Building Automation & Control System
Vulnerabilities
Is there an open door into your facility?

by
Dave Brooks, PhD
Associate Professor, Security Science
School of Science

OVERVIEW
• Background of Research
• Methodology
• What are BACS?
• Why consider BACS?
• Vulnerabilities
• Practitioner Understanding
• Mitigation Strategies
• Outcomes
BACKGROUND OF RESEARCH

• 2010 exploratory research

• Funded by ASIS Foundation

• Supported by BOMA & SIA

• Objectives:
  • Articulate current BACS vulnerabilities
  • Evidence based understanding of security professionals’ BACS awareness & practice
  • (Initial) BACS Guideline

PROJECT METHODOLOGY

Stage 1 Literature Critique
Meta-analysis of BACS
Develop a threat matrix of vulnerabilities

Stage 2 Current Practice
Online survey of 331 security & building professionals

Stage 3 Practice Framework
Develop Guideline of mitigation strategies
Review with Focus Groups
WHAT ARE BACS?

HVAC
IDS
ACs
CCTV
Lighting
Power
Water
Fire & Life Safety
Lifts

BACS
**WHAT ARE BACS?**

- Automated system that converges at a central point to integrate building technology & process the flow of information to create a facility that is safer, more comfortable & productive for its occupants, & more efficient for its owners & operators

- AKA:
  - BEMS, BAS, FMS, BMS, BACS, IB, Smart Building, +++

---

### ARCHITECTURE

- **Management**
- **Automation**
- **Field Devices**

![Diagram of BACS Architecture]

- Corporate Network
- Gateway
- Controller #1
- Controller #2
- Actuator
- Sensor
BACS: THE SECURITY PROBLEM?

- BACS (2016) market valued at $54-78 billion
- Annual growth 12-34% annually
- Global market
- Converging all building systems
- Converging functionality at enterprise level


BACS VULNERABILITIES

Management

- Device access
  - Workstation
  - Insert illegal storage device
- Communication network access
  - Logical connectivity
  - Wiretapping
  - Monitor & analyze traffic

Automation

- Controller access
  - Cover
  - Manipulate inputs/outputs
  - Tamper detection
  - Field programmer
  - Embedded functionality
  - Power
- Communication network access
  - Wiretapping (sniffing)
  - Monitor & analyze traffic
  - Open source programs
  - Data injection (fabrication)
  - Insert illegal Controller

Field Devices

- Device access
  - Manipulation (on/off/alter)
  - Destruction
- Connection access
  - Manipulation (on/off/alter/disconnect)
  - Destruction
  - Tamper detection
### PRACTITIONERS’ UNDERSTANDING OF BACS?

- Majority of security & building operators had neutral understanding of BACS vulnerabilities
- Integrators displayed understanding
- Security: Very limited BACS responsibilities
- 50% of BACS had integrated security systems
- Diverse views on integration & systems

---

**331**
13,803 surveys issued, with a 2.4% percent response rate

**38**
Respondents came from 38 Nations

**48**
Percent of Respondents had BACS vulnerabilities in their Risk Register

**75**
The percent of Respondents believed they had an awareness of BACS architecture

**8**
Percent of builder owners & operators have responsibility for BACS

---

securityexpo.org
MITIGATION STRATEGIES

- Management: Policy, basis of design, security levels & zoning, cross department liaison
- Security risk management: Assessment, threat, criticality
- Personnel security: Procedures, vetting (inc 3rd parties), awareness, training
- Physical security: Access rights, device control & protection
- Cyber security: Logical access control, audit log, time out
- Incident response: Capabilities, exercise
- Continuity planning: UPS, override, exercise
- Maintenance: Schedules plan, known maintainers, asset tracking

Risks are contextual:

- What are your Threats?
- What are your Criticalities?
- What are your Vulnerabilities?

Understand these, you begin to address BACS risks
1. Identify Criticality:
   - Operations
   - Board
   - Financial
   - Reputation
   - Safety
   - Regulatory
   - Information
   - Environment

2. Respond to Questions, in:
   - Management
   - Security risk
   - Personnel security
   - Physical security
   - Cyber security
   - Incident response
   - Continuity planning
   - Maintenance

Do you have a written and endorsed Security Policy?
Is BACS formally assigned to the facility manager's portfolio and if so, who?
Does your facility have a designated criticality rating?
Are your facility's BACS risks captured in your Risk Register?
Do your personnel security practices include pre-employment screening?
Do you have an auditable procedure to authorize access to the BACS?
Are the facility's BACS Controllers, routers and network switches physically protected?
Do you have a policy and procedure for (mechanical) key control?
Does your BACS have remote and external logical access?
Is your BACS logical program and configuration details held in a secure location to enable recovery and reconstitution?
BACS GUIDELINE: MITIGATION STRATEGIES

Facility Security Level 2 Medium

Do you have a written and endorsed Security Guideline or Basis of Design document, which define security levels and zones?
Is physical access to security zones based on role and personnel screening?
Are BACS maintainers pre-employment screened?
Do BACS security breaches get reported and investigated by appropriate personnel?
When a person exits the organization or changes roles, are physical access rights removed or adjusted?
Are security awareness training programs documented?
Are the facility’s BACS physical vulnerabilities documented?
Are BACS tamper alarms annunciated?
Do you have a BACS legacy plan?

BACS GUIDELINE: MITIGATION STRATEGIES

Facility Security Level 5 Critical

Do you undertake a threat assessment?
How often are security seals/stickers for BACS audited?
Do your BACS enclosures, controllers, routers and network switchers use tamper seals to detect actual or attempted manipulation?
Do you carry out technical surveillance counter measure reviews/audits on your BACS on a regular, but random, schedule?
Do your scan for unauthorized wireless BACS connectivity to a defined schedule?
Are all wireless connectivity devices disabled?
Are your BACS maintainers escorted at all times whilst on-site?
OUTCOMES

- BACS Guideline
- Project Report
- SecMan magazine article
- Conference presentation/s
- Journal publication/s
CONCLUDING REMARKS

• BACS will continue to grow, converging more building plant & business functions
• Responsibilities lie across multiple departments/groups
• BACS have vulnerabilities & is a security risk
• Generic security strategies mitigation BACS risks
• But, be aware & understand

### BACS Architectural levels

<table>
<thead>
<tr>
<th></th>
<th>Field</th>
<th>Automation</th>
<th>Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Low</td>
<td>Critical</td>
<td>Moderate</td>
</tr>
<tr>
<td>Network</td>
<td>Low</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td>Software (Application)</td>
<td>Very Low</td>
<td>High</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

 Seeking Volunteers – can you help?

Thank you

& Questions?

ASIS Foundation, BOMA & SIA are acknowledged for their support in this research project