Application Note

Building Management Security

Monitoring & Enforcment by Radiflow

***Synopsis**: SCADA-based Building Management Systems (BMS) are used for central management of integrated systems in complex, multi-system facilities. In recent years BMS networks have become a prime target for cyber attacks, as they are considered unsecure (due to the lack of BMS cyber security tools). Radiflow's security solution, designed specifically for buildings' BMS networks, provides comprehensive cyber-security monitoring & enforcement, all packed into one platform.*

Building Management Systems **(BMS)** control services that are essential for building or facility operation. BMS systems are typically found in banks, Data centers, sports arenas, campuses, hospitals and other facilities that rely on multiple integrated services such as electrical and water supply, HVAC, access control and fire alarms.

Many BMS systems rely on an air gap between the regular office network and the BMS network. While this topology is considered safe, it is not safe enough to prevent sophisticated cyber threats such as insider threats (e.g. PLCs that had been infected during maintenance and returned to service) or outsider threats (unsecure remote access to services).

Since BMS networks encompass a huge number of PLCs, one of the biggest challenges today is providing real-time network visualization and security intelligence. With advanced monitoring of the BMS network, anomalies can be detected indicating a potential attack on the BMS devices. Another challenge in securing BMS networks is providing secure remote access for maintenance operations, while assuring that a technician maintaining one vendor's device will not have a connection to other vendors' devices. Currently, in typical BMS networks there is no mechanism to limit each vendor's access to its equipment only.

Another recent trend among some building management companies is consolidating the BMS network and the building's "regular" network. This consolidation offers many advantages; however, it exposes the BMS network to even more cyber risk.

Many network administrators utilize IT network security products to defend their networks against potential cyber attack. These products are excellent in protecting regular networks; however they are not suitable for protecting BMS networks, since they don't support the relevant protocols (e.g. BACnet and Profibus) and cannot provide an accurate network topology model. Simply put, security tools for regular IT networks don't stand a chance of detecting anomalies and unauthorized activity in BMS networks.

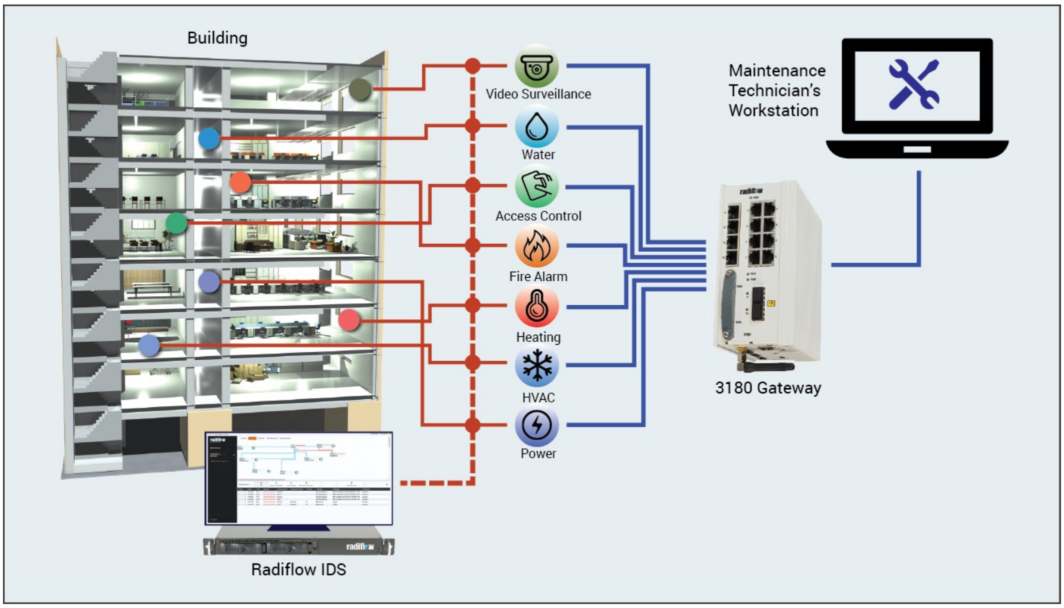
Radiflow's security solution was designed for SCADA/ICS networks, and namely for buildings' BMSs. The comprehensive solution includes an Intrusion Detection System **(IDS)** as well as Secure Gateways. The IDS, which is non-intrusive (no effect on the BMS network) is able to visualize and detect abnormal activity within the BMS network–all within minutes from activation to full protection.

Application Note

Building Management Security

Monitoring & Enforcment by Radiflow

Secure access to the BMS network is enabled by Radiflow's Secure Gateway. 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.



Features

- **Network Visibility:** based on self-learning of the SCADA network through passive (and optionally active) scanning of all data transactions.
- **Anomaly detection:** detection of abnormal activity, including new devices, topology changes, abnormal memory access and firmware changes, compared to the normal network model created by the IDS.
- **Maintenance Management:** an Authenticated Proxy Agent (APA) process for managing maintenance operations from a remote location.
- **VPN:** end-to-end IPsec VPN for secure communications between the control center and the secured facility.
- Support for **Ethernet** and **Serial** interfaces for modern and legacy devices, including **PoE+** support.