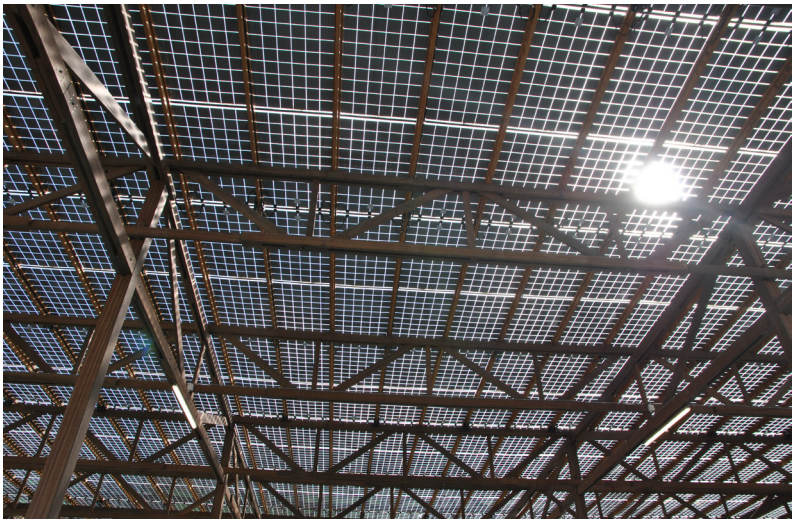
Meeting the solar PV cybersecurity challenge

Cybersecurity | Alexander Hansen Bakken, cybersecurity consultant at DNV, reveals the cyber vulnerabilities arising as solar farm operational technologies become more networked and connected, and recommends approaches to reduce the risk.



Credit: DNV

Cybersecurity threats to the grid-connected solar PV sector are becoming more common, complex, and creative as hackers gradually seek opportunities to disrupt the energy industry. Energy companies have been tackling IT security for several decades. However, securing operational technology (OT) is a more recent and increasingly urgent challenge. OT refers to the computing and communications systems used to manage, monitor and control industrial operations – for example, supervisory control and data acquisition (SCADA) and programmable logic controllers (PLCs).

As OT becomes more networked and connected to IT systems, attackers can more easily access and control systems operating critical infrastructure. It is now possible for attackers to stop solar PV inverters from working, disrupt energy supply in a power grid, shut down a wind farm and disable the safety systems in pipelines, refineries or oil and gas platforms.

The impact of this emerging threat is reflected in *The Cyber Priority*, DNV's study of 940 energy industry professionals on the state of the sector's cybersecurity, published in May 2022. The vast majority (84%) anticipate cyberattacks damaging assets and infrastructure within two years. Most consider it likely that cyberattacks will compromise life (57%), the environment (74%) and disrupt operations (85%).

Cyber attacks on solar assets are becoming more common and sophisticated.

Table 1 illustrates some recent cyber-attacks on energy industries. Two-thirds of respondents to DNV's *Cyber Priority* research say such incidents have driven their own companies to make major changes to their cybersecurity strategy and systems. Three-quarters say cybersecurity has significantly higher priority for their organisation than two years ago.

The 2022 IBM X-Force *Threat Intelligence Index* found 10% of the attacks it observed on industries operating OT in 2021 were in the utilities sector. It commented that while IT networks were compromised in the vast majority of these attacks, "the impact carried over to victims' OT technology in many of these instances".

The evolving threat landscape challenges solar PV asset owners, operators and suppliers to ask: 'What are the cyber risks? What effects could a successful cyberat-

When	Where	What happened
2022	Germany	A cyberattack led to a satellite link fault halting remote monitoring/control of wind turbines and solar PV plants. Thousands of satellite ground-terminal units needed replacing. Some solar PV plants used the radio link but were unaffected. There was speculation that the attack aimed to cripple Ukrainian command and control, with cascading effects impacting European countries, notably Germany. Germany has now issued a plan to prevent a repeat.[1]
2021	US	Ransomware attack on IT led to a six-day shutdown of the Colonial Pipeline carrying 45% of the US East Coast's gasoline, diesel, and jet fuel.[2]
2019	US	Solar PV (and wind) went offline in Utah after a cyberattack on a firewall halted communications between generating sites and a central control centre. Hackers caused similar 'blind spots' at a power grid control centre and small generation sites in California and Wyoming, without disrupting electricity supply.[3]
2019	India	Malware attack on Kudankulam Nuclear Power Plant in Tamil Nadu hit a single PC on an administrative internet server. Plant systems were not affected.[4]
2015 & 2016	Ukraine	The first known cyberattack that targeted a power grid and halted electricity supply (to parts of Kiev), reportedly via remote control of SCADA and substation infrastructure. The 2015 attack was more 'manual' in nature, whereas the similar 2016 incident was malware-induced. The latter, a malware framework known as CrashOverride or Industroyer, uses legitimate and standardized SCADA and grid protocols like IEC 104 and OPC to disrupt grid operation. Ukraine also says it fended off a Russian cyberattack on its power grid during the ongoing Russian invasion in 2022.[5]

Table 1: Selected actual and possible cyberattacks on energy infrastructure 2015–2022

Third-party IT services and cyber risk

Third-party IT services may have cyber vulnerabilities that could be remotely exploited and pose a potential threat for propagating further into IT and OT environments of a solar PV company. An example is remote internet protocol CCTV cameras monitoring the PV plant and normally installed within substation housings/enclosures. This service may well be provided by a third-party vendor with no knowledge or concern about industrial cyber risks. Many such CCTV systems are publicly available/accessible on the internet, perhaps via something as trivial as a default password (i.e. misconfiguration) or a weak password. If this CCTV system is then connected to the PV SCADA server, a hacker could gain access to the server by using the CCTV internet connection as a back door. In India in 2021, hackers are thought to have gained control of internet-connected DVR/IP camera devices for command and control (C2) of Shadowpad malware infections, as well as use of the open-source tool FastReverseProxy (FRP), though not in the solar PV context .

tack have? How do we prevent and detect such attacks? And how do we respond if an attack is detected?'

Cyber vulnerabilities

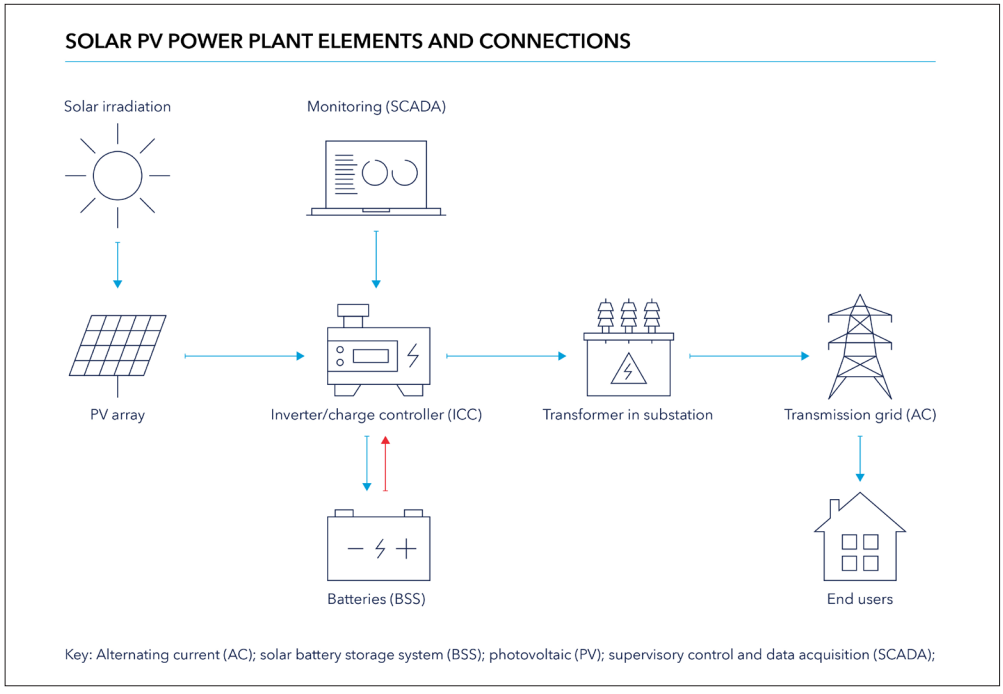
Examples of potential cyber vulnerabilities in grid-connected solar PV include those that can be found in OT that manages generation, inverters and the voltage of power supplied to the grid (Figure 1). Voltage control assists grid balancing to avoid damaging electricity users' equipment or tripping shutdown of electrical equipment.

Inverters are increasingly 'smart'. They are software-enabled, communicating with grids and remote centres handling operations and diagnostics. Some inverter suppliers offer software for remote access and control of their equipment, and several solar PV parks have multi-vendor remote access to aid maintenance and monitoring. These technologies can boost availability of power to the grid, lessen voltage fluctuations, reduce the levelised cost of electricity (LCOE) and raise profitability. Even where software updates and patches are part of the package, however, purchasers need to be sure they will not be exposed to the potential consequences of unacceptable cyber risk (see box 'Third-party IT services').

A cyberattack might result in a solar PV project going offline. An operator detecting a threat to their IT environment may disconnect their OT to guard against malicious actors accessing and controlling their OT. Or a hacker may bypass weak physical security or access controls, thereby directly accessing solar OT. The attacker's motive could be to immediately cut off grid connection or try to obtain a persistent remote command & control channel to disrupt operations in the future. If a company takes solar PV generation offline in a controlled manner, there is less risk of grid instability. If a cyberattack forces it offline, the risk of grid instability significantly increases. The inertia of synchronous generators in traditional power grids help mitigate oscillations. But inertia decreases with increasing penetration of inverter-dominated renewable power plants including solar. This can reduce the quality of the power and makes the network susceptible to power cuts.

Either way, attacks interrupting power supply and/or damaging the grid could lead to an operator paying financial penalties and/or damages. There could also be lost payments for energy not supplied and, if metering is compromised, through underpayment. The attacker could also steal data including names, passwords and other sensitive information. They could then use or sell the stolen data for identity theft purposes including fraud and accessing other parts of the solar and/or grid's OT and IT environments. A hacker accessing OT could damage inverters, motors for moving solar panels and connected battery storage systems (BSS).

In addition, disruption to supply due to cyberattacks could damage the generator's reputation for reliability with customers, including those with which it may have power purchasing agreements (PPAs).



Credit: DNV.

Figure 1: Solar PV power plant elements and connections

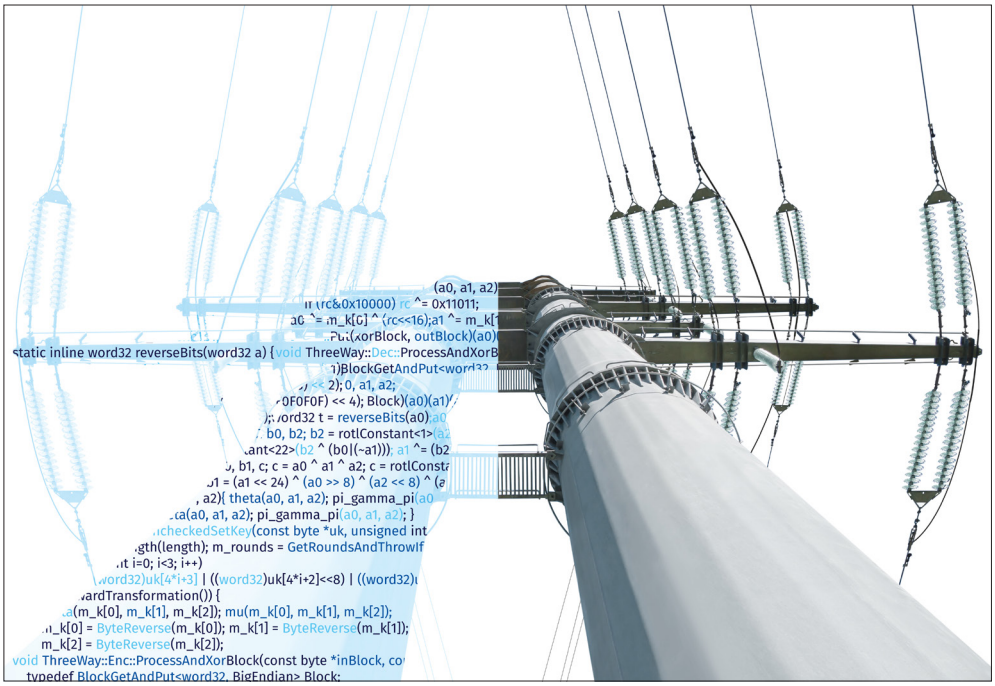
Solar's growing cyber challenge

DNV's latest *Energy Transition Outlook* forecasts that 69% of grid-connected power generation will be from solar and wind in 2050, and that global installed solar capacity will double by 2025 and quadruple to 3,000GW by 2030. Solar PV cybersecurity therefore becomes part of the climate change discussion given the role the sector will play in decarbonising energy. The more critical it becomes to the world's energy systems, the greater target it presents to cyber criminals.

As the frequency and consequences of industrial cyberattacks escalate, regulatory oversight of companies with industrial operations will increase. Heightened risk of cyberattacks on critical infrastructure will bring stricter requirements for organisations to demonstrate control of their own and their suppliers' security.

This trend is already in motion. North America has speedily introduced new regulation in response to rising security threats and recent cyberattacks on companies operating critical infrastructure such as the Colonial Pipeline. New measures have included mandates for government contractors to strengthen their networks. Another example is Europe's Directive (EU) 2016/1148 Security of Network and Information Systems, which is being updated.

Industry standards will also become increasingly important. Companies across the supply chain will more frequently need to apply – and demonstrate the application – of standards, guidelines and best practice in designing and operating energy infrastructure that involves communicating and storing data. For example, the ISA/IEC 62443 series of standards provides a



Credit: DNV.

Top-level managers should have a greater focus on what compliance means to reduce the risk to business, DNV says.

flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems. ISO/IEC 27001 standards provide requirements for an information security management system, enabling any organisation to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties.

The essence of ensuring cybersecurity is to assess and mitigate cybersecurity risks related to people, processes, and technology. At DNV, we recommend companies in the solar PV sector to consider four important issues when addressing cybersecurity: budget for cybersecurity; determine your vulnerabilities; maintain focus on your supply chain; and invest in people.

Budget for cybersecurity

With few published accounts of cyberattacks on solar PV infrastructure, it can be tempting for companies in the sector to assume that an attack is unlikely to happen in their own back yard. They would not be alone. Our research suggests that some energy industry companies may be playing 'wait and see' rather than launching long-term strategies and investment to build defence against attacks that could cost them dearly.

However, with life, property, and the environment now firmly at stake, senior management mindsets towards cybersecurity are tangibly shifting. The default position of company boards and c-suites was once to ensure compliance with cybersecurity regulation and standards, then move on to another year. Now, companies increasingly realise that they can still be compliant even if a significant issue is missed in their cybersecurity audit samples. More risk-averse top-level managers are starting to ask what compliance means and whether it earns them a get-out-of-jail card if a severe incident happens. The answer is 'no'. With cyber risk potentially translating into financial and reputational risk, directors will also want to ensure that the company is always aware of its cybersecurity status and constantly informed of the threat landscape and methods of defence against it.

Those responsible for oversight of the cybersecurity of operations and grid connections will come under increasing pressure to assure boards that the organisation is compliant and confidently cyber secure. But they may still struggle to reserve the budgets they need to upgrade their capabilities while large demands are being made on company finances to pay for digitalisation and energy-transition programmes. *The Cyber Priority* found around a third of respondents, on average, indicated that they are underinvesting in their IT and OT security capabilities. In arguing the case for the investment needed, it pays to articulate and demonstrate how cybersecurity can add value by supporting business continuity, license to operate, reputation, compliance and dealing with regulators.

Determine your vulnerabilities

Nearly two-thirds (60%) of organisations with industrial operations are unaware of their technologies' vulnerabilities, according to Gartner's 2021 *Market Guide for OT Security*. The most urgent task confronting energy sector companies is to discover where projects and operations are exposed to threats before hackers do. What is the attack surface and the potential entry points of attacks? By having a clear and complete overview of their environments, companies can prioritise the vulnerabilities and non-conformities they must address to stay confidently cyber secure. It allows them to put the right people, processes and technologies in place to build effective protection.

Knowing your system's weaknesses and vulnerabilities requires, among other things, a detailed, accurate, up-to-date network topology depicting how components interconnect and communicate (see text box, 'The network topology'). The topology should reflect a complete inventory listing of the solar PV IT-OT network, including both the internal local area network (LAN) and connections to the external wide area network (WAN). It should detail what the 'equipment under control' is, and what every server, switch, wireless transmitter (e.g., Wi-Fi router or SAT-COM terminal), PLC/RTU, internet-connected gadget and so on in the network is used for.

Even the running software services and open physical/logic ports on the devices should be scrutinised, assessed and evaluated with critical eyes. Otherwise, assessing cyber risk may focus too narrowly on the confidentiality, integrity and availability of information, without adequately considering consequences related to safety,

The network topology

Typically a drawing, it may include network segments, switches, servers, routers, workstations, laptops, tablets, smartphones communication protocols, type of wired cables used, device specific information like OS version, IP address, MAC address, the number/type of physical ports, etc. and other details. Operational technology includes any software/hardware interacting with sensors, actuators and controllers, such as programmable logic circuits (PLCs) and human-machine interfaces (HMIs). An asset inventory of all hardware (e.g. inverters) and software running on it is also needed. If the topology and/or inventory is likely to change frequently, generating the inventory dynamically can ensure it is always updated when changes occur. If the system is complex, break it down to several network topographies and have these available before calling in cyber experts such as DNV to assist with actions such as risk assessment, gap analysis and penetration testing. These experts can also assist the development of a network topology.

Log4Shell shows supply-chain risk

The widely reported Log4Shell vulnerability for the popular Java programming language exemplifies risk originating in a supply chain. It was discovered in 2021, in a tool used in cloud servers and enterprise software globally, and in both IT and OT. Hackers could remotely exploit it without needing authentication or special access privileges to servers. Energy sector companies quickly patched and created workarounds for Log4Shell and to safeguard their IT and OT environments. But many may have been slower to assure that their equipment vendors and system suppliers were also taking appropriate action.

reliability and productivity of the assets. For example, a fire in a BSS deliberately overloaded by hackers could have safety and environmental effects and damage assets.

Knowing where your infrastructure has physical vulnerabilities is as important as knowing where you are digitally exposed. Hackers have been known to seek physical access to substations, servers and switches to gain control of critical infrastructure. Physical security therefore also needs continuous mapping, checking and improvement. Investing in proper routines and procedures for both cyber and physical security is imperative to any organisation that values its tangible and non-tangible assets.

Maintain focus on your supply chain

Undiscovered vulnerabilities along the supply chain can completely undermine a solar PV operator's in-house cybersecurity effort. *The Cyber Priority* highlights supply-chain blind spots creating cyber risk. Less than a third of energy professionals working with OT say their company invests in cybersecurity of supply chains and equipment vendors. Just 12% with OT rank such oversight as a core area of maturity.

Many energy companies apply industry standards and recommended practices to help ensure cyber-secure OT/IT implementations. For instance, DNV advises operators and supplies on best practice to ensure conformity to IEC 62443 standards.

Cybersecurity of power grid protection devices

DNV Recommended Practice (RP) DNV-RP-0575 is applicable to companies involved in operating, managing and securing existing (second and third generation) substations. The RP describes 45 risk-reducing measures, covering people, processes and technology, to minimise attack surfaces and counter threats to power systems. These measures are based on a comprehensive review of current EU and US legislation, and currently applicable standards and guidelines on cybersecurity in operational technology. The RP is free to download from the DNV website.

Accurate cyber risk assessment across the solar value chain is also needed to write adequate cybersecurity requirements into contracts with suppliers and subcontractors.

At DNV, we recommend that supply chain audits and vendor cybersecurity requirements are implemented during procurement, installation and operation of equipment, systems and software. Getting a comprehensive view of internal and external risk includes assessing cybersecurity service vendors and cyber risk from other product/service vendors, including systems as highlighted in the 2022 cyberattack incident in Germany (see Table 1). Vendors should also assess their cybersecurity risk to customers.

Regulatory change and lack of common regulations and standards mean energy industries need internal and/or external experts who can anticipate and keep up with what is happening. Closing off cyber vulnerabilities requires cybersecurity leaders with holistic understanding of IT, engineering, health, safety, environment and quality, in the organisation and the specific industry.

Similar considerations apply when assessing other vendor types. DNV has deep knowledge of these through its long record of providing domain-specific cybersecurity verification services for third-party suppliers' components in energy infrastructure. This has involved simulating cyberattacks on converging OT and IT environments to assess for vulnerabilities.

Vendors must also protect themselves and their customers; for example, by knowing what cybersecurity measures are needed to comply with when tendering for or working to contract. Vendors should know if they can comply with terms and conditions agreed with customers, whether they are doing so and, if not, what they are doing about it. Otherwise, a vendor could be exposed to significant liabilities. Vendors should also ask what their approach to cybersecurity says to existing and potential customers about a vendor's cyber vulnerabilities and trustworthiness on other security issues such as data or commercially sensitive documents.

Invest in people

A company's workforce is the first line of defence against cyberattacks. Encouragingly, 78% of energy professionals report their organisation making education/training a priority in cybersecurity budgets. However, when asked where their organisation is most mature in its cybersecurity, they cited upgrades to core IT systems and software (59%) more than training (41%) or introducing cybersecurity expertise (25%). Only 31% of energy professionals are confident they know exactly what to do if they were concerned about a potential cyber risk or threat on their organisation.

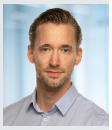
One explanation for these findings is that businesses had to focus on widespread, urgent upgrades (e.g., patches and firewalls) to existing and aging technology infrastructure to block hackers. The industry now needs to invest more evenly across the people and technology disciplines of cybersecurity. Companies should not cut investment in technology upgrades, but need to expand workforce training while exploring what specialist knowledge needs bringing in.

For robust cyber defence, businesses also need deep understanding of each energy domain, whether solar, wind, nuclear, or oil and gas, and assurance that cyber processes will not impact production or their long-term goals around the energy transition. The cyber vulnerabilities of IT and OT environments need understanding both separately and in combination, and always in the relevant industrial context. ■

References

1. 'Germany unveils plan to tackle cyberattacks on satellites', theregister.com, 5 July 2022
2. 'Hackers breached Colonial Pipeline using compromised password', bloomberg.com, 4 June 2021
3. 'First-of-a-kind U.S. grid cyberattack hit wind, solar', governorswindandenergycoalition.org, 3 November 2019
4. 'Cyber attack on Kudankulam nuclear power plant – A wake up call', PK Mallick, Publ. Vivekananda International Foundation, 2019, ISBN: 978-81-943795-2-2
5. 'Russian hackers tried to bring down Ukraine's power grid to help the invasion', MIT Technology Review, 12 April 2022, www.technologyreview.com

Author



Alex is a cybersecurity engineer with a master's degree in ICT with specialisation in cybersecurity from the Norwegian University of Science and Technology (NTNU). His work involves improving cyber-resilience of industrial control systems within different sectors including power and renewables, oil and gas and maritime. Alex has performed multiple onshore and offshore security testing and verification assignments, including windfarms, hydropower plants, cruise ships and drillships, and other critical infrastructure for global companies.