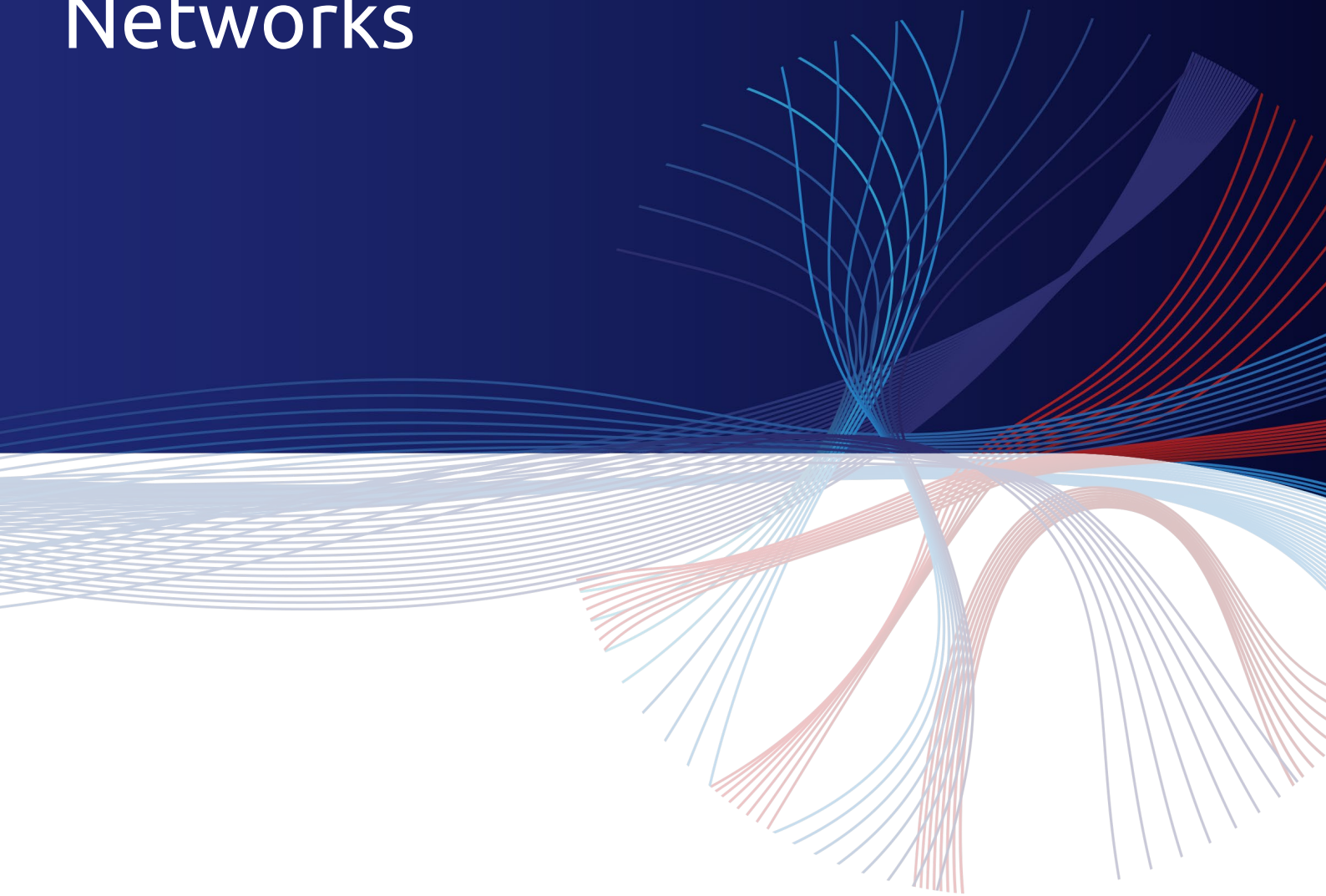
SCADAfence

Whitepaper

Securing Power Distribution Networks



Introduction

Our society depends on electricity. From turning on the lights in our homes, to operating multi-million-dollar manufacturing equipment, to running billion-dollar critical infrastructure systems, electricity is a core component that connects how we work and live. A disruption to electric power distribution networks could cause substantial health, economic and environmental damage.

In recent years, cyber-attacks across the world have caused the disruption of power supply to major populated areas and caused massive damages.

Some examples of these cyber-attacks include *Industroyer*, a malware that targeted switches, breakers and substation communication protocols, and was mainly responsible for Ukraine's power grid failure. *Dragonfly*, a malware that infected hundreds of businesses in an often-successful attempt to collect information on industrial control systems. *WannaCry*, a ransomware worm that affected operations of hospitals, banks and universities. *Stuxnet*, a computer worm that gained control of nuclear facilities and destroyed numerous centrifuges in Iran's Natanz uranium enrichment facility. *BlackEnergy*, designed to launch denial-of-service attacks against SCADA applications in industrial control systems and *Trisis*, a malware that attacked equipment used in energy, oil and gas control systems.

The National Security Agency (NSA) has reported intrusions into ICS by entities with the apparent technical capability "to take down control systems that operate U.S. power grids, water systems and other critical infrastructure." [1]

Nonetheless, power distribution organizations are continuously required to increase the connectivity of their OT networks to other networks. They require more connections between the central control rooms and remote substations (that were previously highly segmented), for more precise and effective maintenance and faster incident response. Power distribution networks now have more connections to organizational systems, and more remote access connections than ever before.

This increased connectivity, in turn, makes power distribution networks more susceptible to security incidents; whether these are malware or ransomware infections, or carefully crafted targeted attacks by well-organized hacker groups, or national threat actors.

According to the U.S. Department of Energy, "The absence of intrusion detection systems (IDS) and monitoring in IT and OT networks means utilities cannot obtain forensic data related to cyber intrusions and attacks. All utilities should have intrusion detection and monitoring tools in place, even as a minimum cybersecurity procedure."[2]

[1] https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf (Page 6)
[2] https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf (Page 33)

The Security Challenges for Power Distribution Networks

When protecting such large, critical and distributed networks, there are many unique challenges and requirements which need to be addressed.

1. **Large Distributed Networks with Remote Assets**
   Power distribution networks are large networks, with distributed and often remote unmanned sites. This means there are many moving parts which could potentially act as attractive entry points for threat actors since they are prone to risks categorized by lack of segmentation, misconfigurations, poor administration and communication shortcomings. Furthermore, perimeter security is not capable of controlling all of the entry points to the network, and if bypassed, attackers can access a wide range of assets, and remain undetected for long periods of time.

2. **Malware and Ransomware**
   An increasing number of malware and ransomware cases target organizations worldwide. They often originate in IT and spread into the OT networks, often paralyzing the OT networks and the OT supporting processes while causing substantial financial and operational damages. Furthermore, specific industrial and electricity targeted attacks (e.g. the *Industroyer* malware that hit Ukraine's electricity grid in December 2016) are specifically created by threat actors in order to cripple power generation and their distribution processes.

3. **Insecure Communication Protocols**
   The communication protocols used throughout ICS networks are of additional concern. Common and long-established ICS protocols such as Modbus and DNP3 used throughout the power system have little to no security measures. Lacking authentication capabilities, these messages may be intercepted, spoofed, or altered, and can potentially cause a dangerous event in an operations environment.

4. **Vulnerable Devices**
   Many automation components, such as programmable logic controllers (PLCs) function via microprocessors and contain function specific software programming. They also have management and communications capabilities over network paths. Such devices have been main target of cyber-attacks as a means of gaining access to a control system.

5. **Remote Access Connections**
   In order to manage geographically widespread assets, to increase convenience and to reduce costs, power distribution organizations (like many other utilities) increasingly rely on remotely accessible equipment and mobile devices. However, vulnerabilities stemming from unsecure access or connection to critical systems via remote tools and devices can lead to severe security incidents and network compromise.

6. **Third-Party Services**
   Some vendors of ICS equipment unintentionally generate cybersecurity problems due to vendor maintenance policies, such as creating intentional or unintentional "backdoors" for access to devices or software, or by threatening to void equipment warranties if reconfigured from factory settings, i.e., changing passwords or installing unapproved security packages.

7. **Smart Grids**
   The shift to a smart grid will mean that utilities will add tens of thousands of devices to their operations, these include new sensors, controllers, relays, meters, and other similar devices. Many of these devices will be exposed to the IT network, the Internet and to the general public, leveraging a range of new communication protocols.

Evaluating a Security Solution for Power Distribution Networks

When evaluating a security solution for power distribution networks, the solution should meet the following criteria:

1. **Suited for the Unique Power Distribution Network Architecture:**
   Communications between remote sites and the central data centers may be limited and unstable at times. The solution you choose should support the local analysis and storage of data, while not requiring substantial bandwidth to operate reliably.

2. **Has Clear Notifications with Straightforward Action Items**
   As equipment can be located remotely in the field and is unmanned – it is crucial that the security solution will provide clear and straightforward notifications to the central control rooms, so no unnecessary visits to the remote locations will be needed.

3. **Is Cost Effective**
   For a large number of remote critical sites, deploying a large number of sensors becomes an expensive burden for purchasing and maintaining. Power distribution networks need a security solution that is cost-effective, not only for initial purchasing but for long-term maintenance as well.

4. **Addresses Regulations and Compliance Requirements**
   The security solution has to comply and also assist in compliance to the increasing regulation for power distribution networks, such as NERC-CIP, and other regulations.

5. **Provides Future Proof Security**
   The security solution should be able to scale to a larger number of devices, technologies and protocols that are introduced by adding systems, or by moving to smart grid technologies in the future.

6. **Does Not Require Expensive Architectural Changes**
   Finally, it is critical that the security solution will not interfere with the production processes, and doesn't require architecture changes to the substation or central network architectures. At the same time, the security solution should integrate with the existing monitoring and security management tools.

Securing Power Distribution Networks with the SCADAfence Platform

The SCADAfence Platform offers full visibility of network assets and their day-to-day operations in power distribution networks. It provides real-time detection of anomalous and non-authorized behavior. The SCADAfence Platform also covers the security scenarios that are “uncovered” by other security tools, such as firewall and anti-virus components. It addresses external and internal attack vectors. It alerts on tampering with security mechanisms, malware and ransomware activity, misconfigurations, and any kinds of hacking attempts (whether they’re targeted or not).

The installation process doesn’t require any downtime to the operational network, and the system algorithms are automatically configured without any tedious input from the user.

Addressing the Security Challenges of Power Distribution Networks

Power distribution networks need to be continuously monitored, in real-time, in order to prevent system abuse or from becoming the targets of a cyber-attack. Furthermore, availability related issues such as internal service malfunctions, failures of equipment and dormant malware that awaits activation, are also important to be continuously monitored for.

The SCADAfence Platform analyzes the network traffic and addresses the following attack scenarios:

- External network access through misconfigured perimeter devices, or routes ‘around the firewall’.
- Unknown malware and ransomware can easily bypass firewall and anti-virus solutions.
- Known malware and ransomware can also infect the network internally via infected devices or USB drives due to limitations of AV or agent installation on the endpoints.
- Unauthorized remote access or authorized access privilege escalation.
- Internal suspicious traffic that might indicate of OT network compromise.
- Direct access to critical OT equipment and the manipulation of production processes – which often involves industrial protocol level attacks.
- IT-OT propagation from authorized stations, gateways, unauthorized wired and wireless routers.
- Operational issues caused by human error/misconfiguration or service or hardware malfunctions.

Scalable Architecture

The SCADAfence Platform supports multiple architecture models, comprised from one or multiple hierarchical layers, and is suitable for managing small or a very large number of sites and monitoring points. These remote sensors perform local traffic analysis.

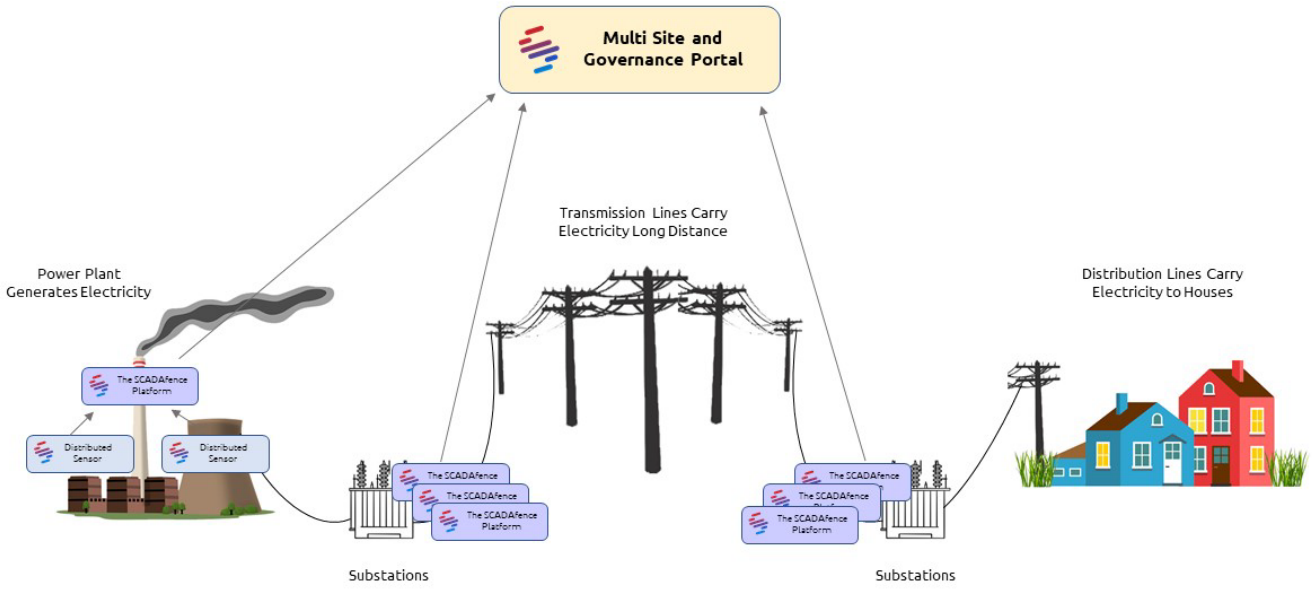


Diagram #1: The SCADAfence Platform's Multi-Layer Architecture

Cost Efficient Deployment

The SCADAfence Industrial DPI Sensors can scale to hundreds of distributed instances, serving tens of thousands of devices, without performance degradation.

The SCADAfence Platform also introduced the unique 'NetFlow Analyzer' feature. This feature allows organizations to skip the deployment of expensive sensors in each and every segment, and thus enables users to monitor remote segments in an "agentless" cost-effective manner. This is done by configuring the supporting network infrastructure to send NetFlow data into a SCADAfence sensor. The combination of the high-performance capabilities of the SCADAfence Platform, combined with the NetFlow Analyzer, offers a feasible and cost-effective way to cover smaller and remote network segments while securing large distributed networks.

Non-Intusive, Integrating into Existing Architecture

The SCADAfence Platform's default mode is to work as a non-intrusive solution, therefore it has no impact on the production process. It does not inherently require production downtime or lengthy maintenance windows. An active mode is also available for further asset data collection.

Furthermore, the SCADAfence Platform is designed so that it will integrate with central security management systems such as a SIEM or Incident Management systems and becomes an integral part of the security and resilience architecture of the OT network.

Deep Packet Level Analysis

In each site, the SCADAfence sensor will discover and monitor assets such as RTUs, IEDs, smart meters and actuators. The sensor will automatically discover the site assets, perform DPI of the network traffic including industrial traffic such as DNP3, IEC-104, MMS and GOOSE and raise alerts on cyber-security and operational events.

The SCADAfence Platform will also alert on attempts to tamper with local assets, shut down critical infrastructure components and initiate unauthorized OT commands to the network devices.

Accurate Detection and Minimum False Positives

SCADAfence's Micro-Granular Baseline is granular, per asset and per traffic characteristics. This unique baseline is designed to provide the most accurate detection mechanism, and without the need to configure or reconfigure the baseline upon any changes.

The benefits of SCADAfence's Micro-Granular Baseline are as follows:

Minimizes False Positives Alerts – The granular and adaptive baseline minimizes the number of false positives alerts, thus making the system usable and trustworthy. The larger the network is, the number of events grows exponentially, and thus makes this issue a critical one.

No Tuning and User Configuration Required – The SCADAfence Platform can be deployed in the network quickly and with minimal effort. There is no need for a lengthy analysis and expert tuning.

No Re-configuration and Restarts - As the baseline is adaptive and not arbitrarily set, there is no need for effort and time-consuming stop/restarts and re-learn steps which make the system unusable for large periods of time and increases network exposure and risks.

Governance and Compliance

The SCADAfence Governance Portal has yet another innovative layer of security management. The portal enables the IT and audit departments to centrally define and monitor the organization's adherence to company policies and to OT-related standards and regulations such as NERC-CIP and the NIST framework, or internal policies and best practices.

It enables CISOs to plan their cybersecurity strategy, as well as to automatically report and measure their organizational compliance based on the actual data derived from the networks.

The SCADAfence Governance Portal can be connected to any 3rd party tool, and become a central organizational compliance management portal.

To learn more about SCADAfence's NERC-CIP compliance solution click here.

Securing the Remote Access Users

The SCADAfence Platform adds an additional unique layer of security by correlating between the users accessing the network from remote and tracks their activities in the OT network. It detects and alerts on anomalous or unauthorized actions and provides association to the user name, originating workstation and application.

To see a short demo video on how remote access security can be achieved in OT, click **here**.

Future Proof Security

Supporting IoT devices and protocols, and having a patent-pending technology with the most advanced feature set for managing large IoT fleets, The SCADAfence Platform is best designed for addressing future growth and adoption of Smart Grid technologies.

SCADAfence

About SCADAfence

SCADAfence is the global technology leader in OT & IoT cybersecurity. SCADAfence offers a full suite of industrial cybersecurity products that provides full coverage of large-scale networks, offering best-in-class network monitoring, asset discovery, governance, remote access, and IoT device security. A Gartner “Cool Vendor” in 2020, SCADAfence delivers proactive security and visibility to some of the world's most complex OT networks, including the largest manufacturing facility in Europe. SCADAfence enables organizations in critical infrastructure, manufacturing, and building management industries to operate securely, reliably, and efficiently. To learn more, go to www.scadafence.com.

NEW YORK,462 W Broadway New York, NY 10012, USA +1-646-475-2173

MUNICH, Schellingstr. 109a 80798 Munich Germany +49-322-2109-7564

TEL AVIV, 4 Menorat Ha’Maor St. Tel Aviv 6744832, Israel +972-3-763-0785

TOKYO, Clip Nihonbashi, 3-3-3 Nihonbashi-Honcho Chuo-ku, Tokyo 103-0023, Japan +81-3-4588-5432

Contact us: info@scadafence.com

SCADAfence