

Red alert for cybersecurity in the energy sector

02 September 2025, 08:48

Tatiana Galibus

Cyberthreats are important and happening, as should be our defense

The threat is real

April 11, 2022. Deutsche Windtechnik, a German wind turbine operator, is forced to deactivate its remote data monitoring connections to the wind turbines. These were then switched off for security reasons and normal activity was resumed only at April 14. It was later confirmed that the failed connection was caused by a ransomware attack.

May 14, 2025. US energy officials announce they are reassessing the use of Chinese-made solar panel power inverters following the discovery of rogue communication devices which may be used as a two-way communication channel with the vendor and associated Chinese parties, and thus form a true threat to the energy grid they’re connected to.

These are but two concrete examples of real and ongoing cyberthreats to our energy sector. And, with the Spanish-Portuguese power outages fresh in mind, there may be dozens of other incidents where the link with cyberthreats and crime is yet to be discovered. Our energy systems and grid are not only vulnerable, they are under attack as we speak.

Are energy systems inherently vulnerable?

A vast majority of the energy systems worldwide face unique security challenges, caused by a worrying combination of potential vulnerabilities.

Most of the energy providers still rely on **legacy OT infrastructure**. The technology consists of grid and SCADA components, which are often decades old, and were never designed to be connected to a public network such as the internet. Cybersecurity was not even an afterthought. Power plants and wind farms, for instance, often use ICS (Industrial Control Systems) protocols without encryption or any form of modern authentication.

Nowadays, however, these infrastructures are increasingly **accessed remotely**, using **interfaces** for maintenance and monitoring that are often **misconfigured or lacking multi-factor authentication**. Needless to say that they thus become easy targets for unauthorized access. Remember the Viasat hack attacking and deactivating part of the Ukrainian satellite communication? This was done using precisely such unsecured remote connectivity to control interfaces.

Add to this the various **components** needed to form the energy **supply chain**. Some of these may be manufactured by **foreign vendors**, as was the case with the Chinese chips in solar systems. Others may contain **third-party software libraries**. In both scenarios, these components may compromise the supply chain and introduce hidden backdoors. The SolarWinds cyberattack in 2020 was a striking example of how such vulnerabilities can be exploited.

Not all vulnerabilities are digital, by the way: the **physical access** to an energy infrastructure may prove risky. Especially for remote or offshore energy infrastructures it is considerably easier to gain access or tamper with the infrastructure without being noticed. Researchers from the University of Tulsa reported that it took less than a minute of lock-picking on one unsupervised turbine's door to gain access to the unsecured server and, from there, to access IP addresses representing every single turbine in the network.

Energy systems are not inherently vulnerable but there are many potential vulnerabilities on various levels that can lead to security breaches. A worrying conclusion given the many cyberthreats circulating today.

What are the most common threats?

The energy industry is vital for any country worldwide, and therefore a popular target for cybercrime and other criminals looking to gain huge profits or to destabilize another nation. Unsurprisingly, there is a variety of threats aimed at energy infrastructures:

- **Ransomware:** cybercriminals attack major turbine manufacturers to disrupt operations and to release it only after a considerable ransom amount has been paid
- **Communication disruption:** cyberattacks targeting satellite or wireless links can disable monitoring and control functions, this may be used as a strategic attack in a general warfare, as was the case with Ka-Sat
- **Supply chain compromise**: Vulnerabilities such as Log4j or SolarWinds expose entire ecosystems to zero-day attacks, even long after they have been deployed

- **Physical sabotage:** as we have read above, a weak physical security can lead to a digital breach. But the physical access may also be used to afflict physical damage to the infrastructure. This is often used in combination with cyberattacks to enhance the impact of their attacks

Note the absence of the words ‘future’, ‘possible’ and ‘eventually’ in the above paragraphs. The threats aren’t just theoretical risks, they are real, escalating, and systemic. And they require an immediate and firm reaction from all parties involved.

EU: stronger focus on critical infrastructures

The required reaction must not be limited to the energy infrastructure providers or their vendors. Nor should it stop at any border, as energy supply has become an international landscape of increasing importance.

Recognizing this reality and the urgency, the EU is rolling out a stronger regulatory framework focused on critical infrastructures:

- **NIS2 directive:** this directive for essential services such as energy supply expands its scope to include renewables, grid operators and energy tech manufacturers, it forces actors in this industry to build a sound strategy around risk management, incident response, and supplier oversight
- **Cyber Resilience Act (CRA):** this regulation introduces baseline cybersecurity requirements for all products with digital elements, this obviously includes all energy IoT, control systems, and industrial software

Both of the above frameworks promote **collaboration and information sharing** between public and private sectors, and enforce **security-by-design** principles across the supply chain.

Even though they are “directives” and “regulations”, you should not consider them as optional or as future worries. Compliance with these regulations is increasingly becoming a core business requirement for any energy stakeholder. So it is not only advisable but simply essential to act now.

What can you do today?

The overarching message 'now is the time to act' applies to everyone involved, whether you are developer, integrator, or decision-maker in the energy industry.

But how can you act? And what needs to be done first?

First and foremost, you need to get a clear insight into the entire Critical Infrastructure Security area, and what you can do to increase security and reduce the threats.

And we can help you achieve these insights and guide your future endeavours.

Have you gained a sufficient level of insight, and are you looking to take the next step?

We gladly invite you to become part of our **COOCK+ collective research project** on “Trusted Connected Products in the Energy Transition.”

By joining this project, you’ll gain access to:

- First-line expert support
- Hands-on tools and scans
- Clear guidelines for product security and regulatory readiness

And if you need any more information on any of the topics above, you can always reach out to me. Just contact me at tatiana.galibus@sirris.be and we can jointly discover what your needs are and how we can help.

Together, we can build secure and resilient energy systems by design.

Contact us

Authors



Tatiana Galibus