GE VERNOVA

# THE FUTURE DIGITAL GRID DEMANDS A ZERO TRUST GRID SECURITY FRAMEWORK



GridOS® Orchestration Software

# INTRODUCTION

Network security is generally described in terms of people, hardware and software technologies, and management processes that combine to protect the integrity, availability, and confidentiality of computer networks. Every computer network, regardless of size or complexity, requires security solutions to safeguard data assets from escalating threats.

Who is behind these cyber threats? The attackers are often described in news reports as an organization's competitors or those attempting to reap financial gain, e.g. with ransomware or by mining cryptocurrencies illegally. However, the number of state actors involved in penetrating operational technology (OT) networks that operate critical national infrastructure such as water treatment, natural gas distribution, and the electric grid is both escalating and escalated by geopolitical tensions.

Little surprise, therefore, that when Moody's studied 70 industry sectors, the top four entities on the list were all utilities because "they often have less advanced cyber risk mitigation strategies, including less developed perimeter vulnerability management programs and less advanced cyber risk management practices."[1] The Electric Power Research Institute reports that the electric grid is attacked 1,200 times per week, increasing yearly.

**The ultimate question becomes: How does a utility protect itself from cybersecurity attacks?**

This paper begins by discussing the cybersecurity threat in the context of electric utilities. It will introduce the framework of Zero Trust cybersecurity principles designed to protect against breaches and offer containment should a breach occur. An in-depth analysis of the strengths and weaknesses of a Zero Trust grid security model will be analyzed for both electric utilities and telcos. The report concludes with essential steps that should be part of any Zero Trust system implementation.

# IDENTIFY THE CYBERSECURITY THREAT

A legacy network security approach erects a protective security perimeter around computer networks and systems within. This security perimeter is often described as a castle with a moat that keeps the attackers away **(Figure 1),** with the metaphorical castle representing the protective "walls" surrounding the network and system that protects data assets within from cyber attacks. All data assets are kept within the castle walls, and once someone (or something) gets inside the castle - past the protective boundary - they are often assumed to be a trusted friend, according to a legacy implicit-trust perimeter security model that can be summarized as "verify, then trust." This model fails to address the trend toward a dispersed workforce, the digital grid, and growing decentralized generation resources and their bi-directional data requirements.

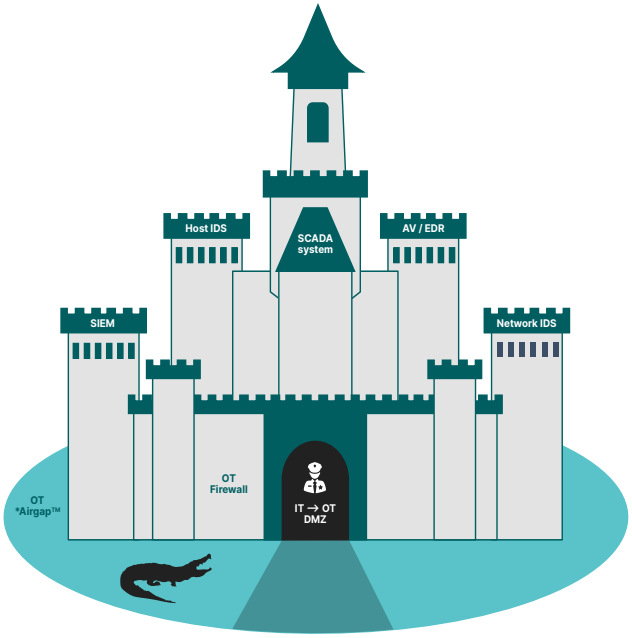



**Figure 1.** Erecting high walls may have worked to keep attackers at bay in the tenth century, but it is a deficient model for complex, interdependent networks commonly in use today. Modern enterprises no longer store data exclusively within the castle walls. Information is often spread across multiple cloud vendors, with data storage geographically dispersed.

The digital grid[2] is accelerating the shift from central power generation and subsequent one-way flow (generation → transmission → distribution → consumer), to more localized and optimized generation with multi-directional flow, including photovoltaics, wind, and energy storage which can be installed behind the meter or located remotely. The digital grid receives and analyzes data from perhaps millions of customer devices nationwide to enable utilities and other players to better serve customers with energy-saving technologies, such as home automation, monitoring and security, energy management, and equipment diagnostics.

1) https://www.moodys.com/newsandevents/topics/Cyber-Risk-00704E (paywall). A summary is available here.

2) The Electric Power Research Institute describes the digital grid as the "next frontier of electric grid modernization, integrating technologies in embedded sensing, advanced intelligence, data analytics, and cloud computing to leverage customer-sited distributed energy resources to enhance grid flexibility and thereby ensure reliable, safe, affordable, and sustainable electric service for customers."

Protecting critical national infrastructure is becoming even more challenging for electric utilities given the new, digital grid's rapidly increasing number of connection points, which take the form of distributed energy resources (DERs) (including rooftop solar, battery storage, micro-turbines), phasor measurement units, smart sensors and cloud services. And these are just the additional protections. A utility is still required (often by legislation) to protect critical energy infrastructure information (CEII), bulk electric cyber system information (BCSI) and customer data. Every data source's ingestion point presents an opportunity for an incursion.

The perimeter security model is no longer scalable, given the millions of external data sources added to a utility's grid network each year. The multidirectional nature of these technologies means that the number of boundary locations requiring cyber protection is steadily increasing. The single-perimeter network security model is obsolete for utilities and does not protect an organization's data assets against modern cybersecurity threats.

Cyber threats are also not static. The threat environment is multi-dimensional and growing increasingly complex each year. Attackers constantly evolve tactics to exploit vulnerabilities within vastly complex networks of devices, data, applications, users, and locations. Often the security perimeter of an enterprise is breached unintentionally from inside the castle's walls through phishing or maliciously altered downloads, allowing criminals to obtain a foothold within the network. Non-employee and contractor access to the organization's network and critical external data sources are other areas that attackers can exploit (application updates, weather data, managed service providers, etc.). Once they've infiltrated the secure perimeter, massive confidential data leaks, ransomware demands, or cyber-physical impacts often follow.

# GENERAL DESCRIPTION OF A ZERO TRUST NETWORK

Today's modern data security problem has become exacerbated as companies no longer keep their data in one place. Increasingly complex enterprise architectures include internal networks, remote offices/individuals, and cloud services. The number and cost of cybersecurity breaches have both risen along with the number of remote users and reliance on off-site data storage. Further, a staggering eighty percent of all attacks involve abuse of trusted credentials within the target's network.

However, an organization must continue functioning efficiently despite growing cybersecurity threats. Cybersecurity needs must be extended to all of an organization's assets and users (i.e., an individual, application, service, or device); thus, a Zero Trust cybersecurity solution is required. Networks must be protected against threats stemming from millions of connected endpoints, and Zero Trust is the solution that scales and protects an organization's data assets.

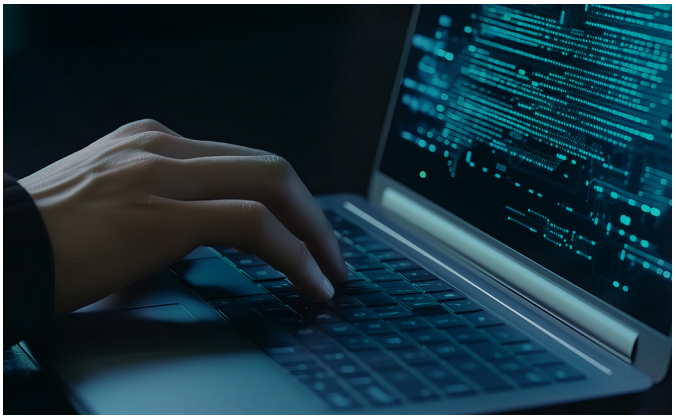
NIST Cybersecurity White Paper (CSWP) 20 defines Zero Trust as "fundamentally comprised of a set of principles upon which information technology architectures are planned, deployed, and operated."[4] Broadly, "Zero Trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised."

The essence of the Zero Trust security model is that a user within the "castle" is no more trustworthy than a potential attacker. No user or data source is trusted by default from inside or outside the network perimeter. Every connection point must be setup with authentication and authorization in advance, as well as upon each individual connection. Zero Trust requires a change in the mindset of network administrators who must move from a "verify then trust" to a "never trust, always verify" operations model. Utilities must develop Zero Trust protocols to protect resources (e.g., data, equipment, actuators, sensors, etc.) and business functions, granting access only to users who are not only initially authenticated and authorized, but, who are continuously authenticated, authorized, and validated **(Table 1)**.

**Table 1.** Comparison of Implicit Trust "Castle" Model with Zero Trust grid software principles for internal cyber threats. Because external and internal network threats are constant and unpredictable, the network location no longer determines who may be trusted.

| How do we know, beyond a shadow of a doubt, that… | Zero Trust grid security principles don't trust: |
|---|---|
| They are who they say they are and haven't suffered identity theft? | **Identity** |
| They're only doing / accessing what they're supposed to and not trying to break into the vault? | **User Permissions** |
| They haven't outstayed their welcome? | **Session Management** |
| The trusted guard hasn't been bribed? | **Administrator** |
| People are only entering via the drawbridge, and someone hasn't dug a tunnel underneath the castle to get in? | **Client Connections** |
| Although inside, the knight isn't flirting with the queen behind the king's back when he's not supposed to? | **Service-to-Service Connections** |
| The gift isn't a Trojan Horse? | **Delivery of Installer** |
| When they're speaking in a foreign language, they're not plotting against us? | **Network** |
| The brick & mortar aren't crumbling inside or the lumber isn't rotting? | **Software** |

3) IBM Cost of a Data Breach 2020.
4) Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication (SP) 800-53, Rev. 5.



In addition, users should only be given access for the time it takes to perform a task. This helps to minimize any ability to inflict harm. Further, policies governing network connectivity must be dynamic and based on the number and type of data sources.

A Zero Trust architecture is a cybersecurity plan that utilizes Zero Trust concepts and encompasses component relationships within the network infrastructure (physical and virtual), workflow planning, and dynamic operational policies. There is no "one-size fits-all" Zero Trust architecture implementation; each solution requires a holistic design approach, carefully considering workflow and development of an organization-wide IT and/or OT infrastructure. There are, however, several bedrock principles that should be followed when developing a Zero Trust architecture[5], whether for an organization's IT system or when developing modern software. It is these principles which form the design basis for the Zero Trust grid security model.

A. **All resource authentication and authorization are dynamic and strictly enforced before access is allowed.** A typical organization will have many networks, users, and processes that must be considered. DERs, for example, will have identities for various software and hardware components. The Zero Trust architecture design must include policies and structure so that authenticated sources (e.g., DERs data collection) perform only authorized operations. The enforcement of the authentication process must also include consideration of endpoint and environmental factors. Authenticating and authorizing users must be based on any number of available data points, including user identity, location, number of connections, time, etc. Also, user access must be limited with just-in-time or just enough access in concert with risk-based adaptive policies.

B. **All data sources and computing services are considered resources.** A typical organization will have a wide variety of resources to perform its mission (e.g., APIs, grid data model, various modeling engines, etc.). All resources need to be considered in a Zero Trust architecture.

C. **The enterprise monitors and measures the integrity and security posture of all owned and associated resources.** Zero Trust architecture must include devices owned by the enterprise and those not owned but used by the enterprise. For example, third party-owned DERs applications have sensors and devices on which the utility must rely for optimized demand-side system operation. The organization and its systems must be aware of the state of these resources, enabling them to react when a vulnerability or attack occurs against one, in order to protect the other resources and the integrity of the data.

D. **All communication is secured regardless of network location.** As noted above, a Zero Trust architecture assumes the network is under continuous attack so that the confidentiality and integrity of data are always protected. The Zero Trust architecture design must limit the damage a breach can cause by segmenting access. Further, the Zero Trust architecture must verify end-to-end encryption and use analytics to get visibility, enable threat detection, and improve defenses.

E. **Access to individual enterprise resources is granted on a per-session basis.** A Zero Trust architecture should authenticate and authorize each connection attempt's needs before the operation occurs to limit potential damage. If not possible, the system administrator should plan for compensating controls, such as logging, versioning tools, or backups to manage risk.

F. **Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.** In other words, the Zero Trust architecture default condition is to deny all connections until explicitly allowed by set policy conditions. The requestor must prove their connection authority and the connection request must be authenticated for each session.

G. **The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.** Perimeter-based architectures typically cannot dynamically adjust to new threats that manifest within the perimeter. An adequately designed Zero Trust architecture and its associated policies can be dynamically adjusted in response to the latest threat, until a "patch" or other corrective measures are available. Fast response to newly discovered threats will lessen the cost and data loss damages.

5) Derived from "Planning for a Zero Trust Architecture, A Planning Guide for Federal Administrators (May 6, 2022). Available here.

**Foundational concepts** for a Zero Trust security system for utility grid management and operational control systems that comply with the NIST Risk Management Framework for Zero Trust security systems:

| | Established paradigm | Established system | But..... | Zero Trust grid security protections |
|---|---|---|---|---|
| **Identity** | Accounts belong to approved users | Accounts presumed to be useable only by its owner via secret password; some accounts have shared passwords | ... a threat actor can gain access to a user's account | No shared accounts<br>Federate individual IDs securely<br>Require MFA or TOTP |
| **User** | Personnel with access are trusted | Users trusted with coarse roles & permissions (e.g. "Control User") which rarely change and have no limits on usage | ... an individual can go rogue | Granular group/role/permission RBAC<br>Advanced policies requiring re-auth or 4 eyes<br>Multi-tiered Areas of Responsibility (AoRs)<br>Limit sessions creation per user |
| **Session** | Once a user has logged in, they're allowed to operate | Sessions keep the same roles & permissions for their duration, which can last until the user logs out - if ever - with no time or volume limits | ... a session can be hijacked | Signed UUID Session Token<br>Session refresh for RBAC changes<br>Max time-to-live session policies<br>Inactivity policies |
| **Administrator** | If super user account is compromised, it's game over | Few admin accounts, but those that exist are typically "all powerful," with changes made accepted as expected, permanent, and difficult to track | ... an admin account can be taken over | Granular administrator RBAC on back-end<br>Infrastructure-as-code to deploy & restore<br>k8s Operators reset changed settings back to expected state<br>Automated reporting vs. hardening benchmark to catch config drift |
| **Client** | Client devices in the OT building or OT network are safe | Since only "approved" clients can connect via routing/ firewalls, allow them to hit server & authenticate | ... clients can be infected | Accept only from Known Clients by IP & certificate<br>Limit sessions from Known Clients |
| **Services** | If an application is allowed through, it's trusted | Since only "approved" services can connect via routing/ firewalls, allow them to communicate with server | ... connecting applications can be compromised, services spoofed & traffic manipulated | Mutual trust configuration required prior to services connections<br>Apply RBAC policies to app connections<br>Encrypted & authenticated communications |
| **Installer** | Checking the hash & certificate is enough | Accept that hashed/signed installer and software in it only does what it needs to & documentation accurately reflects behavior | ... the installer can be maliciously altered | Admission control prevents unsafe containers entering cluster<br>Admission control limits what containers can do |
| **Network** | The OT network is secure b/c of Defense in Depth + "Airgap" | Allow unencrypted & proprietary protocols & hope to catch issues with IDS | ... an attacker can have presence on the network | Use open standards to allow packet inspection<br>Encrypt all traffic |
| **Software** | Patching the visible OS + Middleware addresses vulnerabilities | Once system passes PreFAT, FAT, and SAT, focus patching on only the OS & external middleware as required by regulation & permitted by vendor | ... vulnerabilities are an emerging property in aging software | SBOMs transparently show make up of app<br>Modern release rhythm to remediate CVEs |

Table - Source: GE Vernova

# DEVELOPING YOUR OWN ZERO TRUST ROADMAP

NIST SP 800-37 Revision 2, Risk Management Framework (RMF) for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy[6], describes the RMF methodology. Its seven steps can be adopted to prepare your own Zero Trust roadmap, as seen in NIST CSWP 20 **(Figure 2)**.


**Figure 2**. An overview of the NIST Risk Management Framework for cybersecurity systems.

## A SHORT DESCRIPTION OF THE SEVEN STEPS FOLLOWS:

1

**PREPARE:** Organizational and system preparation.

Inventory all resources, network identities, and roles/privileges that will become part of the Zero Trust architecture. Business process owners define workflows to help determine network security requirements. “The PREPARE step primarily focuses on preparing the organization to manage its security and privacy risks using the NIST RMF and establishing essential activities at the organization, mission and business process, and system levels.”

2

**CATEGORIZE:** Resource categorization.

“Place resources in a low, medium, or high category based on [resource] confidentiality, integrity, and availability requirements in the workflows."

3

**SELECT:** Control selection.

“Additional controls may be added or removed [from the above Categorize step] as part of control tailoring, adjusting the controls to manage risk to the resource, its known attack surface, and its position in the workflow. As Zero Trust emphasizes continuous monitoring and updating of security postures, cybersecurity architects and administrators need to develop a comprehensive monitoring process that can handle the volume of data required by the dynamic nature of Zero Trust.”

4

**IMPLEMENT:** Control implementation.

“Zero Trust encourages automation to have dynamic responses to changing security concerns, and manual changes may not be able to keep up with frequent changes.”

5

**ASSESS :** Control assessment.

“In a Zero Trust architecture, the assessment of controls should be continual to address the ever-changing environment. Modern IT environments and trends . . . mean that a singular assessment of an operating system quickly becomes outdated as improvements and configuration changes are made to mitigate newly discovered threats or modifications to the enterprise infrastructure. The ASSESS step should be thought of as comprising two assessment processes: continual assessment of the system (also part of the MONITOR step below) and the processes used to manage the system.”

[6]CISA See also National Institute of Standards and Technology (2021) About the NIST Risk Management Framework (RMF) and ON2IT (2020) A hands-on-approach to Zero Trust implementation. Also, Kindervag J (2017) ‘Zero Trust’: The Way Forward in Cybersecurity (Dark Reading).

All quotes are from the cited reference unless otherwise noted. Source: NIST CSWP 20

**6** **AUTHORIZE:** System authorization.

"In any architecture a system is more than just its current operating deployment. A Zero Trust architecture should be dynamic and fluid to respond to changing network conditions. Authorizations should not be viewed as applying to the operation of a static system but applying to both the system and its processes for changes or updates."

**7** **MONITOR**: Control monitoring.

"As stated, Zero Trust requires the enterprise to monitor the resources used to conduct its primary mission(s). This encompasses end-point hygiene and user behavior as well as network traffic. In addition to monitoring the current activity and state of enterprise resources, cybersecurity planners should consider how external threat intelligence can help in pre-emptive responses to new conditions."

# FINAL THOUGHTS

Historically, cybersecurity measures have been designed around a trusted private network with a defined security perimeter. Those accessing data when physically or "digitally" located within the security perimeter were automatically trusted entities. The modern digital grid must consider the mounting asymmetric cyber attacks on its infrastructure from many sources, given the increasing use of cloud-based data storage, dispersed workforce, and rapidly increasing bi-directional data flow and storage necessary when using DERs, microgrids, demand side management systems, and so on. As the industry moves to adopt internet connectivity and the cloud, these will also fundamentally change the threat environment.

Zero Trust is based on a security model that requires strict identity verification for every request attempting to accept data or access resources, regardless of whether they are sitting inside or outside the electronic security perimeter. Zero Trust takes the security controls that may have previously been in place only at the perimeter and disperses them throughout the system. Further, Zero Trust assumes everyone and everything is hostile, that there are malicious attackers lurking everywhere, and nothing is safe.

Zero Trust builds security measures that work to shield against these threats by carefully considering distrust in everything: users, clients, connecting services, software, etc. Zero Trust includes a robust process to authenticate users, services, and endpoints. Every connection is authenticated and authorized, not just the first time, but continuously. Zero Trust is essential in grid modernization programs, particularly with DERs and renewables that rely on continuous optimization and data transfers.

GridOS® uses Zero Trust grid security model and its ongoing roadmap addresses three fundamental principles found in the NIST guidelines when developing a client's Zero Trust architecture:

**1. Continuous verification.** Always verify access credentials, all the time, for all connected resources. Credentials should allow access to the minimum capability required to perform assigned tasks.

**2. Limit the impact** of a cybersecurity incursion should an external or insider breach occur. The Zero Trust architecture will limit access paths to give time for systems and technicians to mitigate the attack.

**3. Automate the response.** Collect contextual data from the network to allow an accurate and immediate policy response to the incursion to confine or limit the damage.

GE VERNOVA

GridOS® Orchestration Software

# ORCHESTRATING A MORE SUSTAINABLE ENERGY GRID

Connect with a GE Vernova expert today:

Get in touch

1-833-690-5552

## ELECTRIFICATION SOFTWARE

GE Vernova's Electrification Software is focused on providing a suite of software products and services to customers aiming to accelerate a new era of energy by electrifying and decarbonizing the energy ecosystem through intelligent and efficient data analytics, monitoring, and management.



A_05_DOC