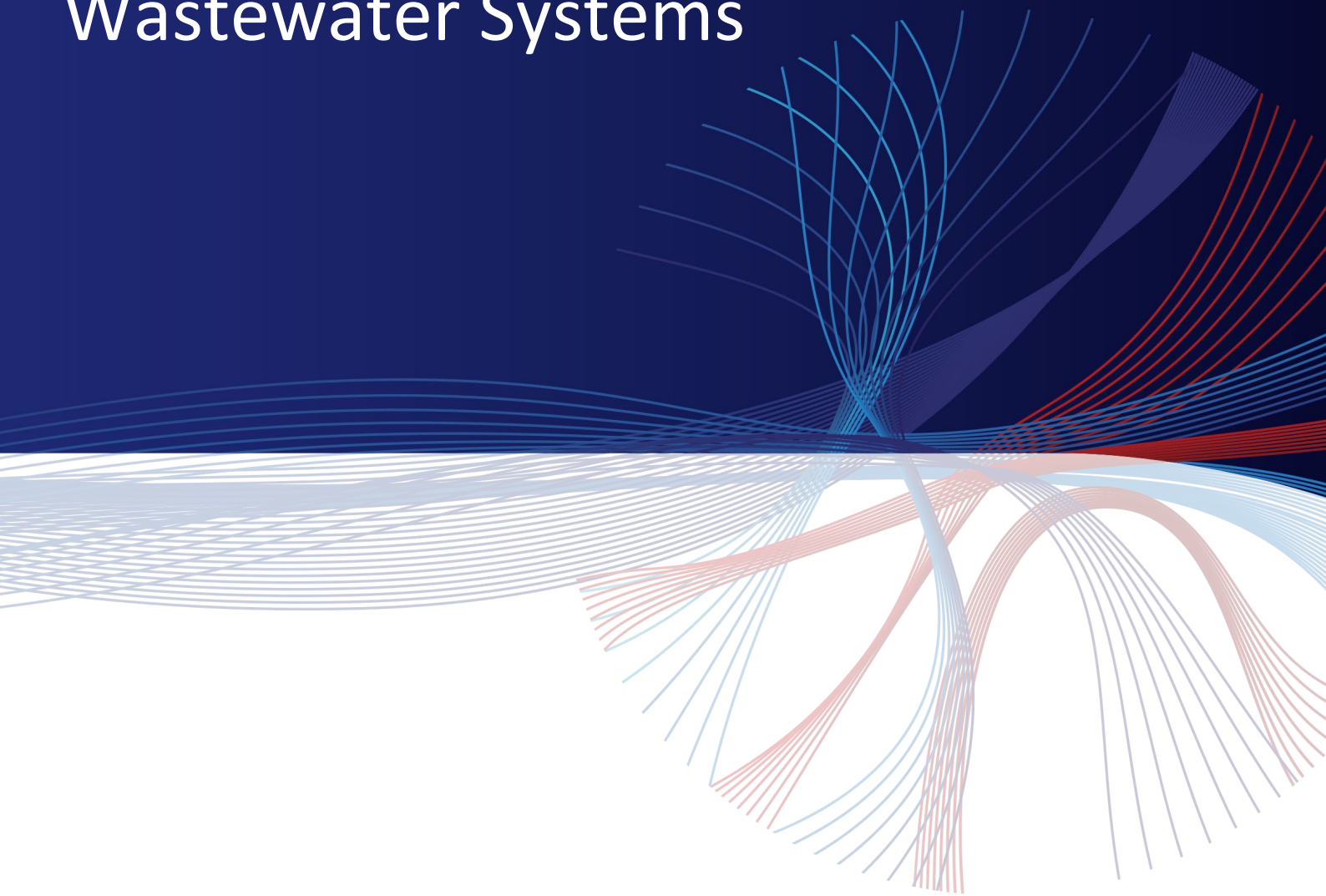
SCADAfence

Technical Whitepaper

Securing Water and Wastewater Systems



Securing Water and Wastewater Systems

Water and wastewater systems depend on automated control systems to operate and monitor processes such as treatment, testing and the movement of water.

In recent years, there has been an increase in connectivity of OT networks to other networks and to the Internet, due to increased process automation, more segments and new remote sensors. The reliance on these Industrial Control Systems (ICS), such as Supervisory Control and Data Acquisition (SCADA), has opened the critical water and wastewater infrastructure to new exposures and threats: whether they are malware or ransomware infections, accidental activities that cause damage, or carefully crafted targeted attacks by well-organized hacker groups and national threat actors.

Components of Typical Industrial Control System in the Water Sector

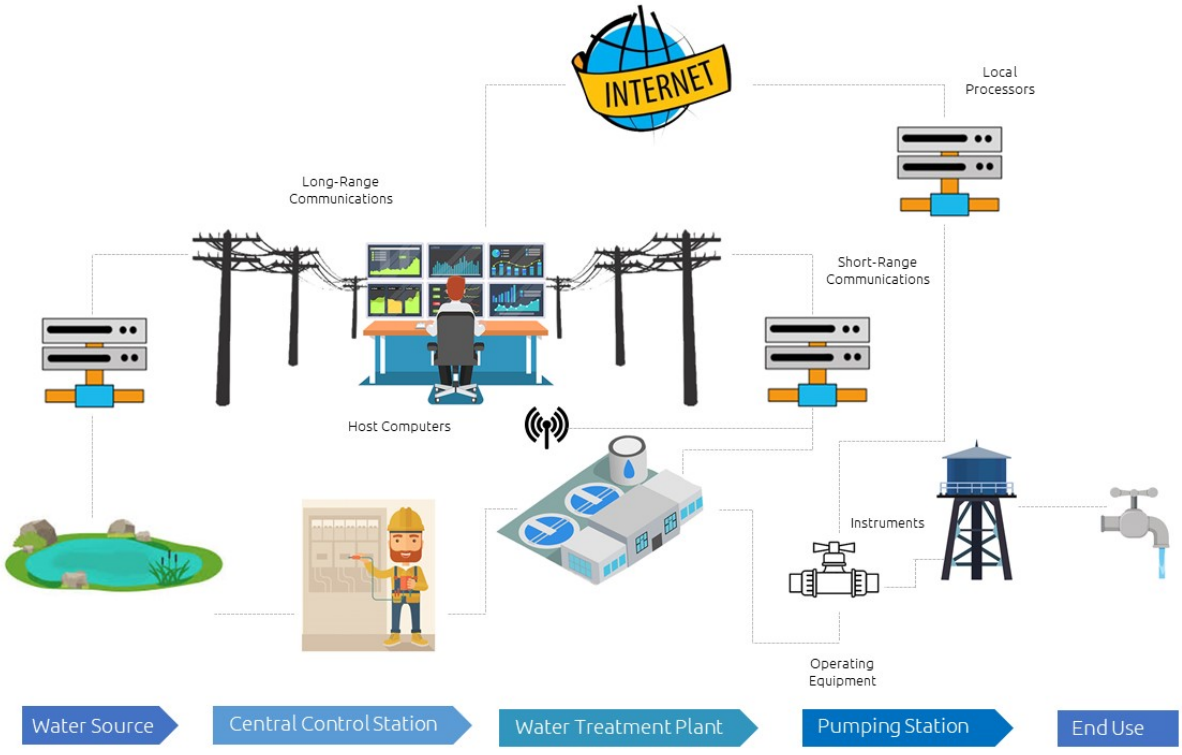


Diagram #1: A Typical ICS System in the Water Sector

In recent years, ransomware and hacking cyber-attacks in the US (and around the globe), have caused the disruption of numerous water and wastewater systems. Ranging from crippling and costly ransomware incidents, up to incidents that risk public safety. These incidents include dam and canal management, sewage spilling, water treatment process manipulations, and many others. These cyber-attacks have caused severe damages to ongoing operations, putting water quality and public safety at risk, while causing millions of dollars in damages.

In 2018, the American Water Infrastructure Act (AWIA) was signed into law. AWIA Section 2013 requires community (drinking) water systems serving more than 3,300 people to develop or update risk assessments and Emergency Response Plans (ERPs).

Addressing the Attack Vectors

Attack vectors into OT networks are constantly changing. They include internal engineering stations, external vendors, attacks of remote equipment, attacks of wired and wireless radio networks, and many more. All of which are not addressed by perimeter firewalls or by a local agent. Real-time and continuous network-based detection is needed in order to prevent system abuse or from being a target of a cyberattack. Furthermore, it is vital to continuously monitor for availability related issues.

A robust network wide intrusion detection covers the following attack vectors:

- Unauthorized external access via misconfigured perimeter devices, or routes alternate to the firewall.
- Malware and ransomware infections – new or known malwares can easily bypass firewalls and anti-virus solutions.
- Unauthorized remote access or authorized users' access escalation of privileges.
- Internal malicious activities by authorized or formerly authorized users.
- Direct access to critical OT equipment and manipulating of production processes. Including tampering with sensors and actuators in central or remote stations.
- IT-OT propagation of threats from authorized stations, gateways, unauthorized wired/wireless routers, etc.
- Operational issues caused by human error/misconfiguration, service, or hardware malfunctions.

Threats to Water & Wastewater Systems

Unauthorized Network Connections – Motivated by either ransomware or vandalism intent, threat actors break into central control systems or into remote unsupervised equipment, via wired or radio networks. These criminal actions put the environment and public safety at risk.

Unauthorized Changes to Programming Instructions – Unauthorized changes by authorized or external users can cause damages to water distribution or wastewater systems. Threat actors can take control of the systems, disable services, and reduce levels or overflow of water and chemicals. They can also program instructions for sewage to spill into public areas.

Disrupting Services at Scale – Threat actors can initiate Denial of Service (DoS) attacks, disabling or severely disrupting operations of water treatment or water supply systems.

Intentional Manipulation of Information Sent to Operators – By changing thresholds or by disabling process alarms, threat actors inhibit appropriate responses by security teams to emergency situations.

Unauthorized Remote Connections – Utilizing authorized or rogue remote access devices and internet connections, threat actors can damage control systems or remote end points.

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

The SCADAfence Platform

The SCADAfence Platform offers full visibility of network assets and their day-to-day operations. The non-intrusive platform provides real-time detection of anomalous and non-authorized behavior. The SCADAfence Platform also discovers security scenarios that are not discoverable by other security tools, such as firewall and anti-virus components. It addresses external and internal attack vectors, tampering with security mechanisms, malware and ransomware activities, misconfigurations, as well as amateur and professional hacking attempts.

Scalable Architecture

The SCADAfence Platform supports multiple architecture models, comprised from one or multiple hierarchical layers. It is also suitable for managing small or a very large number of sites and monitoring points.

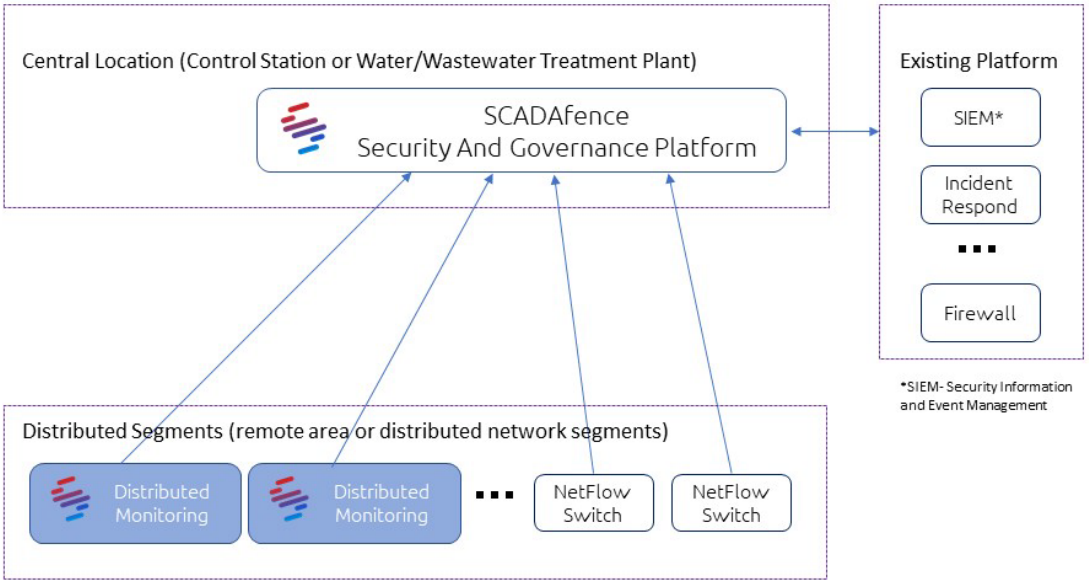


Diagram #2: SCADAfence's Multi-Layer Architecture

The Benefits

Cost-Effective and Non-Intrusive

The SCADAfence Platform's DPI (Deep Packet Inspection) algorithms are designed with performance optimization in mind. The SCADAfence Industrial DPI Sensors can use small hardware form factors with minimal specifications. Additionally, the central SCADAfence Platform server can scale to hundreds of distributed sensors, serving tens of thousands of devices without performance degradation. Furthermore, for large-scale distributed networks, the SCADAfence Platform is able to process NetFlow traffic from remote locations, thus eliminating the need for local sensors, making deployments practical and maintainable.

The SCADAfence Platform's is non-intrusive (default mode), 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. The active polling of devices can be done via "IT" protocols such as SNMP and WMI, and via native industrial protocols. Active polling should be explicitly enabled.

Visibility

In each site, the SCADAfence sensor will discover and monitor assets such as RTUs, PLCs, smart meters and actuators. The sensor will automatically discover the site assets, perform DPI of the network traffic including industrial protocols and raise alerts on cyber-security and operational events. The SCADAfence platform will alert on attempts to tamper with local assets, shut down critical infrastructure components and initiate unauthorized OT commands to the network devices.

Low False Positives

SCADAfence's Micro-Granular Baseline is granular, per asset and per traffic characteristics. This unique feature is designed to provide the most accurate detection mechanism, and minimize the number of false positives in the industry.

Providing a low number of accurate alerts makes the system usable and trustable by its end-users. There is also no need for effort and time-consuming stop/restarts and re-learn steps (which would make the system unusable for large periods of time and increases network exposure and risks).

Automatic Tuning with Continuous Improvement

The SCADAfence Platform's installation is configuration-free by default. Its algorithms, and the Micro-Granular Baseline are pre-tuned to the distributed network architecture making the deployment phase quick and at minimal effort. There is no need for a lengthy analysis and expert tuning.

Upon installation, the SCADAfence Platform creates a baseline, that keeps evolving and learns the network traffic patterns and assets behavior. It then enables it to detect any deviation from the norm and alert on suspicious activities and potential threats.

The SCADAfence Platform's Preventive Approach

Handling incidents once they happen is very expensive (today's malware and hacking attacks spread in a matter of hours and can cripple entire production and production-supporting processes). On the other hand, infiltration and preparation for the attack can take weeks and months.

Therefore, SCADAfence is equipped with a full suite of features, under one umbrella called “Exposure Analysis”, that is constantly analyzing the network traffic and presenting network and security personnel with exposure and threat related information. The information is tailored to their organizational processes, visualizes traffic between their network segments, and provides prioritization of assets according to threat related metrics. This helps identify threats before they are fully deployed and prevent the next security incident.

The SCADAfence Governance Portal

The SCADAfence Governance Portal enables the IT and OT departments to centrally define and monitor the organizational adherence to organizational policies and to OT related regulations. The solution is easily deployed, is not intrusive, and does not jeopardize the process availability in any of the OT sites.

The solution is configured and managed from a central location, and aggregates compliance information from all sites in the organization. It also connects to other security systems, providing a cross-organizational, comprehensive compliance posture.

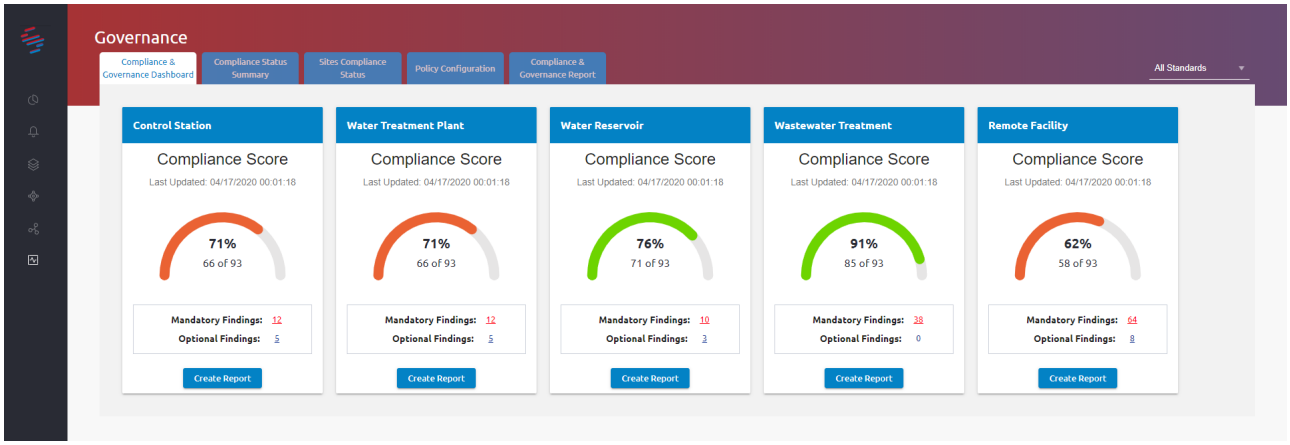


Diagram #3: The SCADAfence Governance Portal’s Compliance Score Dashboard

About SCADAfence

SCADAfence is the global technology leader in OT & IoT cyber security. The SCADAfence platform enables organizations with complex OT networks to embrace the benefits of industrial IoT by reducing cyber risks and mitigating operational threats. The non-intrusive platform provides full coverage of large-scale networks, offering best-in-class detection accuracy, asset discovery and governance with minimal false-positives. 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 manufacturing, building management and critical infrastructure 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