

THERMALWATCH[™] for Thermal Systems

Thank you for your interest in our **THERMALWATCH**[™] Program.

Through this program, we will collect a minimum set of process parameters to enable expert insight into the performance and potential optimization of your system. Our team will analyze the data with the goal of identifying opportunities to improve uptime, yield, energy consumption, repeatability and reliability of your system.

For your participation in the program, **Watlow**[®] will provide a cellular IOT gateway and support the functionality, analyze the data, and share all insights to you through a report.

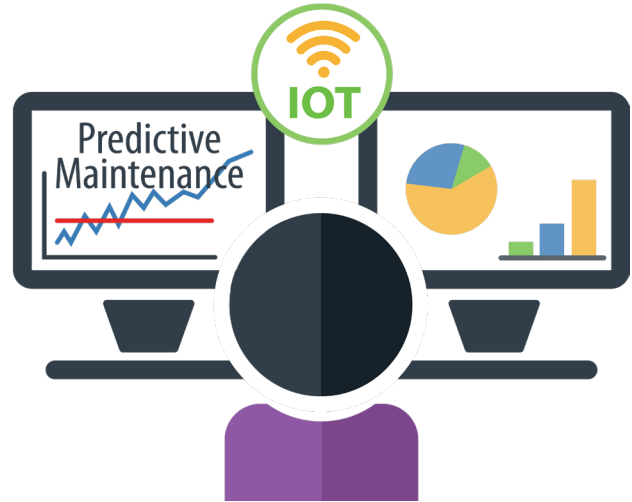
What will **Watlow**[®] deliver?

- Review and analysis of the data conducted by a data scientist and thermal system expert.
- Comprehensive monthly thermal system report showing time series graphics, statistical data, anomalies and an executive summary including insights and recommendations for system improvement. Note: Depending on the parameters captured, the report could also aid Scope 4: Avoided carbon reporting.
- Collaborative touchpoints, engineer-to-engineer, to review the data and develop context.

How will the data be collected?

The **Watlow** supplied Eurotech cellular gateway will need to be installed into (or as a side-panel addition to) your control panel, along with suitably located antennae nearby. This device will pull the desired data from your process controllers via Modbus[®] TCP/Modbus[®] RTU, aggregate the data and send it to the secured cloud via MQTT communications. A differential cellular network connection is enabled through two antennae, which would need to be installed in an appropriate location close to the furnace control panel. The device follows EN 62368-1:2014 safety standards and is rated for both RED (EU wireless comms) and FCC/ISED (NA wireless comms).

Smart Services



Utilize data from connected products in the field to improve our customer's performance and efficiency.



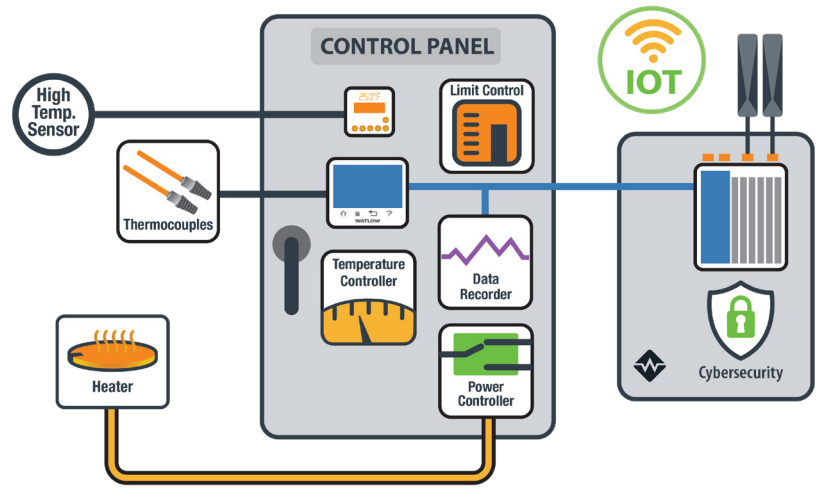
What data will be collected?

The minimum data set required would be thermocouple data (both control and monitoring), controller set point and output details, current and voltage measurements. The more process parameters that can be shared, the better quality the analytics will be.

We will also collect any contextual system data that you may like to include.

Contextual data may include, but is not limited to, flows, pressure, batch timings, heater data, door open/closed sensors, door and conveyor times, process condition changes, process output measurements and maintenance data. This data will help provide a more complete picture to understand how the thermal system affects and responds to the greater process.

Connected Products



Smart system utilize data and analytics to improve overall system performance in real-time.

Will my system remain secure?

The panel connects to the cloud through a cellular gateway, but the data collected from the controllers is restricted to read-only access. The cellular gateway device is integrated with a secure platform to ensure reliable connectivity support. The operation of the data monitoring system will not impact the performance of the thermal system. Our IoT architecture is designed with cybersecurity as a top priority.

Protection at the device level with Eurotech's RELIAGATE 10-14 gateway

- Adheres to IEC 62443-4-1/2 cybersecurity standard and PSA Level 1 certification
- Compliant with California SB-327 password law
- Hardware support for TPM 2.0, Secure Boot
- Always-on physical anti-tampering monitor/logger that is active even when system is removed from power

Best in class Device Management Platform

- IoT gateway devices are effortlessly managed with best in class device management platform, providing real-time monitoring and robust security to ensure seamless and secure device operations
- All components of the device management platform rely on a robust, centralized security foundation layer
- The platform follows the RBAC model to manage user identities and permissions
- The platform manages device-side certificates, granting access only to customer-approved devices

End-to-end encrypted connection between device and Azure IoT Hub

- One-way only communication to the cloud, no access to write control parameters
- Data encrypted using SHA-256 encryption
- SSL/TLS certificate for Device to Cloud connection

Secured and encrypted data throughout Azure cloud environment

- SSO authentication on cloud architecture
- User authentication required at all end points with limited access and dedicated administrative accounts
- Private end point database
- AES-256 encrypted data storage

