# CYBERSECURITY FOR BUILDING MANAGEMENT SYSTEMS (BMS)

radiflow

# COMPANY DESCRIPTION

Radiflow develops trusted Industrial Cyber-Security Solutions for Critical Business Operations. Our portfolio of game-changing solutions for ISC/SCADA networks empowers users to maintain visibility and control of their OT networks. Our intelligent Threat Detection and Analysis Platform for industrial cyber-security 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 industrial system integrators from global cyber-security vendors.

Founded in 2009, Radiflow' solutions, are successfully deployed by major industrial enterprises and utilities protecting more than 4,000 critical facilities worldwide. More at www.radiflow.com.

# CHALLENGES

## The Changing Landscape of Industrial Operations

Cyber threats to Operational Technology networks have in recent years been on the rise. Terrorists and criminals have set their sights on critical infrastructures, manufactures and other industrial operations that utilize ICS systems due to these systems' inherent vulnerabilities and the high financial losses to manufacturing enterprises due to down-time of production lines.

The challenges facing industrial cybersecurity operators stem from several factors:

- The increased use of automation using software-centric and IoT technologies has created more exploit opportunities
- Tools initially developed by nation-state actors to attack critical-infrastructure are now becoming a commodity
- Propagation of attacker activity from IT to OT
- Proven feasibility of cyber-physical attack models in multiple high-profile cases

# SOLUTIONS

## iSID Industrial Threat Detection & Monitoring

- Network visibility based on self-learning of the OT network through passive monitoring
- Automatic mapping of all industrial assets and alerts on parameter change attempts
- Signature-based detection and identification of attacks and PLC & protocol vulnerabilities (e.g. BacNet, Modbus, S7, IEC-61850)
- Anomaly detection: detect abnormal activity on the network compared to the normal device behavior
- Event notifications via multiple reporting methods (GUI, Syslog, SMTP & Modbus)
- Smart collector for low-bandwidth transfer of data to central instance of iSID
- Central management of multiple iSID instances at in-house or MSSP SOC

The iSID Dashboard provides an at-a-glance view of overall network risk, device inventory and alerts

## iSEG Secure DPI-Firewall Gateways

- Authentication Proxy Access (APA) for user authentication & pre-configured task-based access
- Detailed user activity log within each remote access session for compliance and auditing
- Validation of user behavior using a per-port Deep Packet Inspection (DPI) firewall
- IPsec VPN for secure inter-site connectivity between facilities and BMS control centers
- Ethernet & Serial interfaces for local devices connectivity to IP uplinks over Wired & Cellular
- IEC61850-3/IEEE1613-compliant ruggedized appliances

The iSEG RF-3180 Ruggedized Secure Gateway

## iRISK Industrial Risk Analysis

- Assess the actual business-related impact of cyber-risk in OT networks
- Unique calculation of likelihood of attack
- Prioritized mitigation recommendations
- Automatically-generated risk analytics and risk impact reports, based on up-to-date OT TI
- Plain-language mitigation recommendations
- IEC 62443 reporting support

The iRISK dashboard

# BMS SECURITY

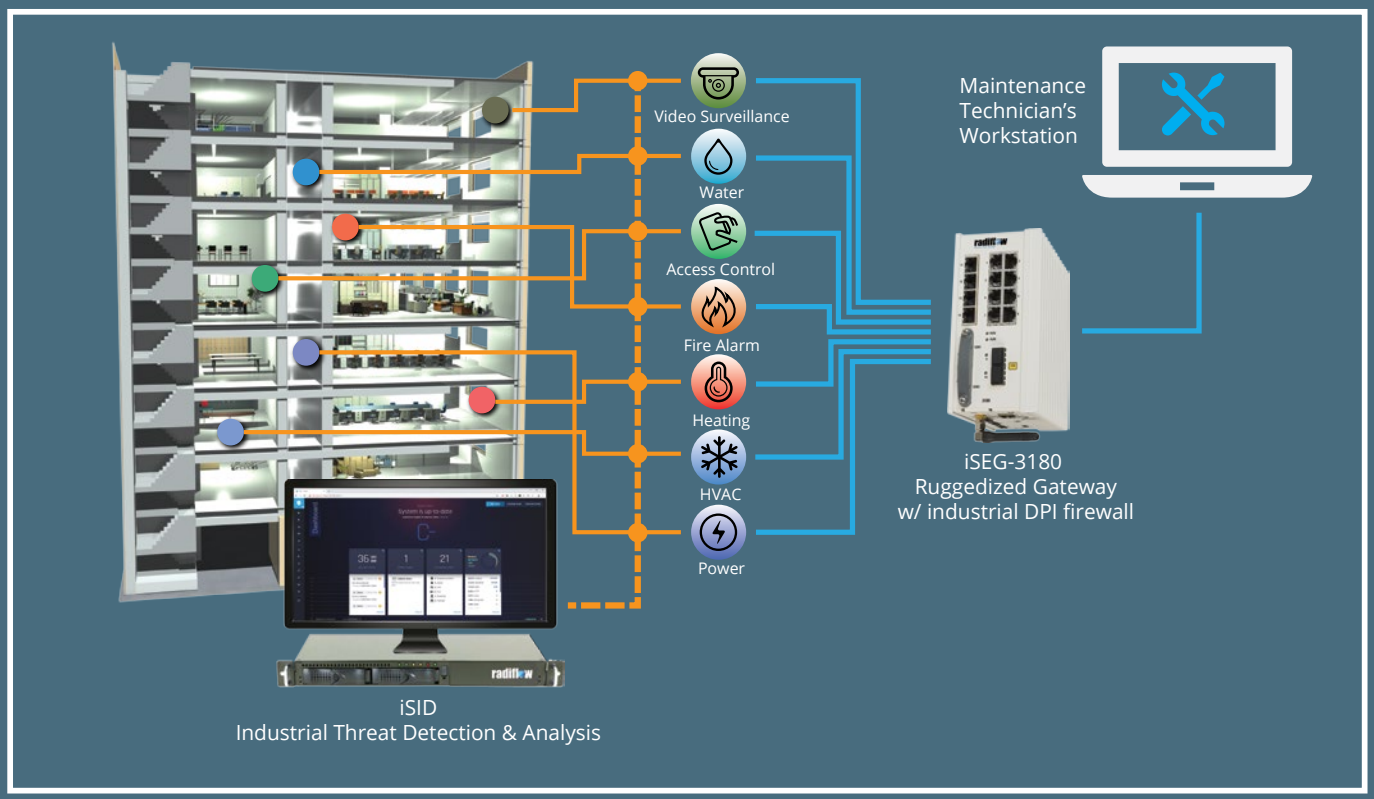
## Securing Complex Arrays of Multi-Vendor Devices

Building Management Systems (BMS) involve integrated services by multiple vendors for electricity, water supply, HVAC, access control, fire alarms and more, which makes it extremely difficult to provide protection, real-time network visualization and cybersecurity insights.

The challenge is compounded by the growing reliance on Cyber-Physical Systems (CPS) for controlling industrial processes, as well as on internet-based automation & remote operations and IT/OT connectivity. In addition, the OT-cybersecurity system faces the challenge of securing building campuses' energy centers and grid connections, an attack on which could disrupt of shut down operations altogether.

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

- Full hierarchical logical interdependency map of all disparate building systems, through iSID Detection & Analysis Platform, using Radiflow's Smart Collectors
- CIA (Confidentiality, Integrity & Availability, as well as Safety) risk evaluation based on per-business process impact, using iRISK
- MSSP/SOC ready with alert prioritization triage and multi-iSID system management solution
- Attack vector and attacker capability analysis provide proactive insights for alert prioritization and optimizing risk mitigation investment
- Protection of buildings' data communication protocols
- Compliance enabler for all common standards and regulations



# HOSPITAL CASE STUDY

## Securing a Large Hospital Campus in EMEA

### Objectives and challenges of the project:

- Securing critical BMS systems (using DPI for ModBus & BACnet protocols): HVAC, electrical, elevators and water; monitoring the storage of medical gases; and monitoring the temperature control systems in cold-storage rooms and appliances
- Protecting the high voltage power supply systems (securing the IEC 61850 protocol)
- Monitoring various HazMat sensors

Most of the challenges are due to the way the hospital's data networks evolved over the years, as a patchwork of systems and no segmentation between critical systems:

- OT and IT systems that share the same LAN, with only nominal firewall protection and no segmentation between buildings, facilities and systems
- No procedures patching or hardening devices, leaving the hospital to rely on vendors
- No system for securing/logging maintenance operations

### Solution & Process

- Thorough OT-security assessment, by means of analyzing all operational data traffic
- Analysis provided a detailed network model of all assets, ports, connections, protocols and vulnerabilities, from lack of IT-OT segmentation to use of default passwords
- Drafting a detailed mitigation roadmap by Radiflow team members and execution in collaboration with the client. The end result was a "clean" baseline topology model which was used thereon as the baseline for ongoing monitoring and threat detection

### Current Status

The Radiflow iSID system is fully operational and is used for continuous monitoring of network activity at several facilities belonging to the hospital chain. Monitoring operations are performed at an OT-MSSP's (Managed Security Services Provider) SOC.

*See all Radiflow case studies at radiflow.com/case-studies*

# radiflow

Scalable, flexible architecture for all types and sizes of industrial organizations

Comprehensive portfolio of detection and prevention tools as well as assessment and monitoring services

Planning value-add:  tools for business-driven risk scoring and mitigation planning

Solution designed by industry experts and validated by external labs, protecting over 4,000 sites worldwide


**US and Canada:**
Tel: +1 (302) 547-6839
sales_NA@radiflow.com

**EMEA:**
Tel: +972 (77) 501-2702
sales@radiflow.com

**UK:**
Tel: +44 (0) 800 246-1963
sales_UK@radiflow.com

**France:**
Tel : +33 1 77 47 87 25
sales_FR@radiflow.com

**DACH:**
Tel: +49 (160) 109 75 65
sales_DACH@radiflow.com