

THERMALWATCH[™]

For WATCONNECT[®] Control Panels

Maximize system uptime, yield and reliability with our powerful **THERMALWATCH**[™] package. We analyze your **WATCONNECT**[®] control panel data to identify opportunities for enhanced efficiency. Receive a comprehensive quarterly thermal system report, providing valuable insights and actionable recommendations.

Seamlessly integrated into your panel, our monitoring capability has zero impact on system footprint. Your data remains secure with a read-only connection to the cloud via cellular connectivity.

What will Watlow[®] deliver?

- Review and analysis of the data conducted by a data scientist and thermal system expert
- Comprehensive quarterly thermal system report showing time series graphics, statistical data, anomalies and an executive summary including insights and recommendations for system improvement
- Collaborative touchpoints, engineer-to-engineer, to review the data and develop context

What analysis is included?

Power and temperature controller health

- Prevent unplanned downtime and perform maintenance as-needed by ensuring basic functionality of system components

Failed element detection

- Prevent unplanned downtime, pre-order replacement elements and schedule maintenance activities in advance

Process continuity (process drift)

- Improve system reliability by monitoring process drift over time; this gives visibility to changes in the system that can prompt maintenance activities to avoid unplanned downtime

Environmental controls within the panel (optional)

- Monitor panel environmental data to alert to changes in environmental conditions that could lead to a failure

Isolated monitoring of field wiring terminals (optional)

- Extend system life and optimize maintenance schedules by monitoring terminal temperature to determine when maintenance is needed to tighten the terminals

Smart Services



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



What data will be collected?

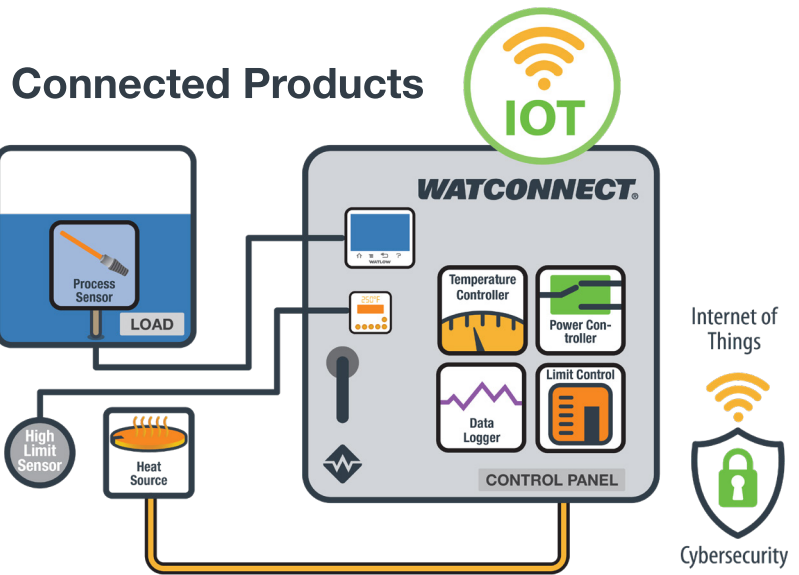
Power, current, voltage, SCR/controller alarms, process values, set point, panel environmental data and wiring terminal temperatures (based on panel configuration).

How will the data be collected?

The panel will include a Eurotech cellular gateway device. This device will pull the desired data from the 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 installed on top of the 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).

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.



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

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