
TXOne Networks
2022
/Q2
Cyber Safe
Green Energy
txOne networks

TXOne Networks

Cyber Safe
Green Energy

txOne networks

Cyber Safe
Green Energy

01 Executive Summary

Green energy systems must be safeguarded all day, every day. From solar panels, wind generators, or geothermal plants through the power grid to your electrical outlet, real-time cybersecurity is needed for the facilities that generate, transmit, and distribute electricity. Once, the power grid only needed to cover the generation of power at large, centralized plants and its distribution to industry, offices, and homes. In contrast, modern smart grids and microgrids allow anyone to generate and distribute energy. This creates on-ramps to the power grid that attackers will exploit.

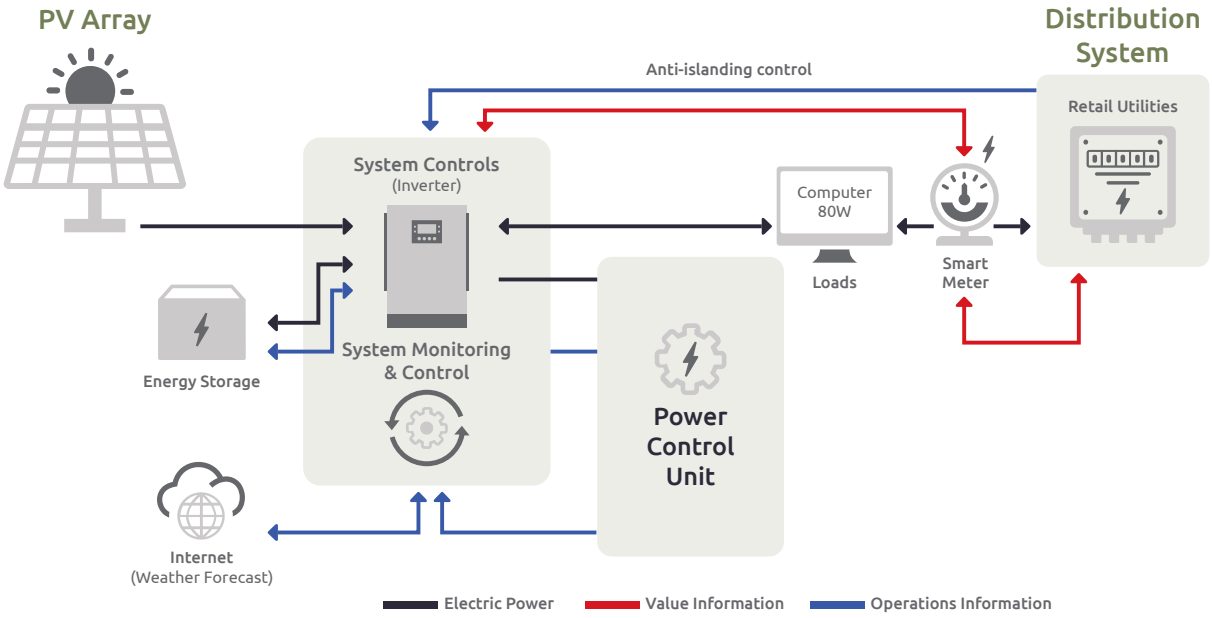
Smart power grids run on a constant feedback loop of generating, buying, selling, and delivering electricity, and must be able to accommodate both modern and legacy systems. Modern home-owners can even install their own solar panels or windmills to power their homes, and then sell their extra electricity back to the grid with one of the bidirectional meters that are now common to the energy sector. These bidirectional electrical meters add a tremendous amount of convenience for operators, but can turn into a force of disruption when targeted by hackers. Once an electrical system is compromised, attackers can carry out a wide range of malicious actions, including damaging equipment, endangering personnel, or even disrupting power delivery.

Any successful organization in today's world can expect attention from cyber criminals, but energy organizations face additional cyber risk from state-employed actors engaged in cyber espionage. While cyber criminals will take control of operational assets and then demand a ransom for their return, attackers conducting cyber espionage are solely focused on disruption. According to the director of Horizon Digital Economy Research and professor at the University of Nottingham, Derek McAuley, ***"The danger to life is significant ... if hackers take control of all the smart meters within a 100-mile radius of Cambridge, for instance, [they] could cause as much damage as bombing a power station."***[1]

[1] *Jim Mortleman, "Secure IoT Before It Kills Us", ComputerWeekly.com, Jan 9 2017.*

02 Where Are the Weak Links?

The following diagram shows key components of a solar energy system. All devices in this system could be affected by previously-discovered vulnerabilities or even a new vulnerability straight from the latest threat advisory.



One vulnerable component is the inverter, which acts as the interface between solar panels and the electric power grid. If attackers compromise the inverter's control software, they may inject malicious commands or modify data. They could change the power delivery schedule, take over grid control devices, shut down power, destroy property, or even endanger human lives.[2]

Bidirectional meters that allow net metering are an extremely appealing target for attackers. If the system produces more energy than it needs to meet demand, then it sells electricity to the power grid. Hijacking this buying and selling process in stealth mode could siphon your profits. Attackers are busy targeting various types of billing systems.

[2] *The Office of Energy Efficiency and Renewable Energy, "Solar Cybersecurity Basics", Accessed Apr 19 2022.*

The attack on a well-known pipeline company started with their billing system, then spiraled out of control, ultimately causing the pipeline to be shut down and a state of emergency to be declared in the eastern USA.

In order for the grid to stay balanced and secure so that electricity flows where it is needed and technicians can work safely, vulnerabilities must be addressed. Some modern assets can be patched during routine maintenance but many mission-critical assets cannot. Asset shields include virtual patching to make sure all your systems are safe even though a vendor may not have developed a patch yet. This line of defense empowers your round-the-clock operation allowing you to meet strict production schedules required to keep the lights on.

03 Case #1: The sPower Denial of Service Attack

In March 2019, sPower became the center of the first cyber incident to ever cause a United States power grid operator to lose connection to its power generation installations.[3] Attackers exploited an unpatched firewall that was intended to protect the sPower microgrid, causing a series of reboots over 12 hours and ultimately resulted in a denial of service (DoS) attack that flooded the system with busy work, making it unavailable to do real work as the firewall rebooted over and over again, unable to secure network traffic. sPower lost control of visibility into their systems across California, Utah, and Wyoming.[4]

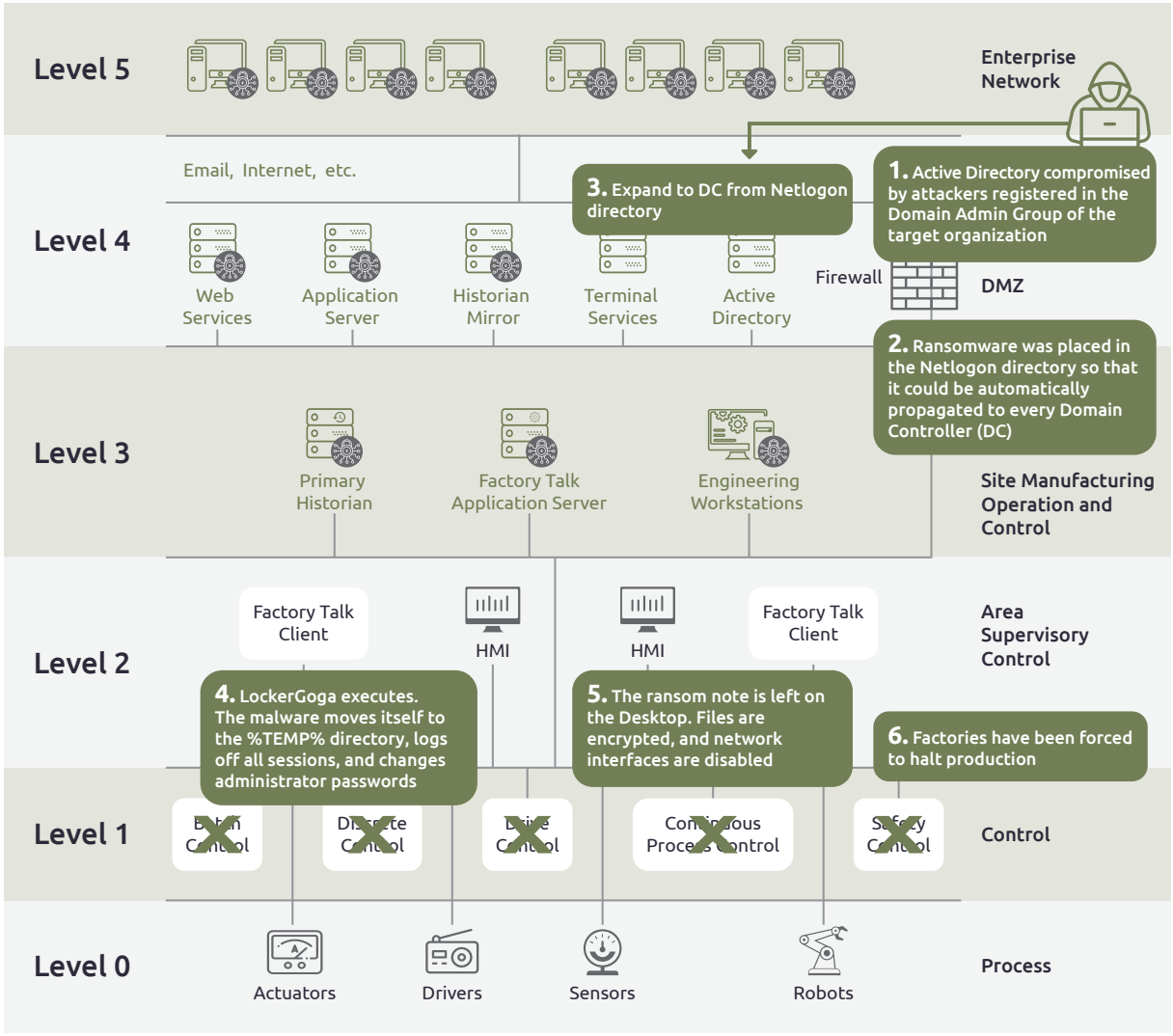
04 Case #2: The 2019 Norsk Hydro Attack

On March 19, 2019, the team at renewable energy and aluminium provider Norsk Hydro found a short note waiting on their desktop: ***Greetings! There is a significant flaw in the security system of your company… Your files are encrypted. We exclusively have decryption software...(send) payment...in Bitcoin...***

That fateful day, Norsk Hydro discovered that hackers had compromised their Active Directory and used it to run amok. The attackers had registered themselves in the Domain Admin Group and used their newly-acquired privileges to copy LockerGoga malware to the Netlogon folder, resulting in it being automatically propagated to every domain controller. As the malware spread, it faced few challenges to its expansion – many firewalls even accept Active Directory information by default.

LockerGoga quietly moved itself into the %TEMP% folder in order to hide its tracks, then used the Windows native tool 'logoff.exe' to log off all sessions other than its own. With everyone else logged off, it reset the password for every account on the system, including administrator accounts, and then encrypted system, data, and program files. Finally, LockerGoga left the network interface for every system disabled and a ransom note on the desktop.

[3] *Catalin Cimpanu, "Cyber-attack hits Utah wind and solar energy provider", ZDNet, Nov 1 2019.*
[4] *Robert Walton, "First cyberattack on solar, wind assets revealed widespread grid weaknesses, analysts say", Utility Dive, Nov 4 2019.*



The infection hit more than 22,000 computers spread throughout more than 170 work sites, with both IT and OT massively infected. Many factories were forced to halt production and Norsk Hydro's logistics were sent into a tailspin, leading to losses of more than $40M in the first week after the attack, but the Norsk Hydro team sent a clear message – "No, we do not pay ransoms" – and then bit the bullet and rebuilt their systems.

05 Regional Leaders in Green Energy Cybersecurity

As of this writing, the Nordic region and Chile are leaders in providing cyber safe green energy, including solar, wind, and geothermal. Their governments have developed standards to bring oversight and consistent cybersecurity policies.

Green Energy in the Nordic Region

The Nordic region includes Denmark, Finland, Iceland, Norway, Sweden, Greenland, the Faroe Islands, and Åland. Together they have a vision of being the most sustainable and sustainably integrated region in the world by 2030. They are actively working together to establish energy policies that include cybersecurity considerations that can safeguard their joint electricity market. They plan to link more systems, to integrate areas outside of the central Nordic energy grid including Greenland, the Faroe islands, and Aland, and to contribute green energy to the European Union. In November 2021, the Nordic countries pledged to follow a "mutual defense" policy for cyber attacks – a cyber attack against one Nordic country, will be seen as an attack on all of them.[5]

Green Energy Powers Opportunity

There are several reasons why green energy is important to the Nordic region. These countries are located near the Arctic, a region which has some of the highest per-capita energy consumption in the world. That electricity is used to heat homes and water during the long, cold, and dark winters and to support a host of energy-intensive industries. By leveraging their abundant natural resources, Nordic countries have been able to base their electricity production primarily on renewable energy sources.[6]

This region's ability to generate affordable, reliable green energy is critical to its industrial development. The situation in the Nordic countries is evolving as ice melts due to climate change and resources including iron ore, lead, zinc, diamonds, gold, copper, uranium and oil become more

[5] *Lisbeth Kirk, "Nordic parliaments agree mutual defence on cyberattacks", EU Observer, Nov 5 2021.*
[6] *NASA Earth Observatory, "Nordic Lights", Accessed Apr 19 2022.*

accessible, creating new business opportunities.[7] Furthermore, countries with rights to explore and to use marine resources have committed to working towards establishing commercial activity in this region.[8]

The Nordic countries must support advanced industry and also many day-to-day lives fully reliant on a continued supply of affordable electricity. Bad actors in criminal organizations seeking to extort as much money as possible or in the employ of hostile state actors seeking to maximize disruption will be eager to hold energy providers and their customers hostage.

Nordic Cybersecurity Regulations

How the Nordic electricity market develops will depend on the energy producers, consumers, transmission system operators (TSOs) responsible for the high voltage network, national regulatory authorities (NRAs), and the power exchanges. Currently, these parties work together at the annual Nordic Electricity Market Forum. In 2018, this forum decided that their vision for their electricity market included cyber-defenses as a high priority.

The Helsinki Treaty governs how Nordic countries cooperate with each other. It established the Nordic Council which has no formal power, but decisions made by the Council are implemented by each country through its legislature.[9] In 2021 the Nordic Council recognized cyber-defense as an important goal for green energy, healthcare, and transportation, and since then cyber experts in these sectors have investigated best practices published by the National Institute of Standards and Technology (NIST), the Cybersecurity Capacity Maturity Model (CMMC), the European Union Agency for Network and Information Security (ENISA), among others. They developed the Cybersecurity Capacity Maturity Model for Nations (GCSCC). It provides guidance for cybersecurity policies and strategies through four objectives: awareness, collaboration, monitoring, and support. Using this umbrella guidance, each country develops a national strategy for each sector along with supporting materials and threat assessments.

[7] *David Nikel, "What's So Great About Greenland? Why Trump Wants It And Why Denmark Won't Sell", Forbes, Aug 16 2019.*
[8] *The Office of the Press Secretary, "FACT SHEET: U.S.-Nordic Collaboration on Climate Change, the Arctic, and Clean Energy", The White House, May 13 2016.*
[9] *Kasper Paulig, "Nordic agreements and legislation", Nordic Co-operation, Accessed Apr 19 2022.*

The Nordic countries collaboratively monitor their strategies and share information collaboratively. Nordic ministers agree on goals, each member of the Nordic ministry passes laws that create standards, and finally they collaborate and share information towards continual improvement. This results in similar electricity regulations from country to country within the Nordic group.[10]

Green Energy in Chile

The National Electric System of Chile (Spanish acronym: SEN) was created in 2017 to unify production of electricity.[11] SEN coordinates everyone in Chile who produces or distributes electricity, covering over 36,000 kilometers of electrical lines and generating electricity for 98.5% of the national population. The following chart shows types of green energy production compared, including hydroelectric, thermal, wind, solar, and geothermal.

In October 2020 the coordinator of the National Electric System in Chile published the ***Standard for Cybersecurity in the Electricity Sector***. Growing inter-connectivity and dependency on the internet has increased the risk of cyber attacks. Instrumentation and control must be protected in order to reliably produce green energy. Both IT and Operational Technology (OT) must be secure because without controls, the door is open for attacks on ICS assets, protocols, control commands, data, and other assets.

[10] The Nordic Council of Ministers, "Nordic eHealth Benchmarking", May 28 2020.
[11] Coordinador Electrico Nacional, "Sistema Eléctrico Nacional", Accessed Apr 19 2022.

Comparison: The NERC CIP, Chile, and the Nordic Region

NERC CIP Reliability Standard	ENISA National Capabilities Assessment Framework – Nordic States in EU	Chilean Standard for Cybersecurity in the Electricity Sector	OT Zero Trust Capability
CIP-002-5.1a Cyber Security - Bulk Electric System (BES) Cyber System Categorization groups cyber assets into BES Cyber Systems so that protections can be applied to groups that could not be applied to an individual asset. It also creates "bright-line" criteria (High - 3000 MW and Medium - 1500 MW) for categorizing BES Cyber Systems based on the impact if they were destroyed, degraded, misused, or otherwise rendered unavailable for more than 15 minutes.	**Section 2.2** 3. Secure digital identity	**Section 7.1** discusses the details of categorizing SEN cybersystems based on high, medium, or low impact.	**OT Zero Trust** protects all systems, no matter how large or small.
CIP-003-8 Cyber Security - Security Management Controls addresses planning and organizing sustainable cybersecurity controls that establish responsibility and accountability for protecting BES Cyber Systems. Controls include organizational controls, operational controls, and procedural controls. The goal is to mitigate risks and to create a “culture of cybersecurity”. Such a culture streamlines compliance with laws, regulations, and standards.	**Section 2.2** 2. Establish baseline security measures	**Section 7.2** addresses security management controls. Controls include organizational controls, operational controls, and procedural controls.	**OT Zero Trust** checks the box for operational and procedural controls. It was designed with compliance in mind. OT Zero Trust features 4 cornerstones: network zero-trust zones, trust lists, device inspection, and virtual patching.
CIP-004-6 Cyber Security - Personnel & Training brings awareness to personnel. It also permits risk assessment for insider attacks.	**Section 2.2** 5. Raise user awareness 7. Strengthen training and educational programmes	**Section 7.3** addresses training your team so they understand the importance of following cybersecurity policies and know how to keep themselves and their workplace safe.	**OT Zero Trust** makes it easy to setup up a training or testing environment.

NERC CIP Reliability Standard	ENISA National Capabilities Assessment Framework – Nordic States in EU	Chilean Standard for Cybersecurity in the Electricity Sector	OT Zero Trust Capability
CIP-005-6 Cyber Security - Electronic Security Perimeter (ESP) controls access to BES Cyber Systems through networks. Key defenders include the Electronic Access Point (EAP) and firewall. Remote access including dial-up must be guarded for both inbound and outbound communications. Multi-factor authentication is recommended for logging on and there should be more than one method for disabling remote sessions.	**Section 2.2** 2. Establish baseline security measures	**Section 7.4** maps to CIP-005. It essentially calls for trust-listing to control both inbound and outbound network traffic including remote access and dial-up connections.	**Network Segmentation** is the practice of dividing your network into segments, sometimes called 'zones'. Only messages from trust-listed devices can enter a zone. Once inside, only trustworthy messages can be sent outside. You can set up more than one zone and create a maze for attackers to navigate before reaching your most critical operations.
CIP-006-6 Cyber Security - Physical Security of BES Cyber Systems includes the plan to secure physical access to cyber assets.	-	**Section 7.5** follows CIP-006 in securing cyber-physical security systems.	Outside vendors should never be allowed to access your devices using unscanned media. Sometimes anti-malware software cannot be installed due to performance concerns or industry regulations. You may not have internet access to download virus signatures or malware pattern files. **OT Zero Trust device inspection** relies on a portable security device that scans for and wipes malware from air-gapped systems and stand alone PCs.

NERC CIP Reliability Standard	ENISA National Capabilities Assessment Framework – Nordic States in EU	Chilean Standard for Cybersecurity in the Electricity Sector	OT Zero Trust Capability
CIP-007-6 Cyber Security - System Security Management shields assets from attack. To guard your systems: deploy methods to deter, detect, or prevent malicious code, close ports, install security patches, log and review cyber-events, generate alerts, enforce authentication, change passwords, implement mitigation plans, and stay informed. Evaluate your patch management system at least once a month and revise your mitigation strategies. Identify individuals who share accounts and create individual accounts where possible. Enforce password length and complexity and regular changes. Limit the number of unsuccessful authentication attempts. Stay informed as new cyber-defenses are invented.	**Section 2.2** 3. Secure digital identity and build trust in digital public services 12. Address cyber crime (III)	**Section 7.6** Security Management Systems contains tables that identify security controls matching CIP-007 along with examples of methods for providing cybersecurity. **Table CIP-007 R1 Ports and Services** – close un-used ports and protect against physical access via removable media **Table CIP-007 R2 Administration of Security Patches** – track and test security patches before installing them. Check for new patches at least once every 35 days. If a patch cannot be applied then create a mitigation plan to guard against vulnerabilities. **Table CIP-007 R3 Detecting malicious code** - implement controls to detect and, if possible, prevent malicious code. **Table CIP-007 R4 Monitoring cybersecurity events** - log cybersecurity events including the success of the attack, the type of breach, and the malware. Generate alerts. Retain records for 90 days. Review a summary or a sample of login events at least every 15 days to identify undetected incidents **Table CIP-007 R5 System access control** – record your rationale for allowing access and maintain a list of users. Establish a password policy: at least 8 characters or the maximum length supported by the cyber asset and at least three different character types (or the maximum supported by the cyber asset). Force password changes at least every 15 months. Limit the number of failed attempts and generate alerts after a certain number.	**OT Zero Trust** brings a new idea about the trustworthiness of equipment. Your machines only receive messages that are **trust-listed** because these are the only messages that the firewall will allow. Your network is constantly monitored by intrusion protection devices. These are smart security devices used to divide your network into network zero trust zones. Messages may only pass through checkpoints on a “need-to-know” privilege. **Virtual patching** makes sure that BES cyber systems are guarded by the most recent signature patterns. Modern machines and devices are guarded. Legacy assets are locked down. Air-gapped devices are inspected and protected. You can watch all these security controls using one console. As cyber-events unfold, you get real-time alerts about any breaches. This bird’s-eye view also shines a light on shadow OT, rogue equipment installed by your workers that can jeopardize your security. When a cyber incident occurs, OT Zero Trust tools create logs and streamline log analysis.

NERC CIP Reliability Standard	ENISA National Capabilities Assessment Framework – Nordic States in EU	Chilean Standard for Cybersecurity in the Electricity Sector	OT Zero Trust Capability
CIP-008-6 Cyber Security - Incident Reporting and Response Planning will save valuable time when an attack occurs. Develop reporting criteria. Assign roles and responsibilities to your response team. Write incident handling procedures. Train your team and test your incident response at least once every 15 months. If your team has not responded to a cyber-event during that time then conduct a paper or tabletop drill or an operational exercise. Within 90 days of an incident, document the lessons learned, update your response plan, notify your team of these updates including the impact of the attack, the attack vector, and the level of intrusion.	**Section 2.2** 4. Establish an incident response capability (II) 13. establish incident reporting mechanism (III)	**Section 7.7** aligns with CIP-008 for incident reporting. Identify, classify, and respond to incidents. Review and update your incident response plan every 15 months. Test the plan by responding to a real incident, conducting a table top simulation exercise or undertaking an operational exercise. Document your lessons learned for continual improvement. Maintain a log of incidences. Cyber-event notifications should include: functional impact, attack vector, level and success of intrusion. Ensure that notification occurs within one hour of determining that an incident should be reported. Provide updates within 7 days.	**OT Zero Trust** logs provide valuable "real-world" data facilities use to improve oversight and eliminate the shadow OT. Logs can be backed up as long as necessary and easily be searched or referenced from a centralized console.
CIP-009-6 Cyber Security - Recovery Plans for BES Cyber Systems are the key to maintaining ongoing operations. Create backup and recovery procedures that include verifying the restoration. Assign roles and responsibilities to the recovery team. Find ways to preserve your data. Test your recovery plans every 15 months with a current and representative sample of data.	**Section 2.2** 1. Develop national cyber contingency plans 6. Organise cyber security exercises	**Section 7.8** addresses recovery plans in CIP-009. Verify the success of your recovery procedures. Plan to preserve data for forensic analysis. Use a sample of representative for table top drills or exercises every 15 months. Test and update the plan every 36 months. Update the recovery plan after an incidence to reflect the lessons learned.	**OT Zero Trust** focuses on real-time protections. Allow lists and trust lists must be included in backup and recovery procedures. Cyber event logs may be archived for forensics analysis.

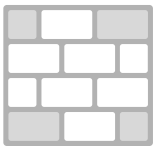
NERC CIP Reliability Standard	ENISA National Capabilities Assessment Framework – Nordic States in EU	Chilean Standard for Cybersecurity in the Electricity Sector	OT Zero Trust Capability
CIP-010-3 Cyber Security - Configuration Change Management and Vulnerability Assessments are helpful in spotting zero-day attacks. They are also a second line of defense should primary controls fail. Create a baseline that includes the operating system, apps, custom software, network ports, and security patches. Verify the software source and integrity for patches and upgrades. Test changes before installing them. Prior to adding new cyberasset perform an active vulnerability assessment. Monitor changes to the baseline once a month. Review vulnerabilities every 15 months. Perform active vulnerability assessment in your test environment and document results every 36 months.	**Section 2.2** 10. Improve the cybersecurity of the supply chain	**Section 7.9** follows CIP-010 and recommends configuration change management standards and vulnerability assessment. The change management system must be smart enough to capture a baseline and monitor subsequent changes against that baseline. A baseline configuration includes: operating systems and firmware, open-source software, software personally installed, open ports, and security patches. The system must also verify the impact of any planned changes to the baseline by testing them. This section includes the requirement to evaluate and develop a plan to mitigate vulnerabilities and to manage transient cyberassets.	**OT Zero Trust** methods are constantly being assessed for vulnerabilities and fine-tuned to stay ahead of attackers.
CIP-011-2 Cyber Security - Information Protection makes sure attackers can not find the secrets that are hidden in your data. Identify and protect BES information. Sanitize or destroy media that contains BES data.	**Section 2.2** 11. Protect critical information infrastructure, OES, and DSP (III) 14. Reinforce privacy and data protection (III)	**Section 7.10** describes information protection also in CIP-011. It requires identifying, classifying, and protecting information during transit and while in storage. Prior to disposal or release for re-use power producers must ensure that information has been properly destroyed.	**OT Zero Trust** device inspection empowers you to inspect all inbound and outbound devices. Stop malware before it walks through the door.
CIP-013-1 Cyber Security - Supply Chain Risk Management addresses the risk posed by working with vendors. Identify and categorize cyber-risks resulting from procuring and installing equipment and software. Consider what may happen when you change suppliers. Verify vendor software integrity and authenticity. Investigate their disclosures of known vulnerabilities. When cyberevents occur, notify vendors and coordinate your responses.	**Section 2.2** 10. Improve the cybersecurity of the supply chain (II)	**Section 7.11** enforces cybersecurity for communications between control centers with a focus on mitigating risks of unauthorized disclosure or modification of real-time data being communicated between control centers.	With **OT Zero Trust**, prevent supply chain attacks from threats hidden in inbound devices by scanning all inbound assets. Document scan records on a central management console for easy reference. Stop supply chains hidden in updates with application trust listing - updates can only run after being approved by an administrator.

NERC CIP Reliability Standard	ENISA National Capabilities Assessment Framework – Nordic States in EU	Chilean Standard for Cybersecurity in the Electricity Sector	OT Zero Trust Capability
CIP-012-1 Cyber Security - Communication between control centers is not currently enforced. However, more and more systems are inter-connected so it is important to assess and to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers. Identify security protections. If the Control Centers are owned or operated by different Responsible Entities, identify the responsibilities of each. Work with a Compliance Enforcement Authority (CEA) as they monitor and enforce compliance. The CEA may be NERC, a Regional Entity, or any entity designated by an applicable government authority. Keep evidence that demonstrates compliance for the required retention period.	**Section 2.2** objectives that may be related depending on who owns and operates the control centers 15. Institutionalise cooperation between public agencies (IV) 16. Engage in international cooperation (IV) 17. Establish a public-private partnership (IV)	**Section 7.12** aligns with CIP-013. Assess the cybersecurity risks of buying products from manufacturers or services providers. Think about what will happen when you transition from one manufacturer to another. When an incident occurs: notify your supply chain and coordinate your responses. Stay aware of remote or local access by vendors. Check the integrity of software patches. Grant access only as needed.	**OT Zero Trust** delivers real-time monitoring of network traffic from all outside sources including between control centers. Machines only receive messages that are trust-listed behind a firewall. Your network is constantly monitored by intrusion protection devices.

References:
https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Glossary:
NERC CIP - North American Electric Reliability Corporation - Critical Infrastructure Protection

06 The Four Cornerstones of OT Zero Trust for Green Energy



In order to protect green energy systems, you must safeguard every vulnerable opening to your network and your endpoints. In addition to the facility's network security concerns, each asset has many points of attack by which attackers will attempt access. This includes at least one physical port and one or more logical ports, and with so many active layers of connections running between assets as they carry out operations, not only cybersecurity but even just creating visibility for proper oversight can seem overwhelming.

Not only that, but in an environment running a mix of legacy and modern assets from different vendors, some assets may have specialized needs, such as security for their unpatched vulnerabilities. Even air-gapped systems, once thought impenetrable, are only as secure as the work site itself – if employees can freely take unsecured USBs, laptops, or other devices in and out of the work site, this creates an exponentially higher risk of insider threat. Similarly, onboarding assets must be checked! The OT zero trust approach offers a reliable, cost-effective way to improve security and streamline maintenance, even in environments running thousands of highly varied assets, which is why many world leaders in green energy innovation and production are already using it to prevent cyber incidents at their facilities and ensure operational integrity.

Security Inspection

Scan all inbound devices brought on site by personnel to stop insider threat, and scan assets before onboarding to prevent supply chain attacks.

90 days

TXOne's threat specialists recommend keeping scan logs for a general minimum of 90 days, and for mission critical assets a minimum of 180 days.

Trust Lists

Trust lists secure endpoints and networks alike by specifying what is allowed and blocking everything else.

Network Segmentation

Network segmentation groups vulnerable assets into operations-friendly safe zones, preventing attackers from moving and malware from spreading.

80 sec.

Malware can strike as fast as it can appear - after file landing, the REvil ransomware only needs 80 seconds to encrypt a typical Windows system and post a ransom note.

Asset Shielding

Shield assets at a network level to secure vulnerabilities in legacy and other unpatched assets without interrupting their work.

Security Inspection

The first cornerstone of OT zero trust is **security inspection**, because it's the first thing that should happen for any device or asset that enters a facility. This means implementing a scan procedure for every device that enters the work site, either brought by personnel or for onboarding, to fend off hackers who will steal trust from employees or 3rd-party technicians to get threats into OT environments. Malware can be hiding in assets arriving for onboarding (a supply chain attack) as well as in devices being brought on-site by personnel (insider threat), both of which can lead to devastating cyber incidents.

Attackers can impact thousands of companies overnight by hiding malware in an asset before the vendor ships it. For an organization high up on the supply chain, this could cause a catastrophe as hackers take advantage of that organization's trust to hit every link of the chain. A quick scan before onboarding is the only way to catch this kind of threat. For equipment manufacturers, outbound device shipments can also be scanned to protect them being the central hub of a reputation-searing supply chain attack.

Unsecured USBs or laptops brought on-site by employees have been a major factor in many high-profile cyber incidents. Intentionally or unintentionally, trusted personnel are one of the most common ways that threats get into facilities today - and this is put completely under control by using a handheld quick-scan device to make sure nothing they're bringing in has a threat on it.

To fulfill this cornerstone, we recommend setting up a checkpoint that is equipped to quickly conduct and log the results of malware scanning and removal for all equipment entering the facility. It's likely that in the near future vendors will need to take a more standardized and rigorous approach to guarantee their products are secure, but until that day every OT organization must take this matter into their own hands.

Security inspection does have one more very powerful benefit, by which it can tremendously ease the hard work of complying with regulations such as the ***NERC CIP*** or ***The Chilean Standards for Cybersecurity in***

the Electricity Sector. By integrating the processes of asset scans and inventories, security teams can verify scan completion, ease audits, and track the vulnerability status of each asset. By conducting these scans with a portable device that can be taken from asset to asset by personnel, even asset scans of stand-alone and air-gapped systems can be tracked from one centralized console.

Trust Lists

The second cornerstone is **trust lists**. With trust listing, you deploy a virtual security guard who can secure networks and endpoints alike by specifying which actions, assets, applications, or users are allowed and blocking everything else. It's critically important to OT defense to shelter each endpoint's specialized needs, covering fixed-use legacy systems as well as the flexible modernized assets that handle a variety of tasks. Furthermore, one aspect that is sometimes overlooked at the design phase is how the security team will have oversight of such different assets – legacy and modernized assets are often secured with two separate solutions, which confuses asset ownership and maintenance. Instead, our specialists recommend endpoint protection that gives defensive oversight of these varied assets in the same centralized overview on a single pane of glass.

Fixed-use assets usually only have more clearly-defined and predictable responsibilities, so we can use the most straightforward kind of trust list to lock down their applications, configurations, data, and USB ports. This ensures that unauthorized applications can't execute, and only trusted users and applications can make changes to configurations or data. Because of their straightforward nature, trust lists customized to fixed-use endpoints take few operational resources to provide reliable defense.

For modernized assets, which usually need more resources to flexibly conduct a wider variety of tasks, this kind of "straightforward" trust list used with fixed-use assets is no longer effective. Instead, we recommend managing application trust with an application trust library of common OT and ICS applications and certificates. This allows the intelligent identification of mission-critical processes so that relevant applications

can be excluded from next-generation antivirus scans and always given the priority necessary to do their work, ensuring fast operation and resource availability for necessary tasks. However, these modernized assets also need one more layer of endpoint protection, which comes in the form of machine learning that can spot suspicious activity without interrupting trust listed processes.

As the Kaseya VSA supply chain attack of 2021 showed nearly 1,500 companies, it can be incredibly difficult to stop malware that's hidden in a trustworthy-seeming update from a vendor. Application trust lists stop updates from running until an administrator has scanned, approved, and scheduled them, protecting your environment from supply chain attacks hidden in updates.

At a network level, trust lists can also disallow certain commands or accesses. Disallowing specific commands requires an OT-native appliance that can understand the protocols that are in use, and prevents hackers from sending malicious commands both by strictly limiting privileges and by setting suspicious or unusual commands to be blocked by default. This approach works best with network segmentation, where these privileges can be defined by zone to cater to the specialized needs of each asset.

Network Segmentation

Segment your OT network into more easily-defended zones based on which assets do or do not need to communicate. Using OT-native solutions, use protocol-based policies to specify approved commands and IP-based policies to determine which assets can communicate with each other. Command-level policy can prevent misoperation in addition to malicious traffic as long as they can understand the OT protocols that the work site's assets use.

The fundamental tools of network segmentation are IPS and firewall appliances. A next-generation IPS micro-segments critical assets or groups of assets that require 1-to-1 protection, while next-generation firewalls transparently create segmentation and broader definition of network security policies. Work site-friendly "OT-native" IPSes and

firewalls can be deployed transparently without changes to existing architecture. We recommend conducting micro-segmentation using trust lists set at both the network level and at the protocol level.

Network segmentation informed by OT zero trust allows for isolating or aggregating vulnerable assets into a safe zone that is more easily kept away from zero day attacks and other dangerous cyber threats. In some cases, such assets play an important role in the production line, so taking them off the grid is not allowed even when there is risk exposure – but a network segmented with OT zero trust-based policies prevents attackers from traveling within your network and puts a stop to the spread of malware, securing high-risk machines.

Asset Shielding

Updating assets depends on a lot of factors. Is the patch available? If it's available, is it compatible? Does the OT environment allow for the asset to be patched? Asset status and patch status are constant considerations within the maintenance process. Through asset shielding, one can secure assets without making changes to their configurations regardless of whether or not their creator has released a security update. Technicians use asset shielding to reduce risk until it's the right time for an update and a vendor-supplied patch has been released and tested, or to indefinitely secure otherwise unpatchable legacy assets.

With this approach, mean time to patch (MTTP) is much less of a concern, allowing the security team to safeguard facilities while still giving due priority to production. The OT-native IPSes and firewalls that make this kind of asset-centric cyber defense possible have rule sets specifically designed to repel attacks without forcing endpoints to conduct an update, meaning no system reboots and no production downtime. Engineers can keep assets operational and secure while they prepare the patch for deployment during a scheduled maintenance window.

07 Conclusion

By securing green energy facilities with the OT zero trust approach, work sites are more reliably defended while production goals are maintained. TXOne's solutions are already creating dependable cyber safety, streamlining maintenance, and making compliance with regulations more achievable for worldwide leaders in green energy.

You can trust the 4 cornerstones of OT zero trust: security inspection, trust lists, network segmentation, and asset shields. TXOne Networks' Trend Micro Portable Security 3, developed in collaboration with our parent company Trend Micro, ensures that all your devices, including stand-alone or air-gapped devices, are malware-free, and creates a centralized, easily-referenced asset inventory while it works. Stellar secures legacy and modernized assets while still maintaining high resource availability, then allows you to view and manage them all from a single pane of glass. Finally, EdgeIPS, EdgeIPS Pro, and EdgeFire prevent the spread of malware, stop hackers from moving laterally, and inspect every message flowing through your network to make sure your machines and your team receive proper work instructions.

As electrical systems become more interconnected and automated, the disastrous potential of their misuse in the hands of hackers will increase. TXOne's OT zero trust is one way we can rise to this challenge and dependably secure facilities against the cyber attacks of today and tomorrow.

Appendix A

Common Vulnerabilities and Exposures (CVE) is a database of vulnerabilities. Those targeting inverters include:

CVE-2019-19229 *admincgi-bin/service.fcgi on Fronius Solar Inverter devices before 3.14.1 (HM 1.12.1) allows action=download&filename= Directory Traversal.*

CVE-2019-19228 *Fronius Solar Inverter devices before 3.14.1 (HM 1.12.1) allow attackers to bypass authentication because the password for the today account is stored in the /tmp/web_users.conf file.*

CVE-2018-12927 *Northern Electric & Power (NEP) inverter devices allow remote attackers to obtain potentially sensitive information via a direct request for the nep/status/index/1 URI.*

CVE-2018-12735 *SAJ Solar Inverter allows remote attackers to obtain potentially sensitive information via a direct request for the inverter_info.htm or english_main.htm URI.*

txOne networks

txone.com


txOne
networks