Cybersecurity for BMS & Smart City Networks

► Full heirarchical logical interdependency map of all disparate building systems, through iSID Detection & Analysis Platform, using Radiflow's Smart Collectors

► CIA (Confidentiality, Integrity, Availability) Risk Evaluation available included as part of iSID's baseline configuration

► MSSP/SOC ready with alert prioritization triage and multi-iSID system management solution

► Attack vector and attacker capability analysis provide proactive health insights for alert prioritization and optimizing risk mitigation investment

WHY RADIFLOW?

Radiflow is a recognized leader in industrial cybersecurity, offering dedicated solutions designed to meet the unique requirements of industrial infrastructures.

EXPERIENCE

Over 10 years' experience discovering and analyzing advanced persistent threats and targeted attacks, including attacks on critical and industrial infrastructure.

EXPERTISE

Dedicated team of industrial cybersecurity experts who understand the colliding worlds of automation and security.

END-TO-END PORTFOLIO

Radiflow offers a holistic portfolio of services and technologies, including secure gateways, Industrial IDS and many more.

Building Management Systems (BMS) and Smart City deployments involve integrated services by multiple vendors for electricity, water supply, HVAC, access control, fire alarms and more.

The sheer number of PLCs in BMS and Smart City networks makes it difficult to provide protection and real-time network visualization and security intelligence. The challenge is compounded by the interdependencies and data flow paths between different systems. These interdependncies put down-path devices at risk in case of outsider attacks (due to unsecure remote access to services), as well as insider attacks (e.g. PLCs that had been infected during maintenance and returned to service).

Radiflow's cybersecurity solution suite, designed especially for Production (OT) networks, provides BMS operators the tools to protect, visualize and safely maintain their systems:

► **System-wide topology learning and visualization**: Radiflow's iSID non-intrusive, passive (optionally active) Threat Detection & Analysis Platform provides a full, heirarchical logical interdependency map of all disparate building systems, with drill-down to each device's attributes, known threats and protocols. Radiflow's solutions, designed for OT, support all relevant OT protocols (e.g. BACnet, Profibus) for accurate modeling and anomaly detection (new devices, topology changes, abnormal memory access and firmware changes) as well as Ethernet and Serial interfaces for modern and legacy devices.

► **Radiflow Smart Collectors**: Smart Collectors send an encrypted mirrored data stream from each subsystem's switch to iSID. The data stream is compressed while maintaining data integrity, using Radiflow's proprietary compression scheme, to prevent network overload.

The Radiflow iSID Industrial Threat Detection & Analysis Platform

► **Alert Prioritization**: iSID's out-of-the-box CIA (Confidentiality, Integrity, Availability) Risk Evaluation triage model significantly improves alert handling. Following the initial modeling stage, CIA values are assigned to each subsystem's devices based on function (e.g. safety systems are attributed high availability, low confidentiality, and high integrity). These values can be later configured by the operator.

Continued...

▶ **Maintenance Management**: Radiflow's iSEG Secure DPI Gateways allow enforcing remote maintenance management rules. Using an Authentication Proxy Access (APA) the network administrator is able to allocate a specific time window for restricted remote access to the specific IED that needs to be maintained.

The APA provides the network administrator the flexibility to schedule remote maintenance tasks without the risk of forgetting to terminate the remote session. This prevents propagation of malware to devices and subsystems outside the scope of the technician's work order.

▶ **Attacker Capabilities and Attack Vector Analysis**: By mapping the interdependencies and data flow between different devices, and the attacker capabilities assigned to each threat on each device, operators are able to better determine which devices need to be prioritized for strengthening and patching, for optimization of risk mitigation expenditure.

▶ **SOC/MSSP-Ready**: Radiflow's solutions support remote monitoring and management at MSSP's SOCs. Using end-to-end IPsec VPN tunnels, Radiflow's Smart Collectors are able to efficiently send large volumes of data to a central instance of iSID at an MSSP's SOC. Alerts are sent to the SOC are evaluated and triaged based on their CIA true risk values.

Management of multiple instances of iSID (in MSSP-monitored multi-network BMS systems) for BMS and Smart City systems is made possible by Radiflow's iCEN management utility, which greatly simplifies the management and maintenance of large-scale networks.
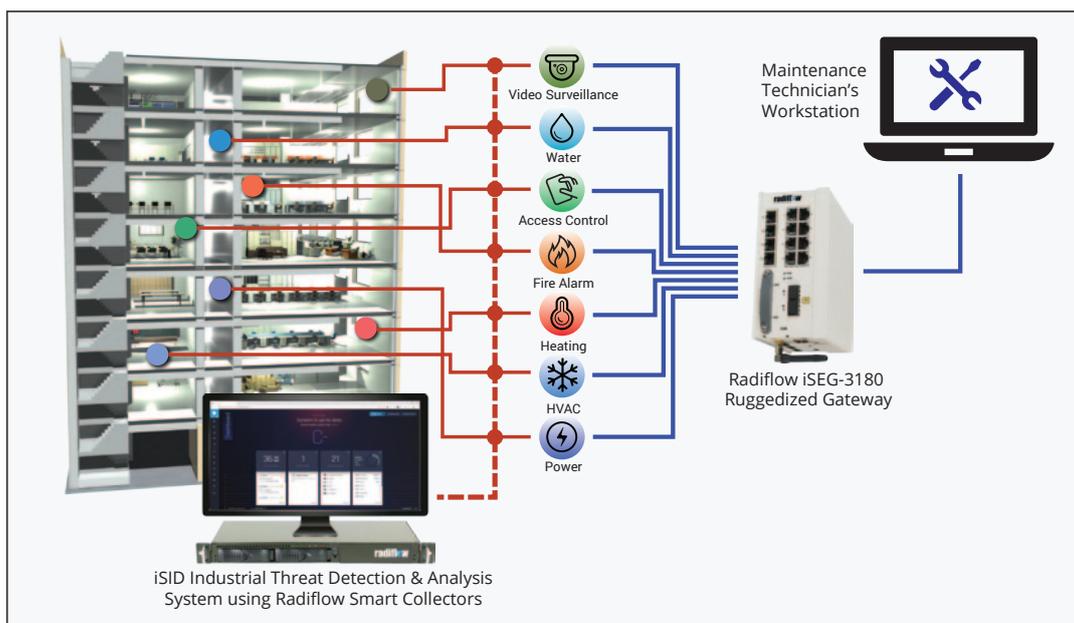
Typical components and layout of a Radiflow-secured BMS system

About Radiflow:

Radiflow is a leading provider of cyber security solutions for critical infrastructure networks. Radiflow's comprehensive portfolio of empowers critical infrastructure and industrial enterprises to maintain visibility, control and security of their operational environment. Our intelligent Threat Detection & Analysis Platform for Industrial cybersecurity minimizes potential business interruption and loss within your OT environment.

Radiflow's team consists of professionals from diverse backgrounds, from cyber-experts from elite military units and automation experts from global cybersecurity vendors. Founded in 2009, Radiflow' first solutions were launched at the end of 2011, validated by leading research labs and successfully deployed by major utilities worldwide. More at www.radiflow.com.