Building Management Systems & IP Convergence for School Districts

Building Management Systems (BMS) must now integrate cybersecurity into their processes. The technology used by BMS and its operators generally belongs to the facility management business unit, which is linked to the IT department within the school district.

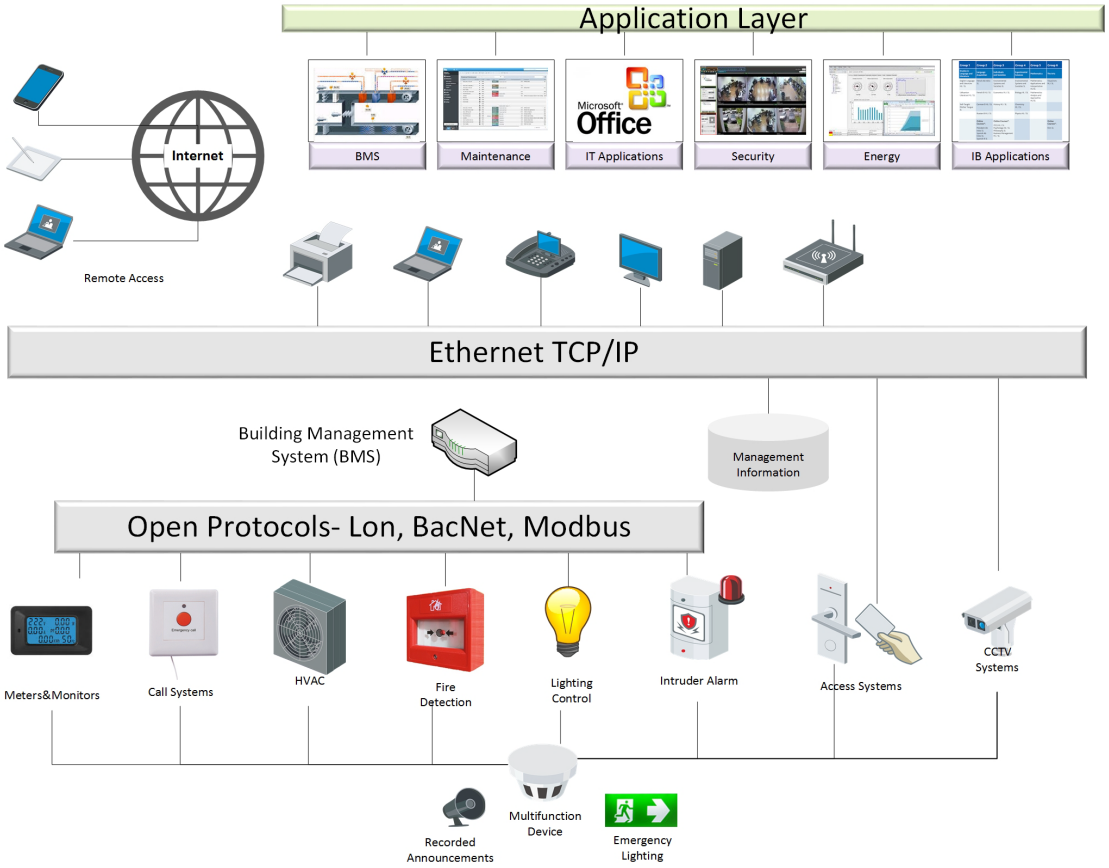
BMS and centralized building management systems, which were previously independent, are now integrated into other systems. Buildings within school districs are now connected to a network with IT data centers and remote access servers used via open protocols.

BMS and IP Converge for Smart Building Network Infrastructure for School Districts

Although Smart Building Systems have substantial advantages, they are also highly susceptible to cyber risks. Because they are more open, more complex and more interconnected on IP networks (IP convergence), they are also inevitably more exposed.

This ecosystem has recently been expanded with the appearance of smart systems (Smart Grid, Smart Cities, Smart Water, etc.) which take the BMS and other systems such as lighting control, security systems (CCTV, Access Control, Intercom, etc...) to a broader level of control and integration. Unfortunately, the control systems for heating, lighting, and security in most buildings have generally not been developed with technology designed to be connected.

This accumulated exposure to the cyber world calls for reinforced cybersecurity measures to confront the increasing security challenges in the era of the Internet Of Things (IoT).



BMS Top Threats & Vulnerabilities

1. **Default Configuration**
BMS comes configured with Out-of-box default or simple passwords and a baseline configuration that makes it easier for attackers to quickly compromise the system.

2. **Legacy Software**
BMS run on legacy software that typically lack sufficient user and system authentication and data authenticity verification, rendering the system more vulnerable for attackers to gain access and control of the system.

3. **Remote Access Policies**
BMS field equipment can typically be connected to invalidated cellular networks or legacy dial-up lines or remote-access servers give attackers an easy backdoor access to the OT network as well as the corporate LAN.

4. **Silos, Policies & Procedures**
Security gaps are created when IT, Facility and OT departments do not agree on their strategy and approach to secure industrial, building and OT networks. A unified security policy needs to be developed and adopted to protect both IT and OT technologies.

5. **DDoS Attacks**
BMS inherent limited access-controls allow and lack of security allows attackers to easily execute DoS attacks on vulnerable unpatched systems.

x10 networks

PARTNERSHIP

X10 Networks partners with leading BMS providers to integrate their systems onto the Building Management Network. X10 will provide the backbone converged network along with low voltage wiring and structured cabling systems as part of a complete turn-key solution.

SOLUTIONS

X10 Networks delivers smart building solutions on time and on budget, while ensuring the security of the entire solutions. Tenants will be assured that their data are safe at all times

DESIGN

X10 Networks will design and configure details of all network equipment (hardware and software) including edge switches, core switches, controllers, gateways and any related components.

Previous Incident

In 2013, Target, the second-largest discount store retailer in the United States behind Walmart, fell victim to a hack that stole debit and credit card data from around 110 million accounts. The Source of attack was through the Building Management system (BMS). Hackers found a flaw in the network of an HVAC (Heating, Ventilation and Air-Conditioning) contractor that was connected to the stores to control their heating and air conditioning installations.

510-1199 West Pender Vancouver, BC, V6E 2R1 info@x10networks.net www.x10networks.net 1-866-442-0565

VANCOUVER | CALGARY | TORONTO | MANILA