 24/7 task that demands a high level of availability and reliability from both the responsible employees and the software systems used. Depending on the area of application of the individual module, system downtime can quickly lead to significant damage in the power system, including a blackout. Reliably running systems are therefore very important for their successful use at TSOs. This also means that most modules used by TSOs will require 24/7 software support. Thanks to the independence of individual providers, it is also possible to flexibly decide who offers support for which module. This could be the provider of the respective module, a third-party provider or the TSO itself.

- **Continuous improvement:** The energy system is undergoing an intensive transition phase, with changing, growing and continuously emerging new requirements. This requires continuous development and adaptation of software systems. A flexible, modular system with agile development options makes it easier than ever to meet this need. In such a system, the TSO can decide individually for each module how and by whom its continuous improvement will be carried out.

In the new eco-system, TSOs have full flexibility over the coverage of the individual areas of the life cycle of their modules. In addition, providers can discover completely new business models by outsourcing services or offering them as Software-as-a-Service (SaaS). The new eco-system does not exclude certain providers; any company that is trusted and has a proven record can offer services in the various software life cycle phases.

Legal Considerations

"The new eco-system will require a legal framework to enable the 'separation of concerns'."

A key aspect of the new eco-system is not only its modular, vendor-agnostic structure but also the elevated relationship between TSOs and providers, as well as between TSOs themselves. New business models and formal rules are needed. Providers and contractors must comply with the rules of the modular contract when developing for one TSO to ensure the modules are available and usable to the rest of the market. At the same time, TSOs must develop their own modules, make them available to other TSOs and be able to use modules developed by other TSOs. An appropriate legal framework is essential to allow modules to be legally distinct in terms of liability and guarantees.

A legal separation of concerns is of great importance in order to develop modules that can survive in this volatile, highly diverse environment. This refers to the practice of treating different legal, regulatory or compliance-related aspects separately in a software solution.

In detail, it means the following:

- **Separation of legal responsibilities:** Different legal requirements or responsibilities are clearly separated to ensure the software complies with the respective laws and regulations in different areas or regions. This is particularly relevant if TSOs from different countries (and therefore different legal situations) want to use the same modules. Particularly in highly regulated industries, such as the energy industry, it may be necessary for a module to have different components or exist in slightly different variants, each covering specific legal requirements. These components are treated separately so that changes or adjustments in one legal area do not have any unintended effects in other areas.

- **Modularity and flexibility:** Separating legal aspects into modular components makes software more flexible and easier to adapt in case of changing laws or new compliance requirements. The concept therefore promotes the adaptability and maintainability of the software.

- **Reduction of risks:** Separating legal responsibilities allows risks to be more effectively controlled and mitigated. Errors or legal violations in one part of the software should not jeopardise the entire operation or other legal areas.

In general, these legal considerations should enable the development of software solutions that are better aligned with legal compliance and promote a systematic, structured approach to integrating legal aspects into software development.

Cross-Source Compatibility

"The new eco-system can accommodate a combination of parts/modules that are open-source, proprietary and/or commercial."

A modular IT landscape allows different components or modules to be integrated and managed independently. By incorporating a mix of open-source, proprietary and commercial modules, TSOs can leverage the unique advantages of each type, creating a robust and versatile IT ecosystem.

Open-Source Modules

Open-source modules offer significant cost savings, foster innovation through community collaboration and benefit from enhanced security and support due to large developer involvement. However, they may require customisation to fit specific needs and may not always be a perfect solution without additional adjustments.

Proprietary Modules

Proprietary modules offer high customisation, internal innovation and better cost control compared to commercial solutions, while also aligning closely with business needs. However, they require significant development effort and ongoing security maintenance, with support varying depending on whether it is handled internally or by external developers.

Commercial Modules

Commercial modules offer quicker implementation through customisable solutions, regular updates and advanced features, supported by dedicated provider development teams. While they involve licensing fees, they provide strong security, compliance and professional support, with ongoing improvements driven by provider incentives and feedback from multiple TSOs.

Strategically combining modules from all sources can also create stronger synergistic benefits that translate to increased functionality, security and control across the control centre infrastructure. The increased level of choice that a modular infrastructure provides, especially as additional business models enter the market, can be highly beneficial for both TSOs, who gain greater choice, and classical providers, who can focus on core competencies.

New Provider Collaboration

"The new eco-system will embrace a new collaboration with providers and facilitate new market models."

The classical relationship between a TSO and a system provider has functions built on top of each other. Existing systems often lack transparency and are created on demand and tailored specifically to the TSO. Existing systems are usually difficult to modify, update or replace by any party, including their initial developer, due to their complexity and interconnected architecture. Updating one aspect of an existing system often leads to a large, multiyear project to build a new system from the ground up in which the same issues endure.

A shift to a modular eco-system built on the principle of separation of concerns implies a new relationship with classical providers, which must be established and will lead to the creation of new market models.

The new eco-system would allow smaller packages to be created in the form of modules. These modules can be built in several ways, including but not limited to:

- A provider can be requested to build an individual bespoke module.
- A provider can be requested to provide an "off-the-shelf" module with some customisation.
- A third party can develop smaller bespoke modules that work with already existing modules.
- A TSO can develop its own bespoke module using internal or external development teams.
- A TSO can license modules from other TSOs.
- Collaborative development can be undertaken between several TSOs for a common module.
- Self-developed/open-source modules can be traded between TSOs.

In addition to expanding market model possibilities, new ownership and maintenance models can emerge by assigning responsibilities to different parties. The flexibility provided by this varied approach ensures that each party leverages its strengths and provides the best possible service.

The new modularity would also allow modules to be developed in shorter time increments than existing systems. Avoiding the usual 10- to 20-year gap between updates allows the latest technologies to be continuously implemented. For providers, this means smaller (although more regular and numerous) contracts, reducing risk for both the providers and the TSOs.

The new eco-system can only take root and succeed if the following holds true:

All parties are willing to dive into a new era of TSO–provider collaboration.

Glossary

Vendor agnostic system (VAS)	A system that is independent of any specific provider, allowing for flexibility and compatibility with multiple providers and technologies.
Eco-system	The new modular paradigm this document seeks to outline, where independent modules that are exchangeable and replaceable are "slotted" into an architectural backbone. The eco-system is a contrast to existing systems.
Transmission systems operators (TSOs)	Entities responsible for operating and managing the electrical transmission network, ensuring reliable power distribution across regions.
Data products	Digital products consisting of data that has been processed, organised and structured to be used by consumers or other systems. These products often provide valuable insights and are intended to be analysed or integrated into other systems.
Information products	Products derived from data that have been processed, interpreted and presented in a way that provides actionable knowledge or context. These often include reports, dashboards or analytics that help decision-makers understand data in a meaningful way.
Existing systems	Existing systems represent the status quo when it comes to control centre systems. They are traditionally characterised as a closed system provided and maintained by a single vendor.
Provider	An entity, such as a company, academic institution or service provider, that offers products, services or solutions to others. In the context of software or technology, a provider may or may not be responsible for supplying and/or maintaining services, modules or platforms.
Vendor	In the context of this paper, a vendor is a subcategory of provider, limited to commercial proprietary solutions.
Cloud-native	Cloud-native practices empower organisations to develop, build and deploy workloads in computing environments (public, private, hybrid cloud) to meet their organisational needs at scale in a programmatic and repeatable manner. It is characterised by loosely coupled systems that interoperate in a manner that is secure, resilient, manageable, sustainable and observable.[5]
Proprietary	Referring to products, software or technologies that are owned by a single entity, including TSOs.
Modular contract	A form of documentation that outlines the terms, expectations and responsibilities between parties involved in using or providing a module. It describes the module's capabilities and usage. When standardised across providers and TSOs, modular contracts facilitate coordination, enabling modules to function in a plug-and-play capacity. Each module has a contract with both the application platform and the technology platform it connects to.

5 toc/DEFINITION.md at main · cncf/toc · GitHub

Contributors

This study was conducted by Working Group Digital & Communication under the Research, Development, and Innovation Committee. ENTSO-E Secretariat would like to thank RDIC, ICTC and SOC members for their valuable contributions during the drafting but especially during the reviewing and commenting phase.

Special thanks to the representatives from 50Hertz, PSE, TenneT, Statnett, Energinet, Svenska Krafnet etc. for their valuable insights and experience crucial to the publication of this position paper.

Review and Drafting team

Anna Gorczyca-Goraj . . . . . PSE S. A. / Convenor WG5

Ralf Heisig . . . . . 50Hertz Transmission GmbH / Convenor TF VAS

Dennis Jansen . . . . . BearingPoint GmbH

Matija Naglič . . . . . TenneT TSO B.V.

Andreas Rudolph . . . . . TenneT TSO GmbH

Morten Småstuen . . . . . Statnett SF

Carsten Strunge . . . . . Energinet Systemansvar A / S

John MacAllan . . . . . 50Hertz Transmission GmbH

Siddhesh Gandhi . . . . . ENTSO-E AISBL

Publisher

ENTSO-E AISBL
8 Rue de Spa
1000 Brussels
Belgium

www.entsoe.eu
info@ entsoe.eu

Design

DreiDreizehn GmbH, Berlin
www.313.de

Images

Cover: iStock.com/sankai
page 7: iStock.com/Lari Bat
page 9: iStock.com/authorstock007
page 12: iStock.com/byakkaya
page 18: iStock.com/ko_orn

Publishing date

May 2025

European Network of
Transmission System Operators
for Electricity