# Industrial Networks Secured

## Our Mission

Claroty was conceived to secure the safety and reliably of OT networks that run the world's most critical infrastructures.

Claroty empowers the people who run and protect industrial systems to make the most of their OT networks.

By discovering the most granular elements, extracting the critical data, and formulating actionable insights, Claroty provides extreme visibility and brings unparalleled clarity to OT networks.

## Your Result

Better security, efficiency and integrity for your critical OT environments.

www.claroty.com



CLAROTY
Clarity for OT Networks

**Power Generation Case Study**
Combined Cycle Power Plant

# Forward

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 OT network 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.

Claroty was conceived to secure the safety and reliability of operational networks running critical processes, like the industrial control systems that power plants rely upon. As such, Claroty was the ideal partner for a power generation company that sought 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.

This case study, focuses on one of Claroty's power plant installations. It 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.

# 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. Our case study relates to a **combined-cycle generation unit.**

A combined cycle generation unit includes both gas and steam turbines, and use the excess thermal heat of the former to generate steam for the latter.

The main auxiliary components include:

- **Heat Recovery Generation System (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 case study describes Claroty's deployment process on a **single shaft 1X1X1** unit, in which one gas turbine and one steam turbine share a common generator.

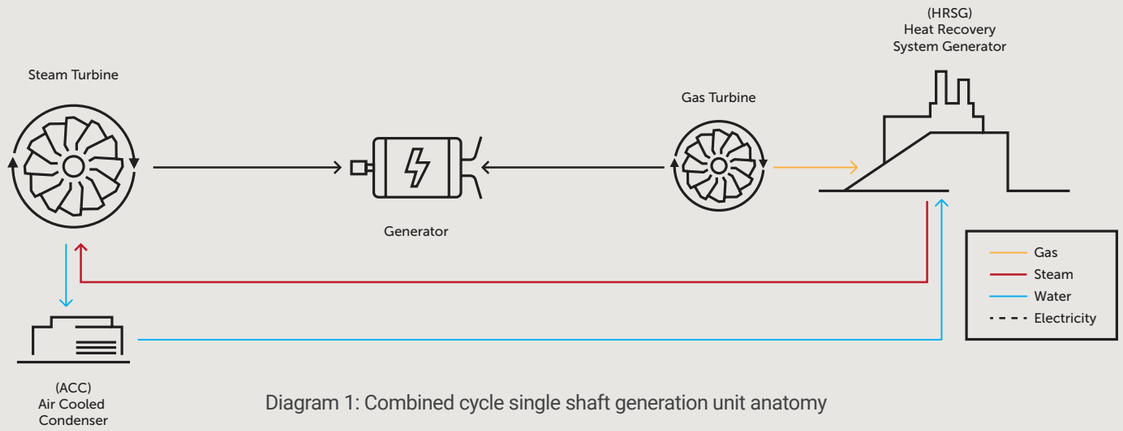



Diagram 1: Combined cycle single shaft generation unit anatomy

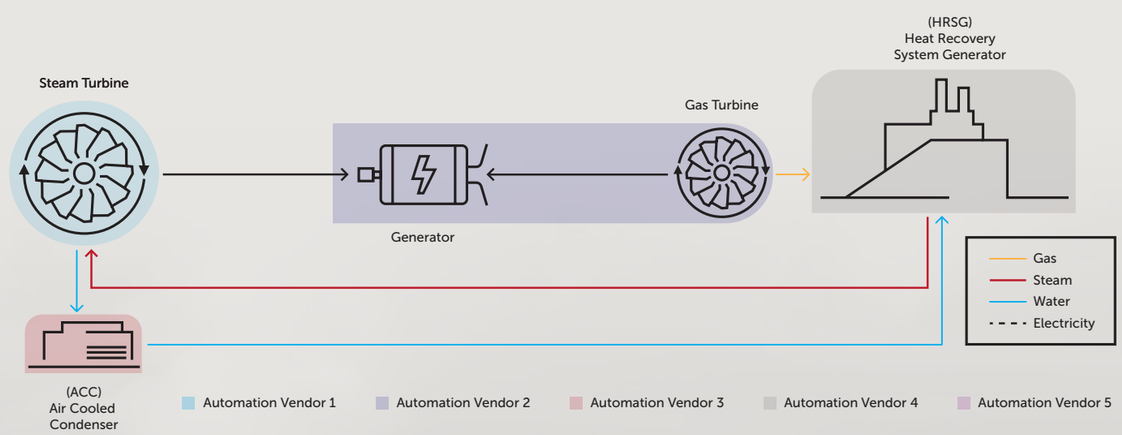



Diagram 2: Combined cycle generation unit OT network

# Security and Operational Challenges

The sound operation of the generation unit relies on the integrity of its operational technology (OT) networks. This system gathers, process 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 Life cycle**

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 XP engineering stations to misconfigured servers, or endpoint 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 PLC.

**Combined Cycle Targeted Attack Example**

Let us illustrate the above with a concrete combined cycle generation unit example.

**HP 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 start-up, shut-down or steam turbine trip.

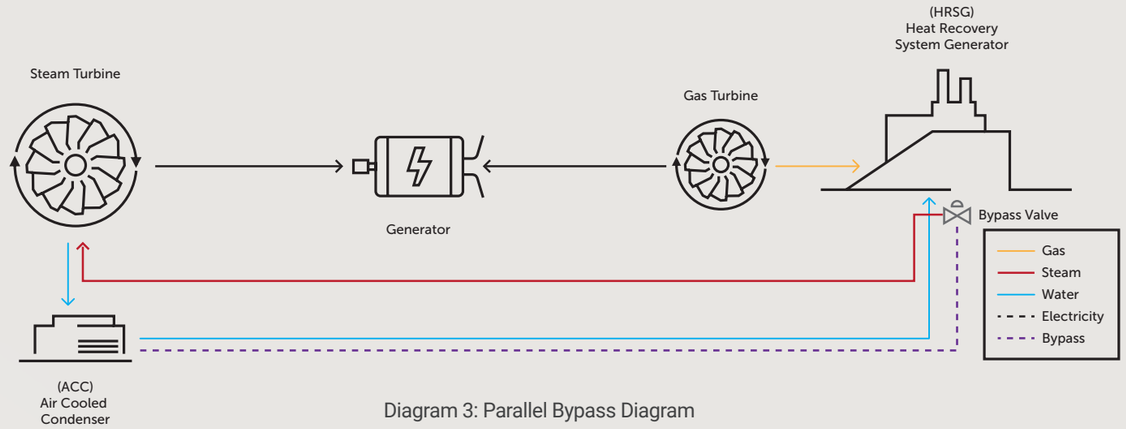



Diagram 3: Parallel Bypass Diagram

Start-up and shut-down require the use of the bypass system due to difference between the gas and steam turbines. The gas turbine takes a considerably shorter timeframe 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.

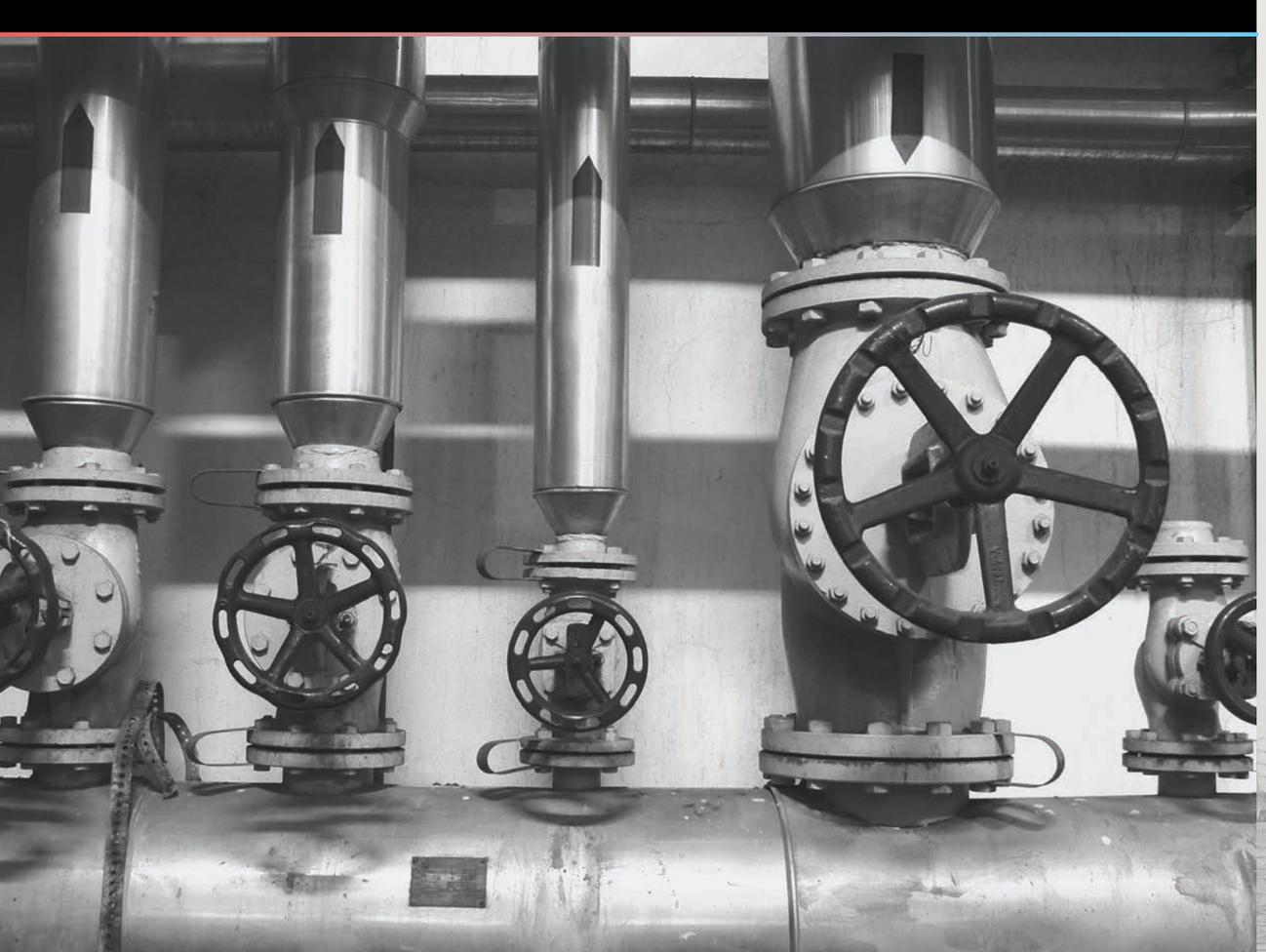
In a similar manner, in a controlled shutdown the bypass system enables the steam turbine to be taken offline at its own pace, increasingly reducing the provided steam load. However, in a case of an emergency trip, the bypass system will be operated immediately in full gear.

## 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 the power plant, and changes that an attacker inflicts on its respective PLC's set points will not have immediate disrupting effect, 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.

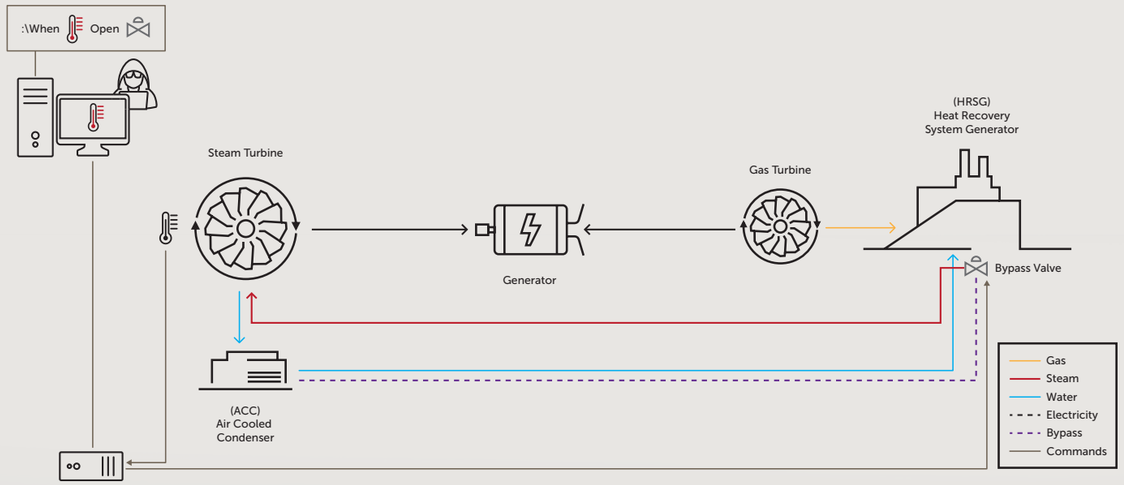



Diagram 4: Attacking the Bypass Valve

## 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 base 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.

We will now zoom into an actual case study which brings together most of what we have discussed so far. Claroty was contacted by a power plant operator, seeking a solution to increase the security posture for its combined cycle generation units. Let us examine, how it was done.

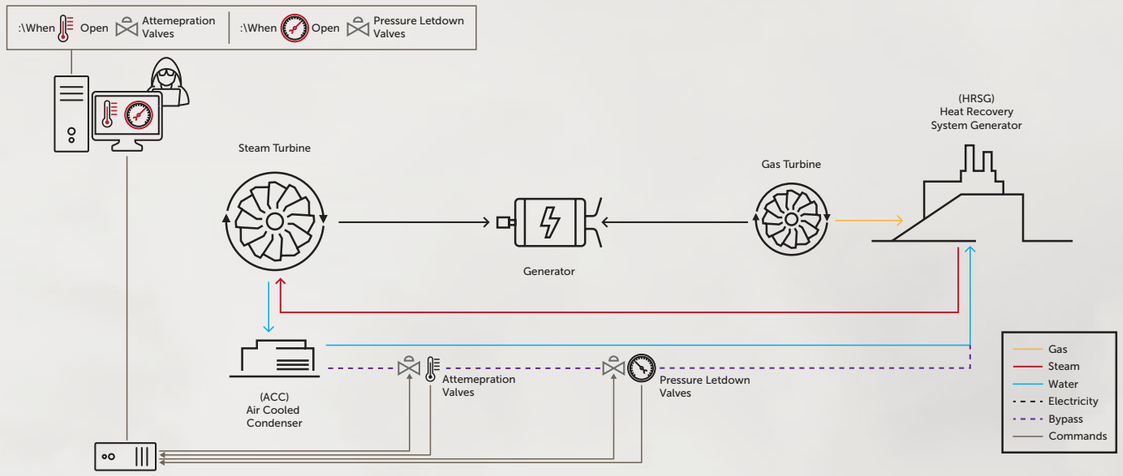



Diagram 5: Attacking the Steam Conditioning Valves

# Claroty Solution

## Deployment Process - Preparatory Steps

The customer's generation unit, follows the path we have described before, with two automation systems, controlling its main components.

| | Gas Turbine | Steam Turbine | Generator | HRSG | Condenser | Balance of Plant |
|---|---|---|---|---|---|---|
| **Equipment Vendor** | Mitsubishi Heavy Industries | Mitsubishi Heavy Industries | Mitsubishi Heavy Industries | BHI | SPX | Various vendors |
| **Automation Vendor** | Mitsubishi Heavy Industries | Mitsubishi Heavy Industries | Mitsubishi Heavy Industries | Emerson | Emerson | Emerson |
| **Protocols** | Netmation | Netmation | Netmation | Ovation | Ovation | Ovation |
| **Networking Vendor** | Phoenix Contact | Phoenix Contact | Phoenix Contact | Cisco | Cisco | Cisco |

The Claroty platform can be deployed on top of any networking infrastructure. However, Claroty's recommendation is to use managed switches that are capable of relaying replicated traffic through SPAN port.

In this case, the OT network was well constructed with a main switch aggregating the all the traffic, enabling Claroty to get all data from this switch's SPAN port.

In this section, we describe Claroty's deployment process, by walking through the generation unit auxiliary systems networks–HRSG and Condenser which are controlled by an Emerson Ovation system.

## Deployment Process – from Training to Operational Mode

Claroty gathers and analyzes network data–basically listening to all the communications to discover control and other assets (e.g., PLC, HMI, remote I\O, engineering stations and networking gear) and to build 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 timeframe required for the entire set of OT assets to generate their routine traffic is approximately 2-3 weeks.

Initially, Claroty is configured to run in training mode, to learn the networks' standard behavior and establish a behavioral baseline. During this learning period the Claroty 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 Claroty deployment team ensures that any malicious presence is detected, remediated and prevented from being absorbed in the baseline.

Once training mode is complete, Claroty shifts to operational mode, where the system provides real-time monitoring and raises an alert upon detection of deviations from the baseline. For example, Claroty 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).

The entire OT network is now visible and monitored through a single console, enabling the customer to track changes and to rapidly detect, investigate and respond to security incidents and potential operational issues.

## Operational Mode – Security Demonstration

**Overall Generation Unit Protection**

Claroty monitors all the traffic on the combined cycle generation unit – turbines, generators condenser, HRSG and Balance of Plant (BOP) – discovering and identifying all PLCs, industrial switches utilized, the Engineering Workstations/HMI's, 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/ Condenser ecosystem.

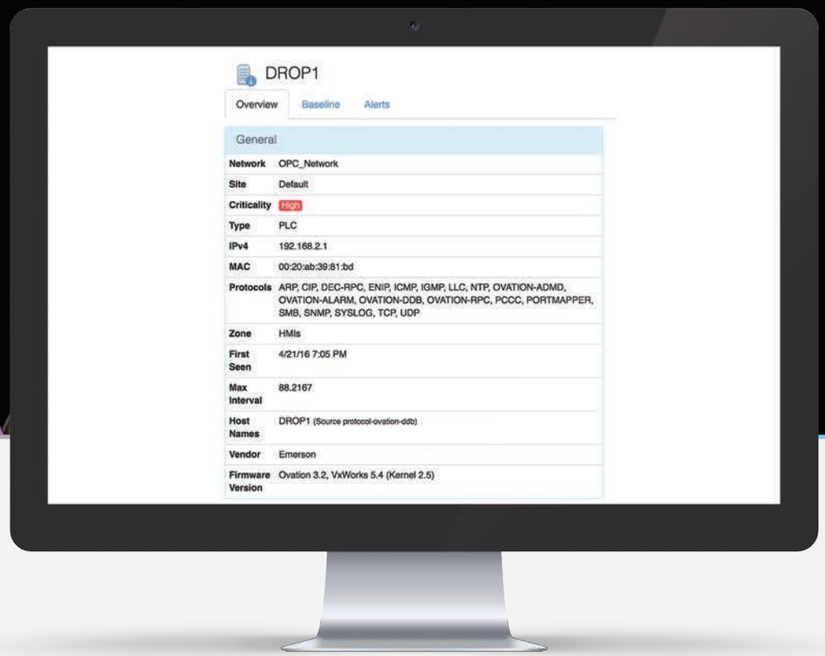
As noted before, the HRSG and Condenser are controlled by Emerson Ovation, utilizing this vendor's proprietary protocols –Ovation DDB, Ovation Alarm and Ovation RPC. Claroty parses and analyzes these protocols, providing a unified view of the entire networking ecosystem:


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 we have omitted the remote I\Os from this graph, due to their large number (~1000 per each PLC).

**Claroty vs Bypass System Attacks**

Considering the threat scenarios described above, we zoom in on the PLC which controls the bypass and steam conditioning valves. For the sake of anonymity, we have changed the PLC name to Emerson's default DROP1.

Let us examine DROP1 more deeply:

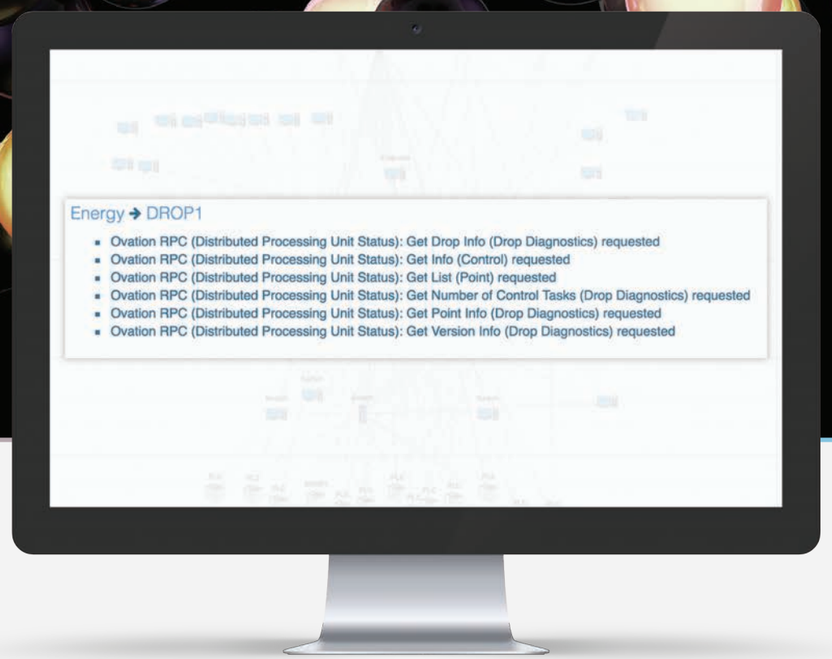



We can now view DROP1 unique descriptors. As we can see, DROP1 utilizes numerous communication protocols, of which the most interesting for our purpose is OVATION-RPC, a proprietary protocol used for standard communication between the PLC and engineering stations.

When we isolate DROP1 in the network graph we can view its immediate ecosystem:

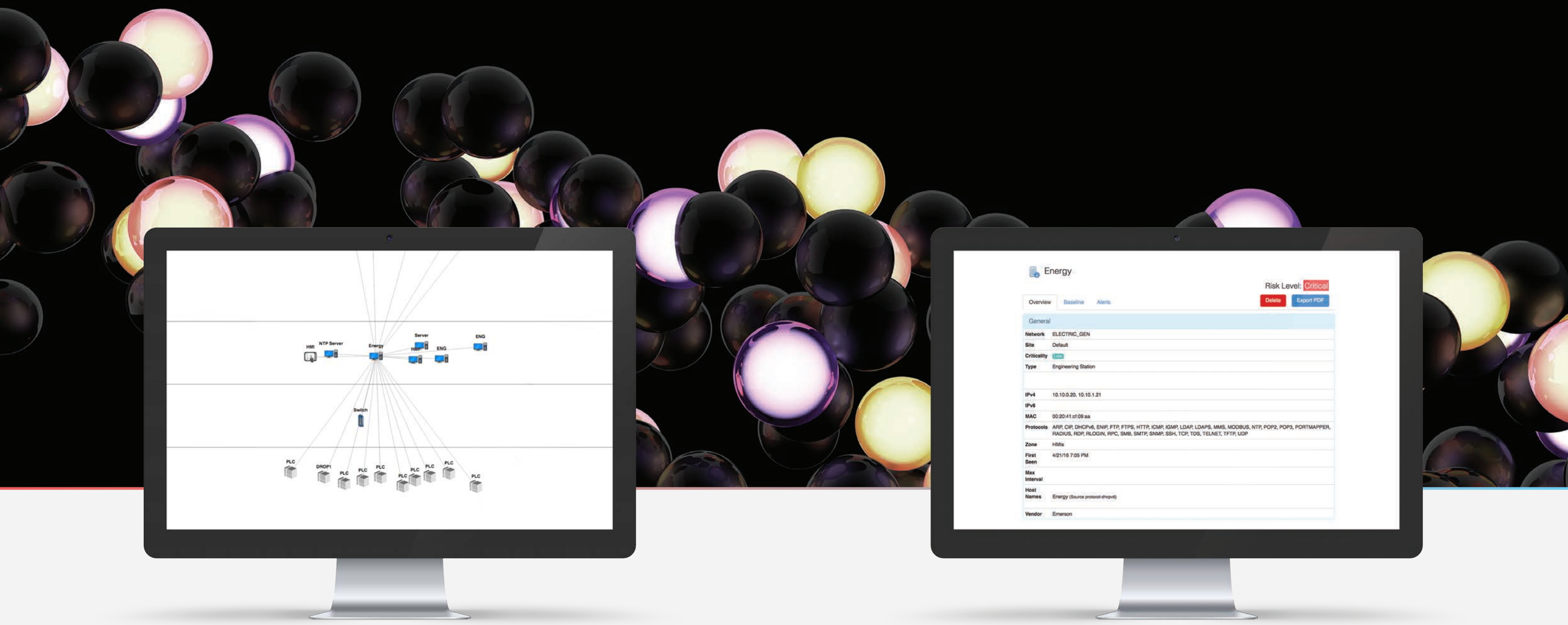

We can now see which assets DROP1 is communicating with. A quick check reveals that one of these assets is an engineering station that we name Energy.

The DROP1 baseline, shown below, reveals the standard communication that is exchanged with Energy. Here is a sample:



All of DROP1 configurations are executed by Energy, which makes it a default target of an attacker that seeks to damage the generation unit by compromising its bypass system, so let us examine the Energy ecosystem as well:

Apparently, Energy controls significant part of the HRSG/ condenser PLCs, which makes it a dominant component in the generation unit OT network. As such, it is interesting to further explore Energy:




From security perspective, it should be noted that Energy runs on Windows XP, which Microsoft dropped support for in April 2014, meaning that it is vulnerable to all the exploits that were introduced after this date.

Claroty in operational mode defines all of Energy's standard communication as its baseline. Assuming an attacker manages to compromise Energy and gain remote code execution capabilities, Claroty would 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 Energy offline and apply the required remediation procedures.

## Claroty: See Know Secure

Claroty provides extreme visibility into all the paths an attacker would take in attempting to compromise the bypass system. The ability to see every action in the network enables the operator to know when an anomalous activity occurs, and secure the system through efficient investigation and response.

In the context of this case study, extreme visibility spotlights all the potential paths an attacker might take when targeting the bypass system. Any lateral movement or communication attempt in the bypass system related critical assets will raise an immediate alert.

## Claroty Deployment Process – Data Transfer over Data Diode

So far, we have seen how Claroty delivered top down security on the generation unit level. The concluding step in the deployment process was to send this data from the remote power plant to the customer's Security Operation Center, where Claroty's Enterprise Manager is installed.

To add another security layer and to comply with local regulations, the customer required that the data Claroty generates at the local site needed to be sent to the Claroty Enterprise Manager over a data diode for secure transfer.

A data diode is an appliance that physically enforces data to travel in only one direction – in our case, from Claroty installed virtual appliance in the power plant through VPN over the Internet to the SOC network. The use of data diode mitigates the risk of attackers leveraging Claroty's Internet connection as an attack vector and ensures that the centralized multi-site display does not impact the sites' security posture.

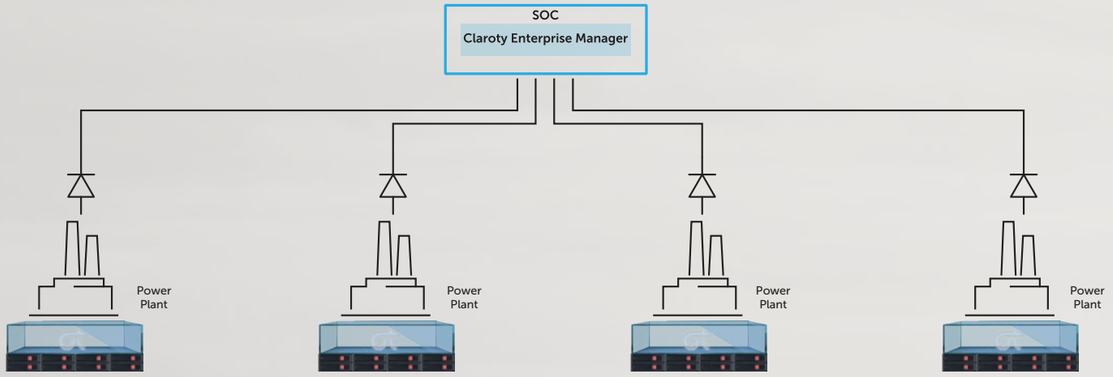



Diagram 6: Data Transfer to the SOC over Data Diodes

## End Result

The fully operational Claroty platform provided the following benefits:
Power plant OT team:

- Overall network visibility across all monitored protocols.
- Immediate detection and response of malicious presence in the OT network.
- Detailed asset information (PLC, HMI, Engineering and Networking Infrastructure).
- Process management - configuration change/logic download, etc.
- Ability to conduct internal security assessment, without operational disruption.

## Conclusion - The Claroty Difference

In this case study, we have intentionally focused on specific likely attack scenarios to demonstrate how Claroty's capabilities reduce this risk. However, Claroty's **extreme visibility** capabilities would enable the plant team to respond with similar efficiency to any 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. Claroty turns the table on attackers and subjects them to real-time detection-preventing adversaries from undermining the safety and reliability of the production system.