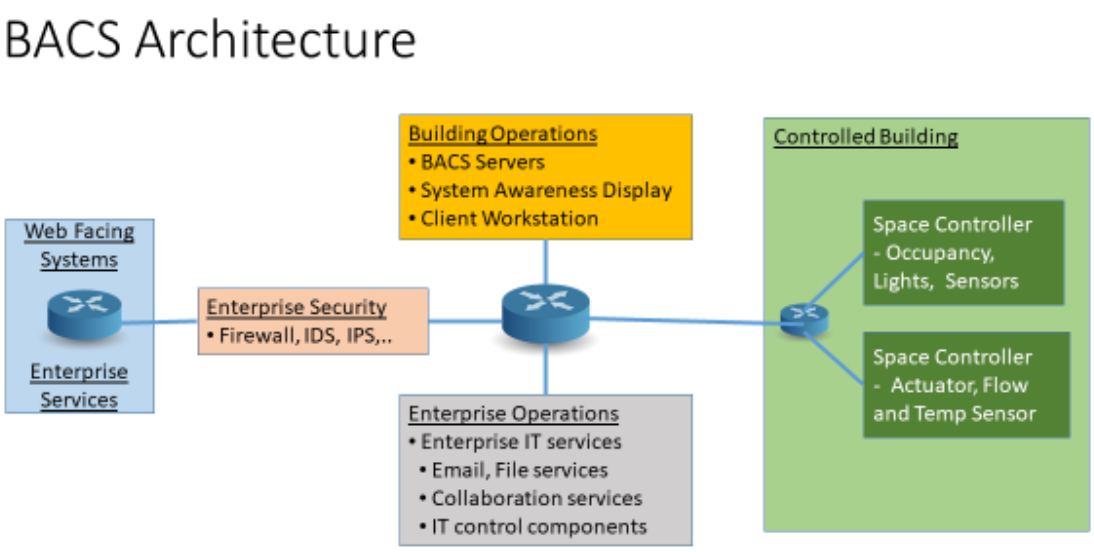
SCIT Labs Inc,
13834 Springstone Drive #200
Clifton, VA 20124

Cyber Security of Building Automation Control Systems

The 21st Century has seen an increasing emphasis on better control of the physical access to, and the environment of buildings. This has led to increasing deployment of Building Automation Control Systems (BACS). Vendors like Siemens and Johnson Control provide products that automate the monitoring and control of the different spaces in a building. For example, such controls facilitate the real time optimization of the energy usage and air quality, in response to changing space occupancy. Often, and increasingly so, these systems are connected to other systems like HVAC control and electrical power management and external systems like corporate networks and payment processing systems In general, the BACS are slowly changing and, like many control systems are not included in regular management monitoring oversight. Thus, once the intruder gets into the BACS system they could stay in for months or even years. Besides manipulating HVAC elements such as building temperature, humidity, air quality, etc. intruders can use this as a gateway and navigate to other corporate systems and cause even more damage. SCIT Labs is focusing on offering software, hardware and services to cyber protect your BACS and connected systems.



The above figure provides a typical BACS architecture, showing some of the interconnectivity between BACS and corporate networks. Buildings such as Data Centers and Pharmaceuticals production facilities rely heavily on automated environmental controls and optimal energy consumption. The increased need for efficient and economical regulation of environmental parameters, make the deployment of BACS vital to these facilities. We have noted that many of the BACS systems are managed by facilities managers who do not have cyber security skills. Further, these systems change so slowly, making monitoring them a low priority among the cyber security team. Reducing the vulnerability of Building Automated Control Systems to hacking and reduced effectiveness/manipulation can be accomplished using SCIT.

The SCIT technology enhances the resilience and security of BACS.

1) Mitigates APT attacks: SCIT reduces the persistence time of the attacker to minutes.
2) Discovers zero days: SCIT continuously looks for and discovers intrusions that exploit vulnerabilities, including zero day.
3) No disruption: Works within your existing security infrastructure i.e. does not replace existing security software but rather, augments them.
4) Malware alerts: SCIT analysis highlights the presence of malware in the system and can alert the facility and cyber security teams.
5) Support requirement: SCIT runs in a semi-autonomous manner with minimal man in the loop requirements, typically until an alert is issued.

Our approach to Cyber Defense of BACS involves the following:

1. Assess the key cyber vulnerabilities in the BACS installation.
2. Determine the inter-building BACS connectivity needs.
3. Understand the legacy BACS systems installed.
4. Design Cyber Security system, develop a monitoring plan and a test plan.
5. Install and test the cyber security of the BACS.