Radiflow SIGA Level Zero OT Resilience

JOINT SOLUTION DATASHEET

SIGA OT Solutions Integration with Radiflow

Advanced Early Threat Detection for OT/ICS Environments

The Problem

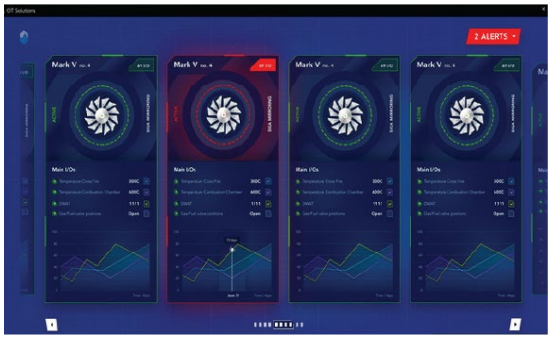
Cybersecurity does not end at network perimeters. You need an end-to-end OT security system that can detect threats even before they enter the production network.

1. Many utilities are not connected to a Cyber SOC or MSSP due to budgetary, regulatory, or operational constraints. They require an on-premises cyber-monitoring solution for all levels of production.
2. The majority of cyber-attacks originate from the network attack vector, such as:
   - » Remote access for maintenance (e.g. vendor supply chain)
   - » Insider threat (e.g. by disgruntled employee)
   - » Connectivity to low-security zones such as enterprise or third-party suppliers, thus, exposed to ransomware and malware.
3. Supply chain attacks originate in procured devices which had been pre-installed with malware. This vector of attack does ***NOT*** start at the network.

   In the case of Infected malware, the threat won't be detected at the network level, and the malicious code would reach the sensors and actuators directly.

Solution Value

To monitor anomalous events within information channels in critical infrastructure environments, Radiflow and SIGA offer a single-pane-of-glass joint solution that delivers full visibility into the I/O sensor and network highways through a single IDS platform. This extends the visibility scope of the IDS down to the the lowest field sensors and actuators.



The SIGA platform's alerts dashboard

How SIGA's technology works:

SIGA's core solution is a powerful anomaly detection platform, based on securing raw data duplication, leveraging fully out-of-band hardware, reliable encrypted data delivery, and multi-layered analysis for identifing process abnormalities and generate new and valuable operational insights.

The SIGA solution is comprising both a hardware layer installed in the critical infrastructure, to measure low-level electric signals, and a software layer applying advanced analytics.

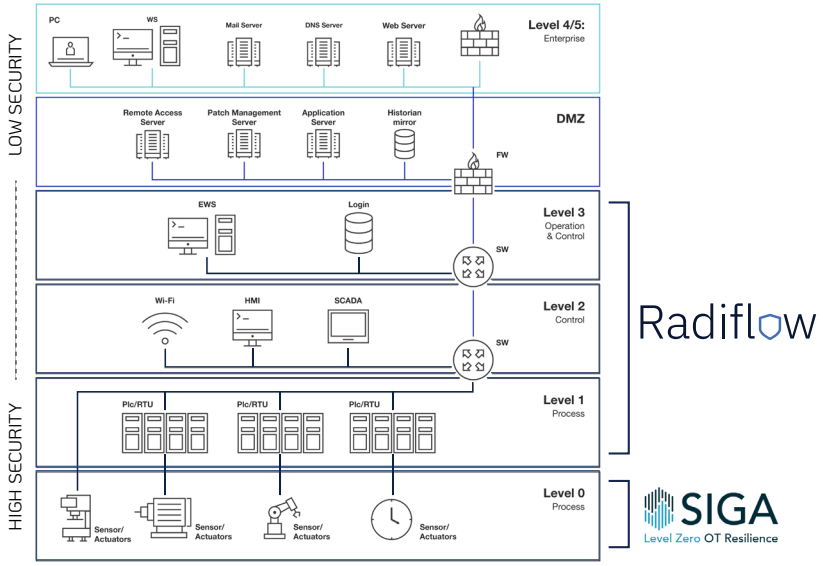
The electrical signals are acquired directly from the control loop between the PLC and the sensors/actuators, using uni-directional isolators, into a separate network. This raw data is analyzed by the SigaPlatform™ smart AI engine providing real-time, totally reliable status of the critical end-devices of the OT network, and send smart notifications according to customer specs.

The SIGA-Radiflow Joint Solution Workflow

- **SIGA Platform deployment:** Upon deployment, I/O sensors and PLCs are correlated, so that anomaliles detected by the SIGA platform in at the levels between lower sensors/actuators and PLCs are correctly associated to specific PLCs
- **Radiflow IDS deployment:** The Radiflow IDS is deployed between the Supervisory and Basic Control levels. Upon connection (via mirrored port) to the network the IDS self-learns the network and all its assets and attributes, resulting in an accurate digital image of the network used as a baseline activity model for anomaly monitoring
- **Alert Correlation:** Radiflow IDS is configured to receive SIGA syslog alerts generated upon detection of anomalous actitivity. Alerts from sensors and actuators are associated in the Radiflow IDS with their relevant PLCs, creating a unified view of all alerts per specific production zone, network segment, PLC, etc.

Thus, by monitoring raw electrical signals at the device level, SIGA enables the detection of anomalies – caused by both device failure and malicious activity – at the source. This capability complements Radiflow's threat intelligence-based IDS, which is tasked with monitoring network communications at higher (supervisory) operational levels.

The result of the joint solution is end-to-end threat detection from I/O to network, that's able to track attacks from network to PLC to sensor/actuator, and from rouge devices with embedded malware. The unified, single-pane solution is intended for use by on-prem automation OCC staff, MSSPs and SOCs alike.



By correlating SIGA-generated alerts on anamalies detected in sensors and actuators with Radiflow IDS's threat monitoring in higher (supervisory) levels of the production network, users are able to detect and handle threats sooner, all through a single pane of glass.

ABOUT RADIFLOW

Radiflow develops unique OT cybersecurity tools to protect and ensure organizations' digital resilience. The company closely collaborates with Managed Security Service Providers to oversee the discovery and management of all relevant data security points. Founded in 2009, Radiflow has offices and partners in Europe, USA and APAC. Its field-proven solutions are installed at over 7000 sites around the globe. For more information: www.radiflow.com

ABOUT SIGA

SIGA OT Solutions is an OT cybersecurity provider for industrial and manufacturing environments, offering early anomaly detection. Through its Incipient Failure Detection solution, The Siga Platform, enables industrial, commercial, and critical infrastructure operators to dramatically improve the reliability, safety, and cyber security of their assets, with minimal financial or human resources and without disrupting existing Industrial Control Systems. Installed on the Input/Output lines (I/Os) between the sensor/actuator and the PLC. Enhancing security at the process and control layers by securing level 0 (Process) and level 1 (Basic Control and Safety) layers of the Purdue reference model. For more information: www.sigasec.com