DSO ENTITY
DSOs FOR EUROPE

CRA Transition for Electrical Substations: DSOs' Experiences, Challenges and Considerations

Drafted by Expert Group Cybersecurity

September 2026

CRA transition for electrical substations: DSOs Experiences, Challenges and Considerations

Drafted by DSO Entity's Expert Group on Cybersecurity

September 2026

DSO ENTITY
DSOs FOR EUROPE

Table of Contents

Executive Summary

DSOs strongly support **Regulation (EU) 2024/2847**, **the Cyber Resilience Act**. Its requirements are necessary to raise the cybersecurity baseline of digital products, improve vulnerability handling and strengthen the resilience of European supply chains.

In primary and secondary electrical substations, however, CRA implementation creates a specific transition challenge (e.g. stranded investment). Protection, control, automation, monitoring and managed power-supply equipment are part of tightly integrated operational architectures, with long engineering, qualification, industrialisation and construction cycles.

The resulting impact for DSOs is therefore primarily indirect but potentially high. If manufacturers and the wider supply chain cannot make CRA-compliant digital products available, qualified and industrialized at the required scale in time, DSOs may be unable to execute regulated substation investment plans, including projects scheduled for 2028 and 2029.

DSOs therefore request a narrow, evidence-based and risk-managed transitional framework. A mitigation strategy not to lower the CRA ambition, but to avoid supply-chain disruption, preserve investment plan execution and ensure that compliant solutions can be standardised, validated and industrialised before becoming mandatory at scale. This framework should be applied only to clearly identified equipment and already committed projects, with documented risk assessment, compensating controls, traceability, vendor support and a binding migration path to full CRA compliance.

To make this framework workable in practice, regulatory clarity is also needed on product classification, conformity-assessment routes and evidence expectations for transitional use.

1. DSOs support the CRA and its security objectives

The CRA addresses a genuine and material need: connected hardware and software placed on the Union market should be designed, developed and maintained with an appropriate level of cybersecurity. DSOs depend on a broad and specialised supply chain. A common European baseline for secure-by-design products, vulnerability handling, security updates, technical documentation and conformity assessment will improve transparency and reduce systemic risk.

The electricity sector is already implementing complementary obligations and good practices through NIS2, CER, the NCCS and established OT-security frameworks. CRA implementation should reinforce this direction by ensuring that product-level cybersecurity is carried out by manufacturers and consistently evidenced throughout the supply chain.

We are fully committed to the Cyber Resilience Act and believe the following aspects are fundamental:

- Update technical specifications and procurement clauses so that future equipment delivers the
- required CRA evidence and lifecycle support.
- Engage manufacturers early on product classification, conformity assessment, secure development, vulnerability handling, updates, support periods and component transparency.
- Qualify and industrialise compliant replacement technologies as soon as they become technically and commercially viable.
- Integrate CRA requirements with sectoral risk management, operational resilience, incident response and supply-chain controls.
- Complete the transition to substation architectures based on CRA-compliant products, without compromising safety, interoperability or security of supply.

IMPORTANT PRINCIPLE
A transitional mechanism shall serve as a bridge towards a fully CRA-compliant architecture. It must make compliance achievable in practice while preserving the integrity of the CRA baseline.

2. The operational reality of substations

2.1 Long-lasting technology and system activity

Substations are not assembled from short-lifecycle, interchangeable digital products. Their protection and control systems are engineered as operational solutions with strict dependencies between devices, communications, configuration tools, supervision platforms, protection schemes and field procedures. Changes that appear limited at product level can trigger redesign, retesting, documentation changes and retraining across the project lifecycle.

Network investments are planned and authorised on a multi-year basis. By the time a substation or an extension enters construction, equipment families, detailed engineering, interfaces, contracts and delivery responsibilities may already be committed. This creates a mismatch between the legal product timeline and the physical delivery timeline of regulated grid infrastructure.

2.2 Qualification is a system activity

A product being marketed as CRA-compliant is necessary, but it is not sufficient for immediate deployment in a live electricity network. **Before becoming business-as-usual, a replacement technology normally needs to pass a chain of DSO activities:**

- product and supplier assessment;
- laboratory and functional testing;
- cybersecurity and interoperability validation;
- standardisation of engineering templates and protection/control schemes;
- integration with telecommunications, time synchronisation, supervision and configuration tooling;
- pilot deployment and operational acceptance;
- industrialisation of project design, procurement, installation and commissioning; and
- training of internal teams, engineering partners, contractors and maintenance providers.

Compressing or bypassing these steps would transfer risk from product compliance into system integration and operation. A secure transition must therefore account for the entire deployment chain.

2.3 Brownfield extensions are especially constrained

Extensions of existing substations frequently need to remain compatible with a legacy architecture. The added bay, protection function, control unit or communication component may have to interoperate with equipment and protocols that will remain in service for many years. A new compliant product may exist in isolation but still be unusable if it cannot be safely integrated into the existing system without a broader redesign.

The regulatory concern is therefore not limited to whether a product exists on the market. It is whether a complete, qualified and industrialised solution exists for the specific brownfield context.

3. The implementation gap created by the CRA timeline

3.1 Already committed projects cannot always be re-engineered in time

Some projects scheduled for delivery after the CRA becomes fully applicable were designed and financially committed while the applicable product classifications, conformity routes, supporting standards, national assessment capacity and vendor roadmaps were still developing. For these projects, an immediate switch of technology may require new engineering, revised procurement, altered construction interfaces, repeat testing and new field competencies.

Where compliant alternatives are not yet deployable at scale, the available options may be reduced to delaying the project, redesigning an operationally mature solution under severe time pressure, or purchasing legacy units in advance. None is a satisfactory default outcome. For DSOs, the critical transition risk is a high indirect impact on investment delivery. If CRA-compliant substation products are not available, qualified, interoperable and industrialised by the supply chain in time, regulated investment plans may become partially non-executable, with consequences for grid development, resilience, connection capacity and budget planning.

3.2 Product classification remains insufficiently predictable

DSOs need clear and stable classification of the products typically used in primary and secondary substations. This includes protection relays and other IEDs, substation control units, remote-control equipment, automation devices, communication gateways, switches, routers, serial/IP converters, time-synchronisation devices, managed power supplies and related software or remote data-processing functions.

Uncertainty over whether equipment falls within the general requirements applicable to products with digital elements, are classified as important products with digital elements (Class I or Class II), or fall within the categories of critical products with digital elements, since it directly affects the manufacturer's conformity-assessment route, third-party involvement, cost, lead time and product roadmap. It also affects the DSO's qualification and procurement planning. Product-by-product analysis will remain necessary, but sector guidance and representative examples are needed to prevent inconsistent interpretations.

This uncertainty is reinforced by the fact that most CRA vertical, product-specific standards relevant to important and critical product categories are still under development. The key issue for the sector is not merely their future publication, but their timely approval or adoption and subsequent citation as harmonised standards in the Official Journal of the European Union. Until those standards are available, manufacturers and DSOs lack a stable technical reference for interpreting requirements, evidence expectations and conformity routes consistently across product families.

3.3 Conformity-assessment capacity must be visible and accessible

For product categories that require third-party conformity assessment, manufacturers and DSOs need early visibility of the competent, notified bodies, their technical scope, geographic availability, testing capacity and expected lead times. In many European countries the institutional framework is progressing, but the practical map of entities able to assess the relevant OT equipment and the scope of their competence is not yet sufficiently clear to support long-term procurement decisions.

This uncertainty is particularly significant for specialised electricity-distribution equipment, where assessment requires both cybersecurity competence and understanding of industrial product families.

3.4 Forced pre-CRA stockpiling is an undesirable outcome

In the absence of a transition route, DSOs may be incentivised to place large orders for individual legacy units before the CRA's full application, solely to preserve delivery of projects already committed for later years. This is legally and operationally burdensome and conflicts with the policy direction of the CRA.

- It locks capital into inventory rather than accelerating secure replacement technology.
- It may extend the operational life of legacy products beyond what would otherwise be necessary.
- It creates storage, preservation, traceability, warranty, obsolescence and unused-stock risks.
- It concentrates production demand before the application date and may distort the supply chain.
- It favours large operators able to finance stock and disadvantages smaller DSOs.
- It does not create better cybersecurity; it merely shifts the date on which specific units enter the market.

4. Requested transitional framework

DSOs request the European Commission to propose and coordinate a harmonised EU-level transitional framework for specific substation product families, with the involvement of competent national authorities for implementation, market surveillance, conformity-assessment capacity and sector-specific oversight. The mechanism should apply only where the DSO and manufacturer can demonstrate that immediate full compliance is not practically achievable for already committed projects and that the residual risk can be controlled.

This transitional framework should be understood as a supply-chain impact mitigation strategy. Its purpose is to prevent disruption caused by the temporary unavailability of CRA-compliant products, while creating a controlled, auditable and time-bound path towards full compliance for each product family.

4.1 Scope

- New substations and extensions or modernisations of existing installations whose engineering, procurement strategy, investment approval or contractual commitments pre-date sufficient market and regulatory readiness.
- Legacy products1 required to preserve interoperability with an existing operational architecture or to execute an already committed standard design.
- Product families for which a CRA-compliant alternative is not yet available, correctly classified, conformity-assessed where required, qualified by the DSO and industrialised at sufficient scale.
- Only the minimum equipment and project population necessary to bridge the verified transition gap.

4.2 Duration

The mechanism should not be tied in this paper to a single fixed period. Its duration should be determined by objective readiness criteria for each product family and deployment context. It should close when a viable CRA-compliant solution is demonstrably available, qualified, interoperable and industrialised at the scale required for planned works, allowing a reasonable operational cutover.

[1] As described by the CRA, “legacy Products” refer to products already placed on the market before 11 December 2027

4.3 Conditions and safeguards of the transitional framework

Condition	Minimum evidence	Purpose
Committed-project test	Approved investment, engineering baseline, procurement or contractual evidence showing the project was materially committed before a viable compliant route existed.	Prevent the mechanism becoming a general market exemption.
No viable alternative	Documented market and supplier assessment showing that a compliant alternative is unavailable, unqualified, non-interoperable or not industrialised at the required scale.	Demonstrate necessity and proportionality.
Cyber-risk assessment	Product and system-context assessment covering known limitations, threats, exposure, dependencies and residual risk.	Make the legacy constraint transparent and risk based
Compensating controls	Segmentation, hardened access, monitoring, controlled remote access, secure gateways, operational restrictions or other measures appropriate to the risk	Reduce risk during the transition
Traceability	Unit identification, manufacturer, version, placement/supply records, project allocation and configuration baseline.	Enable market-surveillance and lifecycle accountability.
Vendor commitments	Vulnerability disclosure contact, incident cooperation, available fixes or mitigations, support boundaries and obsolescence information.	Preserve minimum lifecycle support.
Migration plan	Named target architecture, qualification and industrialisation milestones, procurement cutover criteria and accountable governance.	Ensure a credible exit from legacy technology.
Periodic review	Regular reassessment of alternative availability, risk, incidents, vulnerabilities and migration progress.	End the transition as soon as justified.
Supply-chain continuity plan	Manufacturer roadmap, delivery capacity, product family transition dates, support commitments, qualification milestones and fallback options for constrained products.	Avoid disruption of regulated investment plans and ensure that manufacturers remain accountable for the transition to CRA-compliant products.

4.4 What the transition period enables

A transition period is not passive delay. It is the implementation window needed to convert a product-compliance obligation into a repeatable, safe and scalable operating model across the full substation lifecycle.

1	**Regulatory and product clarity**	Confirm scope and classification by product family; identify the applicable conformity-assessment route; map notified-body capacity and relevant standards.
2	**Supplier and product readiness**	Obtain manufacturer roadmaps, declarations, technical documentation, support commitments and evidence against CRA essential requirements.
3	**Qualification and interoperability**	Perform laboratory, cybersecurity, functional and interoperability validation in representative legacy and target architectures.
4	**Engineering and standardisation**	Update reference architectures, standard designs, technical specifications, configuration models, protection schemes, textbooks and acceptance criteria.
5	**Industrialisation**	Prepare repeatable engineering packages, procurement catalogues, logistics, factory acceptance, site acceptance and commissioning processes.
6	**Workforce and contractor readiness**	Train DSO engineering and operations teams, project industrialization departments, construction contractors, maintenance providers and commissioning personnel
7	**Controlled cutover**	Set product-family cutover criteria, stop new legacy commitments, complete in-flight eligible projects and monitor the target architecture in operation.

4.5 Target state

At the end of the transition, new and extended substations should use architectures in which all products with digital elements placed on the market are CRA-compliant, supported by clear conformity evidence, secure lifecycle processes and procurement requirements aligned with the DSO's sectoral cybersecurity obligations.

These activities cannot be compressed into a short administrative transition. Standardising engineering designs, validating protection and control behaviour, updating project documentation, training engineering partners and industrialising delivery processes require calendar time, supplier maturity and repeated execution before they can be safely deployed at scale.

5. Recommended EU and National Measures to Support CRA Implementation in Electricity sector

A. Targeted transitional measure

The European Commission should propose an appropriate EU-level legal mechanism establishing a limited and risk-managed transitional route, distinct from the transitional provisions set out in Article 69 of the CRA, allowing eligible legacy equipment to continue to be supplied and installed in already committed new installations and extensions while replacement technology is qualified and industrialised. Competent national authorities should support implementation through coordinated supervision, traceability expectations and market-surveillance practice.

B. Classification guidance

The European Commission should coordinate sector examples or guidance for typical substation and secondary substation products, including the treatment of integrated systems, components and remote data-processing functions, so that classification is interpreted consistently across Member States.

For protection and control systems, CRA implementation should not be assessed only as a sequence of isolated devices. While manufacturers will need to obtain the required CE marking and conformity evidence for each product with digital elements, DSOs also need guidance on how product-level compliance translates into validated protection and control architectures, especially where IEDs, gateways, switches, engineering tools, time synchronisation and supervision platforms operate as an integrated system.

C. National conformity-assessment map

Competent national authorities, coordinated at EU level, should provide a current, accessible view of notified bodies and laboratories, their accreditation or notification status, technical scope, accepted standards and capacity for industrial OT product families.

D. Brownfield interoperability guidance

Clarify how CRA compliance should be approached when a new product is integrated into an existing complex system, and interoperability constraints prevent immediate replacement of the complete architecture.

E. Evidence model for transitional use

Define proportionate documentation, traceability, risk assessment, compensating controls and market-surveillance expectations for products used under the transition mechanism.

F. Regulatory coherence

Align implementation with NIS2, CER and NCCS risk processes so product-level CRA compliance complements — rather than duplicates or conflicts with — electricity-sector resilience obligations.

G. Structured sector dialogue

The European Commission should establish a practical EU-level forum involving DSOs, TSOs, manufacturers, ENISA, competent national authorities, market-surveillance authorities, conformity-

assessment bodies, standardisation organisations, and any other relevant stakeholder for the EU electricity sector to monitor readiness and remove bottlenecks,

H. Technical interpretation and advisory mechanisms

Manufacturers, conformity-assessment bodies and operators would benefit from access to a recognised technical interpretation mechanism capable of providing consistent guidance on product classification, risk-assessment approaches, system boundaries, conformity expectations and the application of relevant standards.

Such a mechanism would help prevent divergent interpretations across Member States, reduce implementation delays and support a more predictable transition towards CRA compliance for operational technology products used in electricity networks.

The absence of a recognised interpretation mechanism may result in manufacturers adopting different compliance approaches, increasing approval lead times, delaying product availability and creating additional uncertainty for regulated investment programmes.

6. Boundaries of the DSO request

THE REQUEST IS	THE REQUEST IS NOT
Targeted by product family and project population ✓	A blanket exemption for electricity operators ✗
Temporary and linked to readiness evidence ✓	Permission to place unsupported products on the market indefinitely ✗
Conditional on risk assessment and compensating controls ✓	A relaxation of vulnerability or incident-management responsibilities ✗
Traceable and reviewable by competent authorities ✓	A way to avoid manufacturer accountability ✗
Paired with a funded and governed migration plan ✓	A reopening of already clear rules for installed assets and genuine like-for-like spare parts ✗
Designed to prevent unnecessary stockpiling ✓	A substitute for qualifying compliant products ✗

7. Conclusion

The CRA is necessary and DSOs support its ambition. A more secure European product supply chain is essential to the resilience of electricity distribution networks. The sector's request is not to delay that objective, but to ensure that the route to it is technically safe, operationally realistic and compatible with already committed network investments.

Substation technology cannot be replaced at consumer-product speed. The transition requires product classification, conformity-assessment capacity, qualified alternatives, interoperable architectures, industrialised project processes and a trained delivery ecosystem. Where those conditions are not yet present, a narrow transitional mechanism is the most proportionate way to preserve security of supply and investment delivery while maintaining a binding path to full CRA compliance.

A well-designed transition mechanism would enable operators to plan the transition smoothly, avoid unnecessary disruption to investment and procurement cycles (e.g. stockpiling legacy equipment), and ensure that compliant products can be deployed as they become available. . With a controlled transition, DSOs can accelerate the right outcome: compliant products deployed through mature engineering, procurement, construction, operation and maintenance processes across Europe's electricity networks.

In this context, the DSO request should be seen as a proportionate mitigation of high indirect impact. The absence of available, qualified and industrialised CRA-compliant products in the supply chain could prevent the execution of regulated substation investment plans, particularly for 2028 and 2029. A phased, risk-based and evidence-driven implementation route is therefore essential to avoid supply-chain disruption, budgetary impacts and delays in grid development, while keeping manufacturers fully accountable for delivering compliant products and supporting the migration to the CRA target state.

PROPOSED OUTCOME
A coordinated European transition framework that keeps committed grid projects deliverable, prevents unnecessary stockpiling, makes residual risk transparent and brings each substation product family to full CRA compliance as soon as a viable end-to-end deployment route exists.

8. Legal and policy references

- Regulation (EU) 2024/2847 — Cyber Resilience Act
- European Commission — Blue Guide on the implementation of EU product rules 2022
- Commission Delegated Regulation (EU) 2024/1366 — Network Code on Cybersecurity
- Directive (EU) 2022/2555 — NIS2
- Directive (EU) 2022/2557 — Critical Entities Resilience