Tripwire Industrial Visibility for Power Generation Plants

Power Plant Gains Deep Visibility

As a fundamental critical infrastructure component, electric utilities are a distinct target for threat actors that seek to disrupt the day-to-day life of citizens. The increasing interconnectivity between automation control systems and IT networks across power generation, transmission and distribution introduces a growing attack surface within the electric utilities ecosystem and introduces a security imperative upon the industry's key stakeholders worldwide.

Power generation plants are a major part of the electric utilities ecosystem, and will be discussed in detail in this paper. Power plants vary greatly from each other, in terms of fuel, size and age, but all of them utilize operational technology (OT) networks to govern the critical processes that they manage. Due to their role as critical infrastructure, power generation plants were the first to be required to comply with various OT cybersecurity regulations.

Tripwire can secure the safety and reliability of operational networks running critical processes, like the industrial control systems that power plants rely upon. As such, Tripwire is the ideal partner for a power generation company that seeks not only to comply with regulatory requirements, but to increase its cybersecurity posture by gaining the ability to detect and respond to targeted malicious activity.

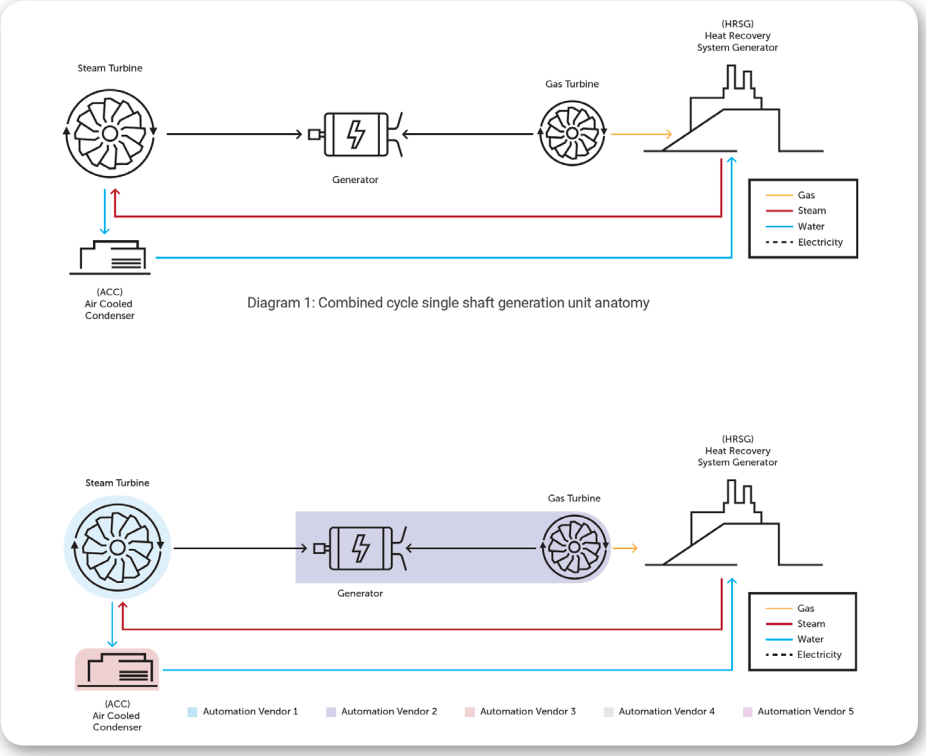

Fig. 1 Combined cycle generation unit OT network

This document illustrates challenges and solutions that are both unique to the power generation sub-segment, as well those that apply to the broader context of OT cybersecurity. It then describes how Tripwire's industrial solutions can secure these types of environments.

Electric Generation: Combined Cycle Power Plant

A power generation unit is a multi-component environment, consisting of a core—turbine and generator—and various auxiliary systems that handle the energy availability and utilization.

The nature of these systems varies per the generation unit energy source—thermal, hydro, etc. Power generation units are commissioned by an engineering, procurement and construction (EPC) contractor. The commissioning process involves independent bidding for each of the unit's components, as well as their respective automation networks.

Specifically, a combined cycle generation unit includes both gas and steam turbines, and uses the excess thermal heat of the former to generate steam for the latter. The main auxiliary components include:

- Heat recovery steam generator (HRSG) that captures the excess heat to generate steam from water and streams it to the steam turbine.
- Condenser that captures the excess steam from the steam turbine and condenses it back to water. This water

is then streamed back to the HRSG for another reheating cycle.

It is common for EPC contractors to commission generation units in which each of these components are manufactured by a different vendor. In respect to the EPC bidding strategy, the corresponding automation systems are either embedded by the equipment vendor or bid separately. Thus, a standard combined cycle generation unit will typically feature a complex multi-vendor and multi-protocol OT network.

This section describes security challenges on a single shaft 1X1X1 unit, in which one gas turbine and one steam turbine share a common generator.

Security and Operational Challenges

The sound operation of the generation unit relies on the integrity of its OT networks. This system gathers, processes and acts based on real-time temperature, pressure and flow data. An attacker seeking to inflict long-lasting damage on a power plant would likely refrain from a movie-style "hit and run" approach.

Indeed, power plants are typically designed with sufficient redundancy to withstand a sudden component failure. The approach taken, from a determined attacker, would likely be to inflict continuous small-scale damage, which aggregates over time into severe damage to equipment and plant safety.

Attack Lifecycle

Based on pre-attack reconnaissance efforts, an attacker would typically know in advance what systems within the generation unit to target. However, the attacker would try to establish an initial foothold on the most vulnerable point, which is not necessarily part of the desired system. There are numerous entry point possibilities, from outdated Windows XP engineering stations to misconfigured servers or endpoints that initiate internet facing communication.

Upon completion of the initial compromise, the attacker would begin to carefully explore the environment and seek a path to the system it has predefined as the desirable target. This path varies in respect to the initial compromise vector, but it will typically include breaching an engineering station and altering the configuration of a programmable logic computer (PLC).

Combined Cycle Targeted Attack Example

Let's illustrate the statements above with a concrete combined cycle generation unit example:

Bypass System

The bypass system is a critical component in combined cycle generation units. Its main purpose is to isolate the steam turbine from the flowing steam, which is accomplished by redirecting the superheated steam to dedicated piping leading to the condenser. Steam bypassing is necessary during startup, shutdown or steam turbine trip.

Startup and shutdown require the use of the bypass system due to differences between the gas and steam turbines. The gas turbine takes a considerably shorter time frame to achieve full operating speed, verses the steam turbine which should not be started before the metal in the rotor and blades reaches the steam temperature. Thus, the gas turbine's excess thermal energy is available to the HRSG steam generation before the steam turbine can accept it.

In this case, the bypass system redirects the generated steam directly to the condenser.

In a similar manner, in a controlled shutdown, the bypass system enables the steam turbine to be taken offline at its own pace, increasingly reducing the provided steam load. However, in a case of an emergency trip, the bypass system will be operated immediately in full gear.

Bypass System Controls

The tasks of the control system involve the throttling of the redirection, pressure letdown and attemperation valves. The orchestration of these operations relies mostly on processing of temperature and pressure data. Typically, the respective PLC set-points are determined and configured upon the initial system setup. Malfunction of the bypass system directly impacts the lifespan of generation unit components—exposing the turbine metal to thermal stress and undermining the metal's reliability. Another example is a scenario in which the bypass system operates as expected, but a failure occurs in the process of steam attemperation. In this case the condenser will be exposed to steam at a temperature level it is not equipped to handle.

We have now established why the bypass system might appeal to an attacker. In addition, let us remember that this system is not part of the day-to-day routine operation of power plants, and changes that an attacker inflicts on its respective PLC's set points will not have

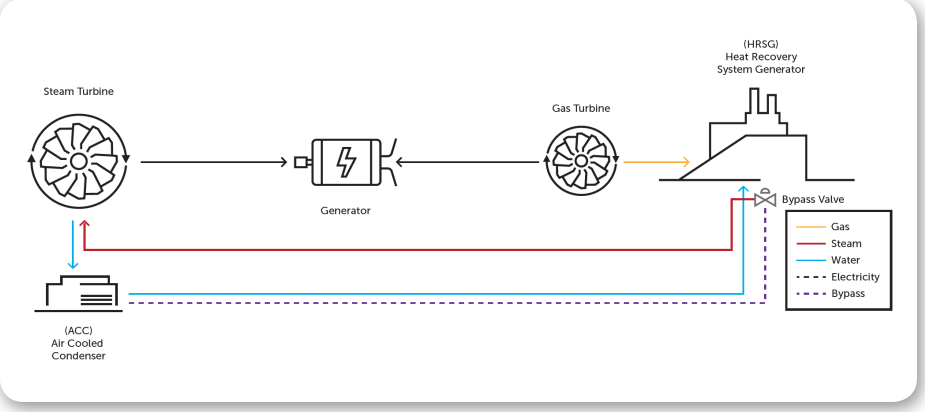

Fig. 2 Parallel bypass diagram

immediate disrupting effects, and thus will likely go unnoticed by the generation unit operators.

Attack Vector 1: Attacking the Bypass Valve

Object: Damage the steam turbine

Method: Causing the steam turbine to start prior to metal parts reaching required temperature

Path: The PLC sends the valve actuator open/close instructions that are based on temperature data it receives from the steam turbine's I/O. Once the metal temperature in the steam turbine reaches the required temperature, the PLC instructs the actuator to open the bypass valve and assume standard steam flow from the HRSG to the turbine.

The attacker alters the temperature set points in the engineering station of the respective PLC, causing the redirection valves to prematurely cease bypass and allow superheated steam to flow into the turbine.

Attack Vector 2: Attacking the Steam Conditioning Valves

Object: Damage the condenser

Method: Allowing superheated and high pressure steam to enter the condenser

Path: The temperature and pressure of the superheated steam from the HRSG must be reduced prior to entering the condenser. This process is known as steam conditioning, and involves the use of attemperation and pressure letdown valves on the steam prior to its entering the condenser. Steam conditioning is required, because the condenser is initially built for the post turbine excess steam which features significantly lower temperature and pressure levels.

Introducing superheated high pressure steam to the condenser would cause aggregated damage to its metal parts.

The PLC controls the throttling of the valves based on steam temperature and pressure data. Similar to the scenario above, the attacker lowers the temperature set points in the engineering station of the respective PLC, causing the spray valve to prematurely cease and exposing the condenser to superheated steam it is not designed for.

What enables such an attack to succeed is the lack of sound monitoring tool for OT networks. Without visibility into network communications, attackers can reside undetected, learn the network topography, understand system behavior and gain the knowledge required to inflict harm. Having visibility includes, for example, knowing when a high-risk change to a set point on a key PLC happens. But it also includes visibility into the actions and activities of an attacker before the attack—when the adversary is trying to interrogate the environment and move laterally to the target.

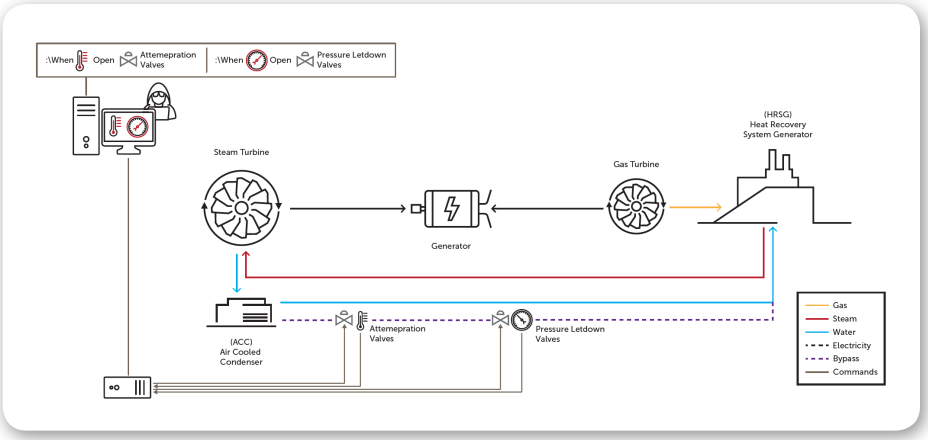

Fig. 4 Attacking the steam conditioning valve

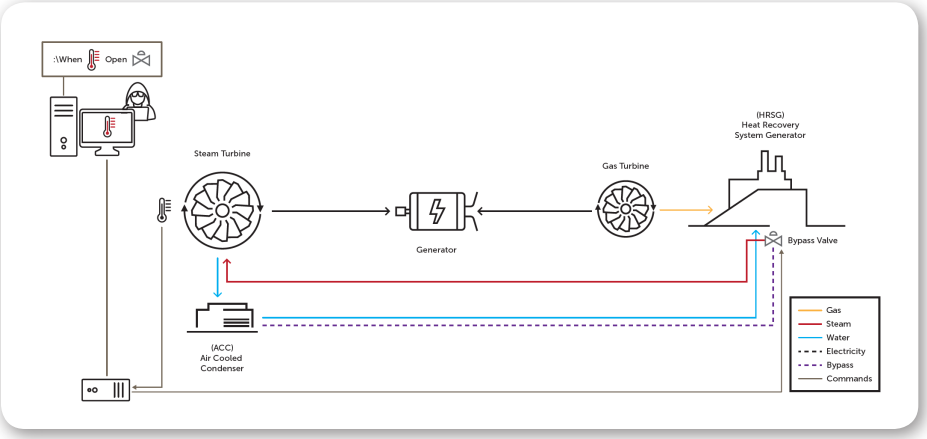

Fig. 3 Attacking the bypass valve

Tripwire's Solution

In this section, we describe Tripwire's deployment process to address the various vulnerabilities faced by the power generation sub-segment.

Deployment Process: Preparatory Steps

The Tripwire solution can be deployed on top of any networking infrastructure. However, Tripwire's recommendation is to use managed switches that are capable of relaying replicated traffic through a switch port analyzer (SPAN) port.

Deployment Process: From Learning to Operational Mode

Tripwire gathers and analyzes network data—basically listening to all communications to discover control and other assets (e.g., PLC, HMI, remote I/O, engineering stations and networking gear), and builds a detailed "baseline" model of the 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 2–3 weeks.

Initially, Tripwire® Industrial Visibility is configured to run in learning mode to learn the networks' standard behavior and establish a behavioral baseline. During this learning period, the Tripwire team reviews the aggregated findings with the customer—sharing immediate insights on the OT ecosystem. These insights range from pure security findings, such as insecure remote connections, inadequate segmentation, or week 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 learning mode is complete, Tripwire 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 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).

Tripwire enables customers to track changes and to rapidly detect, investigate and respond to security incidents and potential operational issues, allowing the entire OT network to be visible and monitored through a single console.

Operational Mode – Security Demonstration

Overall Generation Unit Protection

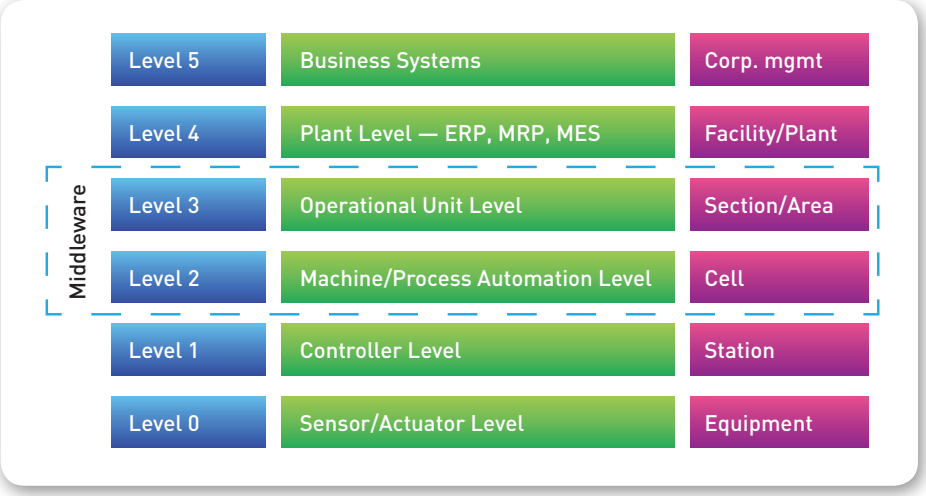

Fig. 5 ISA-99 Purdue model

Tripwire can monitor all traffic on combined cycle generation units—turbines, generators, condensers, HRSGs and balance of plants (BOP)—discovering and identifying all PLCs, industrial switches, engineering workstations, HMIs and other various components within the OT network. Since displaying the entire system on a single graph creates a crowded view, we show an overview of the HRSG and condenser ecosystem.

The Purdue Model outline enables the team to intuitively see the assets' distribution and relations across the different production layers. It should be noted that due to high volume (~1000 per each PLC), we have omitted the remote I/Os from this graph.

Tripwire can also zoom in on the specific PLCs that control the bypass and steam conditioning valves to view descriptors (including utilized communication protocols, their immediate ecosystems, exchanged communications and more). With this information, customers are able to pinpoint their most vulnerable assets. For example, they may find that their PLC is communicating with a critical engineering workstation.

With this sort of information, Tripwire Industrial Visibility can further evaluate the ecosystem and operating details of the critical workstation. In operational mode, Tripwire can define all of its standard communication as a baseline. Assuming an attacker manages to compromise the asset and gain remote code execution capabilities, Tripwire would then raise a baseline deviation alert as soon as the attacker attempts to initiate a non-baseline communication. Given that the attacker is obliged to initiate such communication to gain knowledge of, and a foothold on the targeted environment, their presence will be detected, enabling the site operators to take the asset offline and apply the required remediation procedures.

Tripwire provides extreme visibility into all the paths an attacker would take in attempting to compromise a bypass system. The ability to see every action in the network enables operators to know when an anomalous activity occurs and secure the system through efficient investigation and response. Any lateral movement or communication attempt in the bypass system related to critical assets will raise an immediate alert.

Deployment Process – Data Transfer

The concluding step in the deployment process is to send data from the remote power plant to the customer's security operations center (SOC), where the Tripwire Industrial Visibility Management Hub would be installed. If additional layers of security are required, Tripwire can send the data generated at the local site

to the Tripwire Industrial Visibility Management Hub over a data diode for a secure transfer. A data diode is an appliance that physically enforces data to travel in only one direction – in our case, from Tripwire's installed virtual appliance in a power plant through VPN over the Internet to a SOC network. The use of a data diode mitigates the risk of attackers leveraging Tripwire's internet connection as an attack vector and ensures that the centralized multi-site display does not impact a site's security posture. As shown in the figure below, Tripwire supports Hirschmann's data diode, along with many others, to secure the data transfer.

Tripwire Benefits for a Power Plant's OT Team:

- Overall network visibility across all monitored protocols
- Immediate detection of malicious presence in the OT network
- Detailed asset information of PLCs, HMIs, engineering and networking infrastructures.
- Process management - configuration change/logic download, etc.
- Ability to conduct an internal security assessment without operational disruptions

We have intentionally focused on specific likely attack scenarios to power generation plants to demonstrate how Tripwire's capabilities reduce these risks. However, Tripwire's extreme visibility capabilities would enable plants to respond with similar efficiency to other threat scenarios that involve critical OT assets. Currently, OT operators do not have the tools to provide visibility or real-time monitoring for the networks they are accountable for. This makes it extremely easy for attackers to establish an initial foothold and move laterally until they reach their target. Tripwire turns the table on attackers and enables plant operators with real-time detection, preventing adversaries from undermining the safety and reliability of their production systems.

Get a Demo

Let us take you through a demo of Tripwire Industrial Visibility and answer any questions you have. Visit **tripwire.com/contact/request-demo/**

As a Belden company, Tripwire is uniquely positioned to bridge the cybersecurity gap between your IT and OT environments. Tripwire solutions integrate seamlessly with the industrial products you already have in play, like Tofino firewalls and Hirschmann switches.

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

CSTIVPG1a 1910