Tripwire Industrial Visibility in the Chemical Industry

Multi-Unit Agrochemical Plant

The cyber threat landscape for operational technology (OT) networks is changing rapidly. The classic nation state threat actors are now joined by multiple groups that are leveraging newly disclosed attack tools (such as the ones leaked from the NSA trove by The Shadow Brokers). New threats include both cybercriminals executing impactful ransomware campaigns as well as the rising potential for terrorists to leverage widely available and sophisticated tools and techniques to cause harm.

During the second half of 2017, adversaries using leaked tools disabled numerous OT networks. Unlike nation state threats, the recent attacks did not specifically target plants. However, the indirect or "overspill" damage from these ransomware attacks on various manufacturing plants have mounted to hundreds of millions of dollars. The bottom line is that multiple new and potentially potent threats exist that chemical plant asset owners must now monitor for and actively defend against.

Within the OT ecosystem, the chemical industry features a fundamental dependency between process control and human and environmental safety. The production of fertilizers, plastics, pesticides and petrochemicals entails the storage and processing of toxic materials, which necessitates additional safety responsibilities on top of plant reliability and productivity requirements.

According to Eric Cosman, an industry leader in cybersecurity for industrial systems and a recognized expert in chemical manufacturing controls:

"Virtually all chemical plants have some sort of computer-based automated control system. If you somehow compromise [that system], bad things could happen depending on the nature of the plant—that could range from spills of material to some sort of overpressure or venting, or, in the worst case, even some sort of explosion."

Chemical companies worldwide are acknowledging the rising risk of a cyberattack on their industrial network and the impact an attack can have on the safety and reliability of industrial processes. For example, cybersecurity is natively integrated in the U.S. Responsible Care® Security Code. Advanced organizations are responding with specific efforts to enhance the cybersecurity posture of their industrial networks. However, securing a chemical facility network holds several unique challenges, related mostly to how these networks are designed, built and maintained.

A typical chemical facility network consolidates several production sites into a single network, typically with no logical isolation between sites. As a result, many endpoints within these networks can serve as a stepping stone, enabling attackers to access multiple sites. Additionally, routine maintenance activities, such as firmware upgrades, security patches and network troubleshooting are carried out independently by external contractors who often accessing these networks remotely, providing adversaries with additional attack vectors.

Unmonitored remote connections, combined with the production sites internal connectivity create additional security blind spots that often go unnoticed and unattended due to lack of a working culture between the process control and the IT networking teams, and the lack of technology providing visibility into OT network configuration and traffic. The resulting lack of coordination and visibility exposes chemical plants via an expanded attack surface.

This document provides an example of an agrochemical plant's physical and network structure, followed by the security concerns and threat scenarios raised by the plant's team. It then shows samples of the findings and explains the risk mitigation role of threat detection solutions.

Plant Description

Physical Architecture

The plant produces vast assortment of products—insecticides, plant-protection, raw chemicals for various industries, and others—which involve the processing of highly toxic materials. There are 12 production units within the site, nine of them currently active.

Each production unit has its own local control room with two Windows machines acting as both a human machine interface (HMI) and an engineering workstation (EWS). The standard routine is that major changes (such as between batches) are performed by the central team, while minor adjustments are carried out internally using Online Edits. Each site comprises 10–12 controllers in an outdoor cabinet, connected to approximately 1000 remote I/Os.

All production units send data to a central control room for a holistic view of the entire plant's activities. There is a dedicated team manning the central control room, governing overall continuity and configuration changes within the production sites.

Network Architecture

Process Logic vs Network Logic

The nine production units operate independently from each other—the various sites are not logically separated from each other and feature various connections between sites.

The reason is simple: As in many chemical plants of its kind, there is no in-house networking team. The initial building of the network was carried out by the turnkey contractor that was commissioned when the plant's network was shifted to Ethernet. The contractor chose the most cost-effective networking implementation that would keep all assets connected. Maintenance activities throughout the years were conducted by external contractors as well. This resulted in a significant mismatch between the network topology and the production logic. While this gap does not bear any implication on the plant's productivity, it introduces multiple redundant unmonitored connections and cross-site connections, which threat actors can leverage for sustained presence and lateral movement.

Remote Connections

Both the central control room and the sites networks feature occasional internet connections to various third parties—automation vendors, network technicians and software providers. These connections are not monitored in the central control room and do not abide to a central access policy.

State of Network Visibility

The plant's control team knows which controllers govern each process due to the local and central HMIs that fully capture all process data in real time. However, there is no equivalent visibility into the underlying networking infrastructure and to the network's actual exposure to the internet.

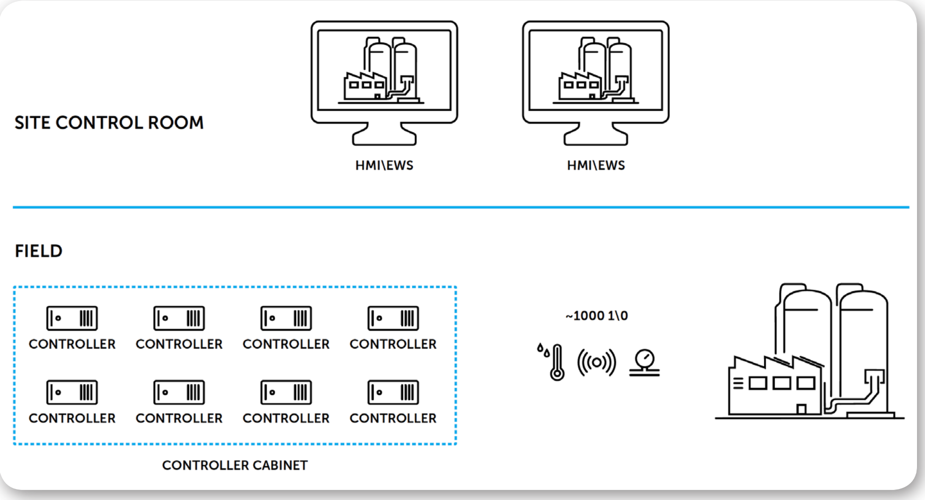


Fig. 1 Site: Controllers, machines

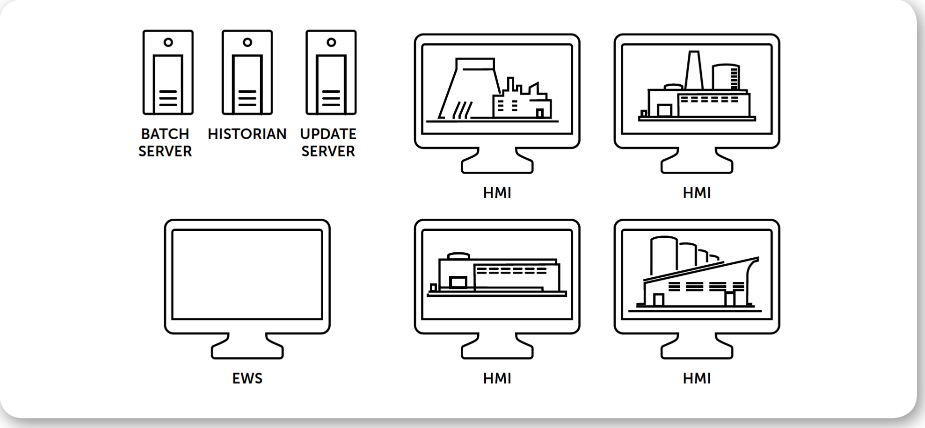


Fig. 2 Central + sites

Cyber Threat

Non-targeted attack

- **Description:** Non-OT malware shutting down or slowing performance of OT Windows machines (HMIs, batch servers, historians, etc.)
- **Vector:** Internal people or third parties using an infected computer to perform maintenance activities

Impact

- **Dysfunctional HMI**: Loss of functionality would probably lead to a shutdown until the HMI becomes functional again, through either malware removal or machine reimaging.
- **Dysfunctional batch server**: Compromise of data and system integrity: Various regulations require detailed documentation of all process stages. Failing to comply with these requirements could result in disqualifying the entire batch and production would be halted until the batch server is restored to operational routine, compromising data and system integrity.
- **Degraded performance of HMI/batch server**: Malware which consumes the HMI/batch server CPU would cause slower response and result in degradation of batch quality. Discovery of this issue would depend on the plant's quality assurance process. Failing to discover it would result

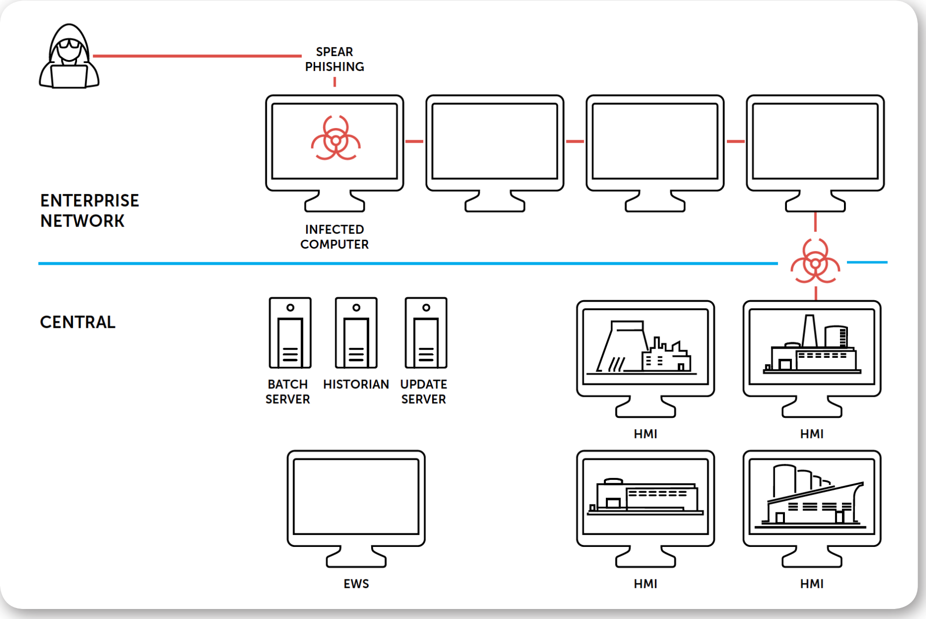


Fig. 3 Non-targeted attack

in shipping lesser quality products, damaging the brand, and exposing the company to liability claims.

Unlike the previous dysfunction scenarios, a more rigorous investigation would be required to isolate the problem's root cause and pinpoint the infected endpoint, eliminate the malware and close the security gap that enabled the initial infection.

Targeted attack

Description: Purpose-built attack on the plant's OT network, leveraging its built-in security weaknesses. Threat actors would aim at causing high-profile physical damage to equipment, environments or, in extreme cases, even human safety.

Vector

- **Physical:** The site's large size enables attackers (insider or external) to approach the controllers in stealth and perform logic changes through a USB drive.
- **Network:** The OT network architecture introduces various attack surfaces for both initial compromise and prolonged damage. As explained before, the standard routine in the plant is that configuration downloads are carried through the EWS in the central control room, while minor parameter adjustments are owned by each site's control teams, which use Online Edits from a single Windows machine that contains both HMI and EWS software. An attacker that successfully compromises one of these local site machines could easily leverage its EWS software to download a rogue configuration code, changing the process values.

Impact

- **Release of toxic materials in the plant:** Endangerment of human safety and downtime until the plant is cleaned
- **Release of toxic materials to the environment:** Considerable environmental damage, heavy costs of cleaning and restoration activities, as well as exposure to legal claims

Tripwire Solutions

Deployment Plan

Tripwire provides fully integrated cybersecurity solutions purpose-built for OT systems:

- **Tripwire Industrial Visibility**: Passive monitoring for real-time detection of malicious presence and activity with deep packet inspection (DPI) capabilities
- **Tripwire Industrial Visibility Management Hub**: Centralized management interface that

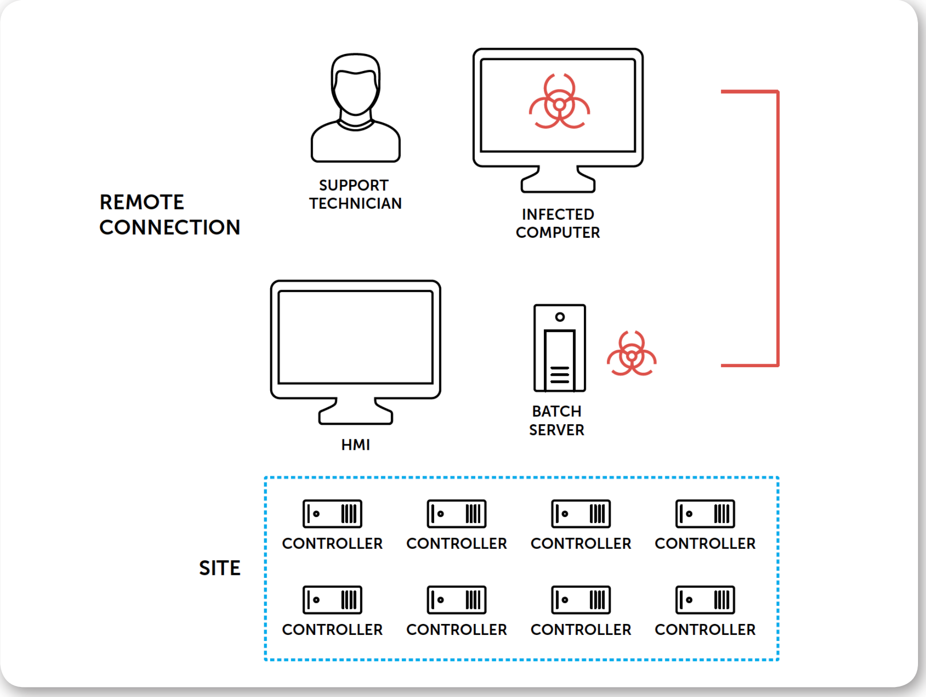


Fig. 4 Non-targeted attack

aggregates the data from multiple sites and displays a unified view of their assets, activities, alerts and access control

Tripwire Industrial Visibility

Tripwire Industrial Visibility passively gathers and analyzes network data—basically listening to all the communications to discover assets (e.g., controller, HMI, remote I/O, engineering stations, and networking gear) and to build a detailed "baseline" model of normal network operations. Different assets generate network traffic in varying time intervals, depending on the specific function of the asset and the environment. The common time frame required for the entire set of OT assets to generate their routine traffic is approximately two to three weeks.

Initially, Tripwire Industrial Visibility is configured to run in learning mode to learn the network's standard behavior and establish a behavioral baseline. During this learning period, the Tripwire team reviews the aggregated findings with the customer, sharing immediate insights about the OT ecosystem. These insights range from pure security findings—such as insecure remote connections, inadequate segmentation, or weak passwords—to various server misconfigurations that affect operational workflow.

During the learning period, it is important to be aware of the possibility that the environment might be already compromised. The Tripwire deployment team ensures that any malicious presence is detected, remediated and prevented from being absorbed in the baseline.

Once training mode is complete, Tripwire Industrial Visibility shifts to operational mode, where the system provides real-time monitoring and raises an alert upon detection of deviations from the baseline. For example, Tripwire Industrial Visibility can generate an alert when a new device is plugged into the network (e.g., a contractor laptop), when critical changes are made (e.g., a PLC configuration download or PLC mode change), and when malicious activity is detected on the network (e.g., port scan, man-in-the-middle, unknown/anomalous traffic).

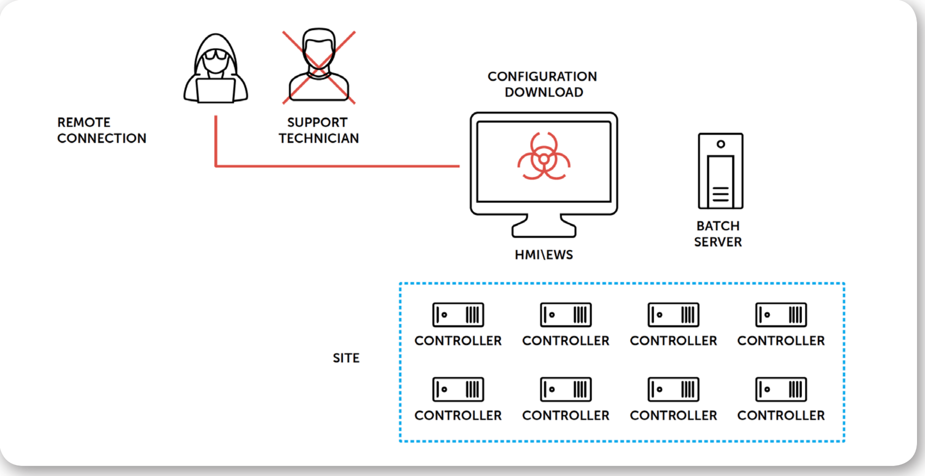


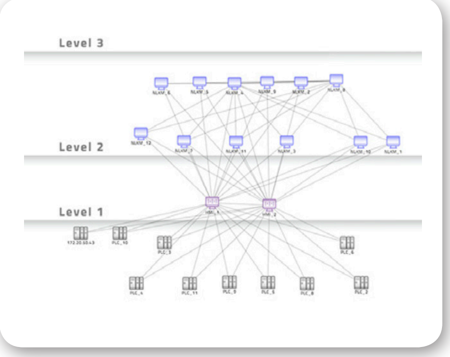
Fig. 5 Targeted attack

Tripwire Industrial Visibility ultimately enables customers to track changes and to rapidly detect, investigate and respond to security incidents and potential operational issues.

Sample Site Findings Using Tripwire Industrial Visibility

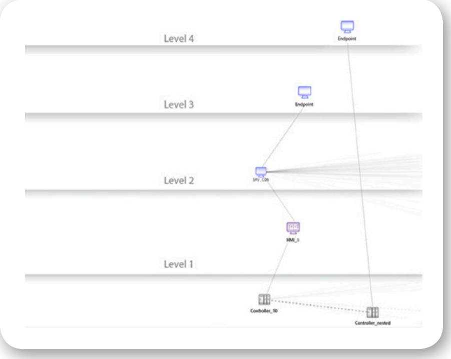
Sample Site Network

This network graph shows the typical network layout of a production site in the facilities and the connections between assets in various levels (the remote I/Os are omitted here).



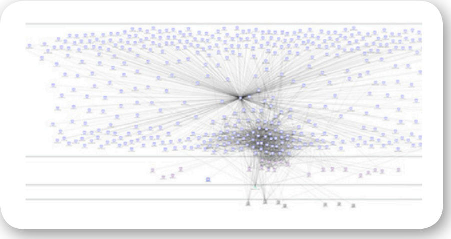
Nested Asset Communicating with DMZ

Nested assets present a security challenge that can only be addressed through knowledge of both OT and cybersecurity domains. The nested controller (Level 1 bottom) uses a network card to communicate with the HMI/EWS via the nesting controller (Level 1 top). However, it has an additional network card through which it communicates independently with a Windows machine in the DMZ—most probably for remote vendor maintenance activities. This is a security gap because compromise of the DMZ machine can open a path to a controller and through it to the entire site's network.



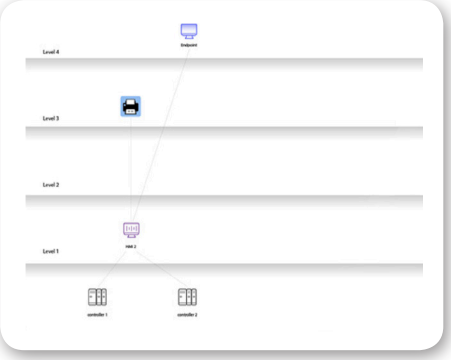
Open SMB Ports

SMB is a common vector for self-propagating malware (the classic example is Conficker, but two prominent attacks in 2017—WannaCry and NotPetya—have utilized it as well). As the screenshot here shows, SMB traffic is present in nearly all nodes in the sample facility's OT network. The immediate action item is to limit SMB traffic to only the nodes that essentially need it, and closely monitor their respective traffic.



Non-Monitored Remote Connections

Site operators often have no way of knowing if these outbound connections of control level nodes are leveraged by threat actors to enter the network.



Conclusion: The Tripwire Difference

Tripwire's solutions can address the most critical cybersecurity challenges that chemical customer face: monitoring the network's internal traffic to detect malicious presence and actions and monitoring the multitude remote access connections the plant's network encloses.

It is only through visibility and control of all assets and traffic that a true shift in security posture can occur. Tripwire rises to this challenge with fully-integrated solutions that provide security insights to enhance the network's security hygiene, advanced filters for proactive threat hunting within the network, real-time anomaly detection that pinpoints any critical changes in network traffic and monitoring for remote connections.

As a Belden company, Tripwire is uniquely positioned to bridge the cybersecurity gap between your IT and OT environments. Tripwire Industrial Visibility is a vendor- agnostic solution and can identify potential risks that can impact the resiliency of your industrial control network and identify threats that can negatively impact safety, productivity, and quality.

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **Learn more at tripwire.com**

***The State of Security*: Security news, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook