

The resilience gap in CNI: How OT virtualisation addresses modern cyber-kinetic threats

LESSONS FROM UKRAINE'S ENERGY GRID

Table of contents

1	Threat landscape: Why CNI needs greater resilience	3-4
2	Key challenges and root causes	4-5
3	How the problem can be solved	6-9
4	Impact on the grid and TSO	9
5	What we have learnt	9-10

1 Threat landscape: Why CNI needs greater resilience

Russia's full-scale invasion of Ukraine has introduced a new mix of cyber-kinetic threats to CNI that have never been experienced before. The adversary uses an almost unlimited pool of resources to attack Ukrainian infrastructure in both the physical and virtual worlds.

This white paper presents our expertise of protecting the Ukrainian transmission system operators (TSO). It describes the security challenges we encountered and the solutions developed and deployed by Cossack Labs to help the TSO withstand some of the most complex cyber-kinetic threats: from the physical capture or destruction of communication paths and critical assets at substations and data centres to sophisticated cyberattacks and attempts to disrupt or manipulate the people operating the system.

1.1 Critical infrastructure, including power plants, control rooms, communication channels, and data centres, is subject to physical attack

The threat landscape posed by cyberattacks is relatively well understood. Full-scale war, however, has placed an additional dimension: the risk of losing connectivity, equipment, and people engaged in CNI operation. We have identified the following key factors that need to be considered:

- ▣ **Control rooms, data centres, and power plants can be destroyed**—by a missile, a drone or a cyber attack—achieving the same operational result. Either way, the operator loses visibility of the process and the ability to act on it. In the electricity sector, the inability to manage islanding can turn a local incident into a wider blackout.
- ▣ **CNI operations must continue while the physical threats persist.** Infrastructure under attack cannot suspend operations until the threat passes, and no engineer can be sent to a substation being shelled. Every component must be operable, recoverable and re-securable with as little human presence on site as possible.
- ▣ **Capturing a data centre or power plant by an adversary.** This creates entry points and platforms for persistence and can give the attacker full control over the infrastructure. In this case, **restoration activities are carried out under pressure.**
- ▣ **Communication channels are targets in their own right.** Communication channels are also part of the physical infrastructure and can be damaged or destroyed by physical attacks. Near real-time connectivity among energy assets, substations and data centres is vital for managing the whole system.

1.2 End devices and RTUs are inherently distributed and physically exposed

Field devices are spread across the service territory. Their number keeps growing: RTUs, sensors, meters, and distributed energy resources. This increases the attack surface and means that, under wartime conditions, the possibility of an endpoint being captured must also be considered.

Furthermore, when territory is occupied, substations and remote sites are taken over while still operating. The attacker then has full physical access to the equipment. They can open cabinets, read or remove memory, and connect their own tools. Attackers can take as long as they need without having to hide.

1.3 Legacy OT protocols are not designed for secure operations

CNI networks still run on protocols designed for closed communication channels such as Modbus, IEC 60870-5-101/104 and IEC 60870-5-104. Both were later encapsulated in TCP/IP without being redesigned. They provide no message authentication, integrity checks, or encryption. Any existing checks address line quality, not security.

So anyone who reaches the network can read every value, write every command, and have the equipment obey.

1.4 The missing section that explains it all

In summary, energy infrastructure consists of distributed endpoints connected to data centres by unsecured communication channels. Security is provided by air-gapping the whole communication infrastructure. However, this becomes a significant challenge once air-gapped channels are replaced with public internet connections.

2 Key challenges and root causes

The factors described above create a range of problems that should be addressed holistically.

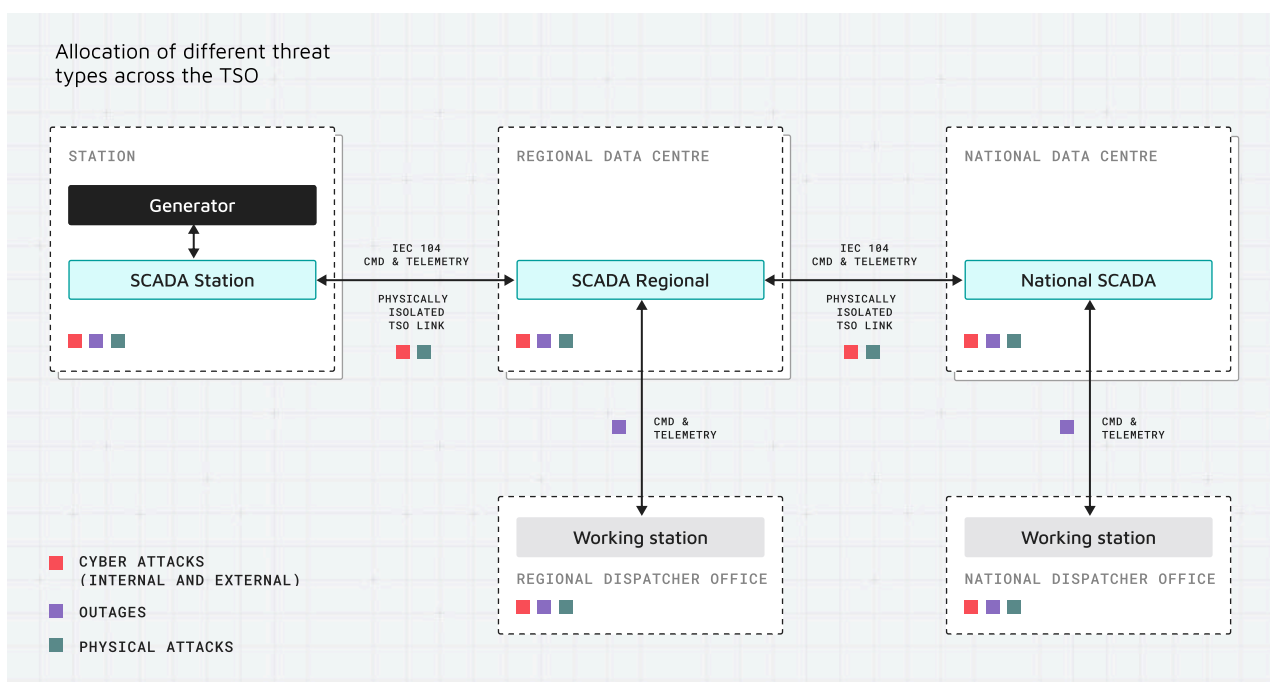
The main problem is the loss of connectivity to control rooms and data centres, which in case of physical damage, leads to a loss of grid visibility and control. As a result, there is no way to get telemetry and deliver commands to remote objects. Consequently, the grid faces a partial blackout. In normal mode, this risk is well mitigated by having a trusted reserve OT infrastructure. However, protection against sabotage or direct, coordinated cyber-physical attacks requires a different type of response.

Moreover, personnel operating grids, substations, and RTUs face constant risks. They work under constant time pressure and attack threats while restoring and maintaining equipment.

Besides that, unprotected protocols have already been the source of real attacks on critical infrastructure, repeatedly in Ukraine. Industroyer in 2016 and Industroyer2 in 2022 both communicated directly with substation equipment using IEC 60870-5-104. In Lviv in January 2024, FrostyGoop in, used ordinary Modbus TCP writes to heating controllers—nothing malicious installed on the devices themselves—and left roughly 600 apartment buildings without heat for two days in sub-zero weather.

As a result these issues may result in the following consequences:

- ▣ **Imbalance in the power system.** An attacker who gains access to the network can alter telemetry in transit, inject false measurements, or block them entirely because the protocols verify neither the sender nor the content. The operator follows the correct procedure based on the information they see but reaches the wrong result. Generation and load drift apart, while frequency and voltage exceed their permitted limits before anyone can react.
- ▣ **Disconnection of consumers.** The same attacker can send commands directly, and the equipment accepts them as if they came from the control centre. Opening breakers disconnects consumers immediately—as Industroyer did in 2016. In addition, physical damage to communication channels would prevent the operator from managing remote consumers, even if there is enough power to meet their needs.
- ▣ **Blackouts.** Recovery depends on the same channels and telemetry. An attacker who controls them—or has physically destroyed them—can prevent the operator from managing islands and re-energising the network, causing a local outage to spread into a wider blackout and last longer.



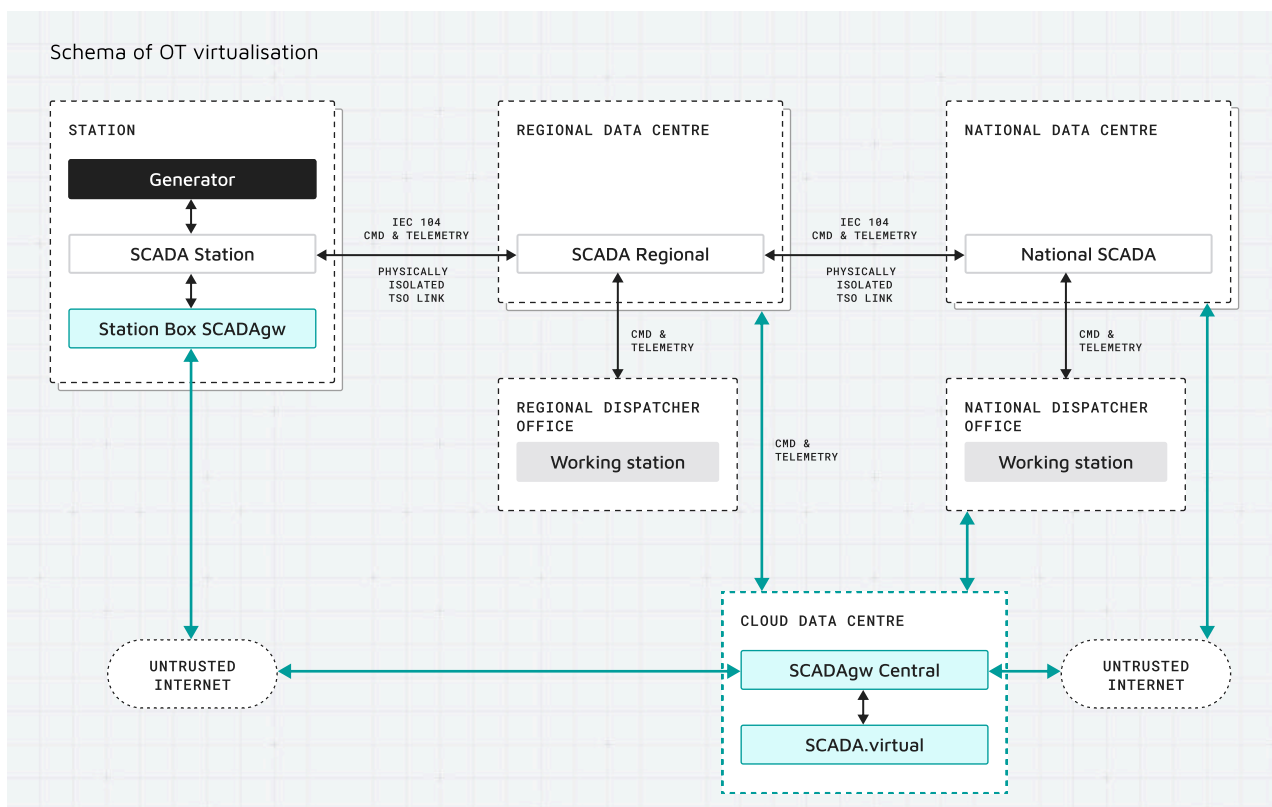
3 How the problem can be solved

We developed secure virtualisation of OT networks for the Ukrainian transmission system operator, operating over open communication channels and public clouds, to address the reliability and security threats highlighted above. We expect that this approach applies to other use cases.

Our solution ensures resilient, secure delivery of telemetry and commands across CNI systems when trust in ground infrastructure or edge devices is contested. That capability does not depend on the control rooms, data centres, hardware or network that the primary system depends on.

Besides that, running a national grid under daily attack required our solution to provide additional capabilities:

- Non-disruptive integration. The system was deployed into a live national grid without interrupting operations. No equipment had to be taken out of service, and no outage window was needed.
- Cryptography with minimal performance impact. Encrypting network traffic does not slow data exchange, so communication remains near real time.
- Flexible and secure routing of telemetry and commands between RTUs and SCADAs of TSOs, establishing reserve management systems.
- Operator-configured telemetry mapping. The operator's staff configure protocol value mapping, so subsequent telemetry changes do not depend on vendor availability.
- A platform-agnostic solution that can be migrated between cloud and on-premises environments with minimal modifications.



OT virtualisation

As noted above, damage to physical channels can significantly impact operations. Accordingly, OT virtualisation over redundant public communication channels, supported by appropriate security controls and direct equipment integration, addresses these risks. In addition, an OT virtualisation solution helps mitigate most single points of failure across the system.

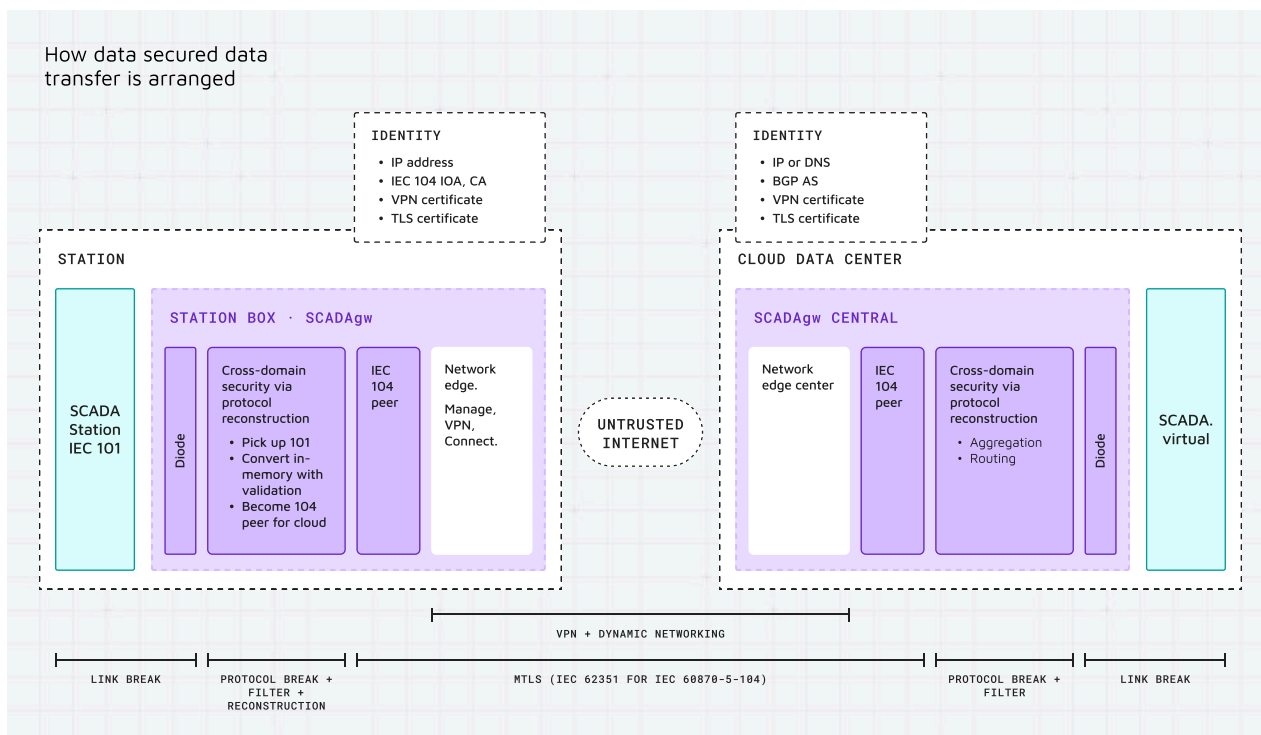
The solution establishes and maintains a reserve, virtualised copy of the operator's data acquisition and supervisory capability. The copy runs as software on general-purpose infrastructure. Kept live and up to date, its state matches the primary environment rather than being restored from a backup. Operations can move to the reserve copy when the primary environment becomes unavailable, compromised or no longer trusted.

Traffic carrying telemetry and commands is transmitted over public networks, including the public internet. To maintain high connectivity during communication channel outages, we use multiple channels in parallel. This approach reduces confidentiality and integrity risks while increasing the availability of the whole solution. Accordingly, we are designing a topology with as few single points of failure as possible. Besides that, each endpoint authenticates the other, and the payload is encrypted between them, so a carrier on the path sees only ciphertext and routing information. These measures also address the challenges highlighted in section 1.3.

The underlying network does not have to be private, dedicated or trusted, as the protection does not depend on any of these characteristics.

To ensure secure operation over public communication networks, the solution applies three principles:

- ▣ **Zero Trust Network Access.** Every connection is authenticated and authorised independently. Network location grants no privileges: a device inside the operator's own network has no more rights than one arriving from the public internet.
- ▣ **Zero trust in the underlying cloud infrastructure.** From an architectural point of view, all components authenticated one another, and granular security controls are built on top of the cloud platform. For data confidentiality and integrity, all traffic and storage data are encrypted, so the infrastructure running the system is never in a position to read or alter what it carries.
- ▣ **Cross-domain security.** Data is transferred between distinct security domains under controlled and verified conditions. Connecting two domains does not merge them; data is strictly classified and validated while passing through data gateways.



Station boxes and fleet management

The whole perimeter of virtualised operational technology (OT) networks should be protected, including TSO SCADA and substations edge devices. As part of the solution, specialised station boxes are deployed across the grid network to provide a secure communication layer between field equipment and the central control infrastructure. They enable the secure collection of telemetry from RTUs and the delivery of control commands back to them.

The distributed nature of station boxes and the associated risks prompted the development of a dedicated fleet management subsystem. This subsystem safeguards substation devices throughout their lifecycle, including in contested and disconnected environments.

Two conditions shape how it all works, both arising from working under fire:

- ▣ Every step can be carried out during an attack, while dispatchers and engineers are in shelter. Setup, deployment, monitoring, taking equipment out of service and removal can all be performed remotely. No one needs to be near the equipment or seated at a console in the control room.
- ▣ In a crisis, the system is built to minimise the number of manual steps required. During a rocket attack, the individuals who would normally take those steps are not at their desks.

Besides that, the whole solution should address the risk of a station box being captured. Accordingly, the following requirements have been incorporated into the solution:

- ▣ Physical access to the enclosure should leave visible evidence for the operator while giving the attacker nothing they can use.

- ▣ Keys and configuration must not be readable from the device. Removing the storage or reading the memory must not allow them to be recovered.
- ▣ Every device must be cryptographically unique. Secrets taken from one device must open only that device — not the fleet, not the control centre, not another site's traffic.
- ▣ It must be impossible to clone the device.
- ▣ Devices must be protected against tampering intended to modify their operating mode and/or data.
- ▣ Revocation must work remotely and immediately. The operator must be able to cut a captured device out of the network without travelling to it, and the rest of the network must continue running once it is removed.

4 Impact on the grid and TSO

Deploying OT virtualisation provided the national transmission system operator with the following advantages:

- ▣ Losing connectivity through the main communication channels does not mean losing the system. Telemetry and commands run over three independent communication channels, and operation continues unless all three are absent at the same time.
- ▣ If the grid is partly destroyed, supervision will continue over components that are still reporting.
- ▣ A new source of telemetry can be brought online quickly, before the main OT infrastructure is extended to reach that point.
- ▣ A telemetry feed can be redirected to a different recipient, so a SCADA migration does not require rebuilding the feed.

These measures have helped strengthen the resilience of the energy grid and reduce the duration of blackouts.

5 What we have learnt

Running the transformation of a Ukrainian TSO gave us experience that also applies to security engineering in peacetime. Security was a driver for moving old air-gapped OT systems onto modern open infrastructure. At the same time, security is the main bottleneck, that requires a lot of creative engineering rather than standard templates.

Moving OT infrastructure to the cloud opens new use cases and brings new challenges. To build virtually isolated systems that work in practice, teams need to understand cross-domain security in data analysis and apply zero trust: no user, component or data flow is trusted by default, and every exchange between domains is checked.

Air-gapped systems were protected by being cut off. Once they connect to shared networks and platforms, that protection is gone, and security controls have to take its place. Every new connection, data flow and access path must be justified and protected before it goes live. This is why security both opens the way for modernisation and sets its pace.

In the cloud, OT data can be used for monitoring, analytics and remote operation that a closed network did not allow. The same data now crosses domains with different levels of trust: control systems, corporate IT and external platforms. Virtual isolation holds only if every crossing is controlled: data is filtered and checked at each boundary, access is granted per task, and nothing is trusted because of where it sits on the network.

Above all, the key is how fast the team adapts: threats and risks change all the time, and the security of the system depends on responding to them as quickly as they appear.

Authors



Eugene Pilyankevich
CTO



Igor Luzhansky
CNI Solutions Lead



Dmytro Shapovalov
Head of Infrastructure & Hardware Engineering

About us

Cossack Labs is a UK-headquartered company that designs, builds and secures critical systems that must remain operational in high-risk environments.

Since 2014, we have helped defence, critical-infrastructure, finance, and technology organisations bring complex capabilities into operation — and keep them running under pressure.



Cossack Labs Limited, 12 New Fetter Lane
London EC4A 1JP, United Kingdom

New engagements
sales@cossacklabs.com

General enquiries
info@cossacklabs.com