BUILDING MANAGEMENT

BUILDING MANAGEMENT

MONITORING OF HVAC SYSTEMS PROTECTS CRITICAL INFRASTRUCTURE FROM CYBER ATTACK

Challenge: The critical infrastructure (pumps, heaters, chillers) of a national data-center required online monitoring and anomalies detection capabilities.

Solution: SigaPlatform was connected to the mission-critical sensors of the end devices and learned the normal operating pattern of the data center and the smart building.

Results: SigaPlatform provides exclusive indications of the Building Management Systems end-devices and process with no false alerts. The system detects ANY process or end-device malfunction as result of nationalgrid fluctuations, end-devices and PLC faults. The accuracy of SigaPlatform, on the one hand, leads to the ability to distinguish process and process deviations, as well as the possibility of optimizing processes and the ability to conserve power consumption, by keeping the operating requirements.

In details:

Siga's unique platform is installed in a sensitive building where a large number of data centers and other systems require constant and uniform voltage, continuous faultless cooling, temperature monitoring and emergency response capability for generator operation.
The platform is connected to the critical sensors of the process which are the main funnels for building processes and continuously monitors the electrical signals obtained from the chiller frequency, heat pumps, operating commands, etc.

The platform has learned completely autonomously the nature of the normal operation of the process in such a way that it is possible to identify operational faults in early stages, report to the operations manager and to prevent aggravation. By this autonomously learning stage the platform develops the ability to identify anomalies in the process in advance.

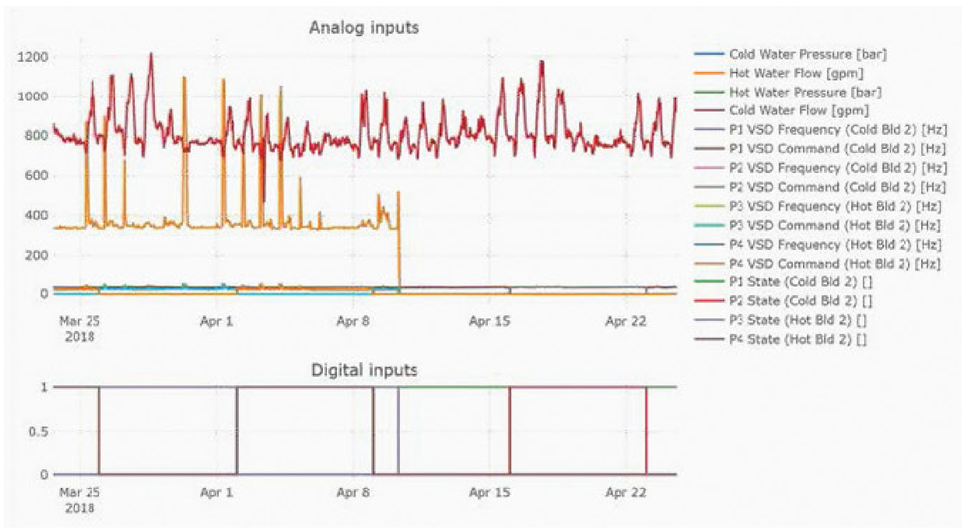

Figure 1 – Normal pattern of Cold/Hot water pumps

Figure 1 shows an example of a normal process in which both chillers and heat pumps operate simultaneously. The accuracy of SigaPlatform, on the one hand, leads to the ability to distinguish process and process deviations, as well as the possibility of optimizing processes and the ability to conserve power consumption, by keeping the operating requirements.
The advantage of continuous monitoring, protocols agnostics, enabled to save a “human-hours” by producing automatic and continuous operational reports according to the customer's demand, either by receiving real-time data on each process and / or critical end-points for monitoring as a separate and independent system which detects faults in real time.

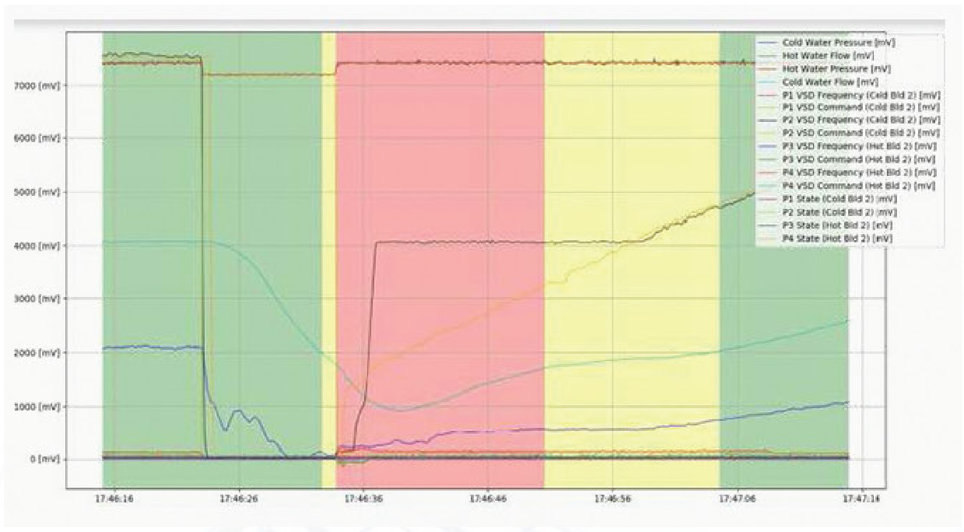

Figure 2 – Anomaly detection in Pump2 (cold water)

Figure 2 shows an example of a fault of rapid continuous operation and shutdown of pumps (may result from voltage fluctuations in the electrical grid, malfunctioning PLC or manual malfunction by purpose). The system detects the fault at the initial stage but alerts in real time when it identifies a deterioration in the process. The system sends an accurate detailed SMS/Screen notification (in any required logs) describing the specific alert.

Siga is the only vendor targeting and securing level 0 (Process) and level 1 (Basic Control and safety) layers of the Purdue reference model, which is where the real damage can be caused to OT owners and operators by a cyber-attack or equipment malfunction. Siga’s offering is agnostic of the OT protocol and equipment being used as it analyses only the **electrical signals, not data communications**. Thus, it can be connected to monitor and analyze any end device equipment or sensor connected to a PLC or an RTU irrespective of the OEM and the version. In line with the current trend in cyber security solutions, Siga OT Solutions uses machine learning and predictive analytics to detect process anomalies in real time, whether due to a cyber-attack or a technical malfunction, SIGA provides this technology in its product SigaPlatform. It is installed at the client location between the PLC and end-device equipment without interfering with or impeding ongoing operations and in complete isolation from externally connected communications networks. This isolation from the enterprise network eliminates the risk of an adversary's manipulation of ML algorithm and provides resiliency.
Siga is already in use in a range of critical infrastructure operations and has demonstrably improved the reliability, safety and security of our clients' assets. Siga also just been named as a Gartner "Cool Vendor" for Industrial IoT and OT Security.