Protecting Against Building Automation Vulnerabilities

Dave Brooks, PhD

Michael Coole, PhD

GSX
GLOBAL SECURITY EXCHANGE

POWERED BY ASIS INTERNATIONAL

23-27 SEPTEMBER 2018

LAS VEGAS CONVENTION CENTER | LAS VEGAS, NV

Overview

- Background of study
- What are Automated Buildings
- BACS security problem
- Practitioner understanding
- BACS Security Guidance:
  - Criticality
  - Mitigation Strategies
- Security recommendations

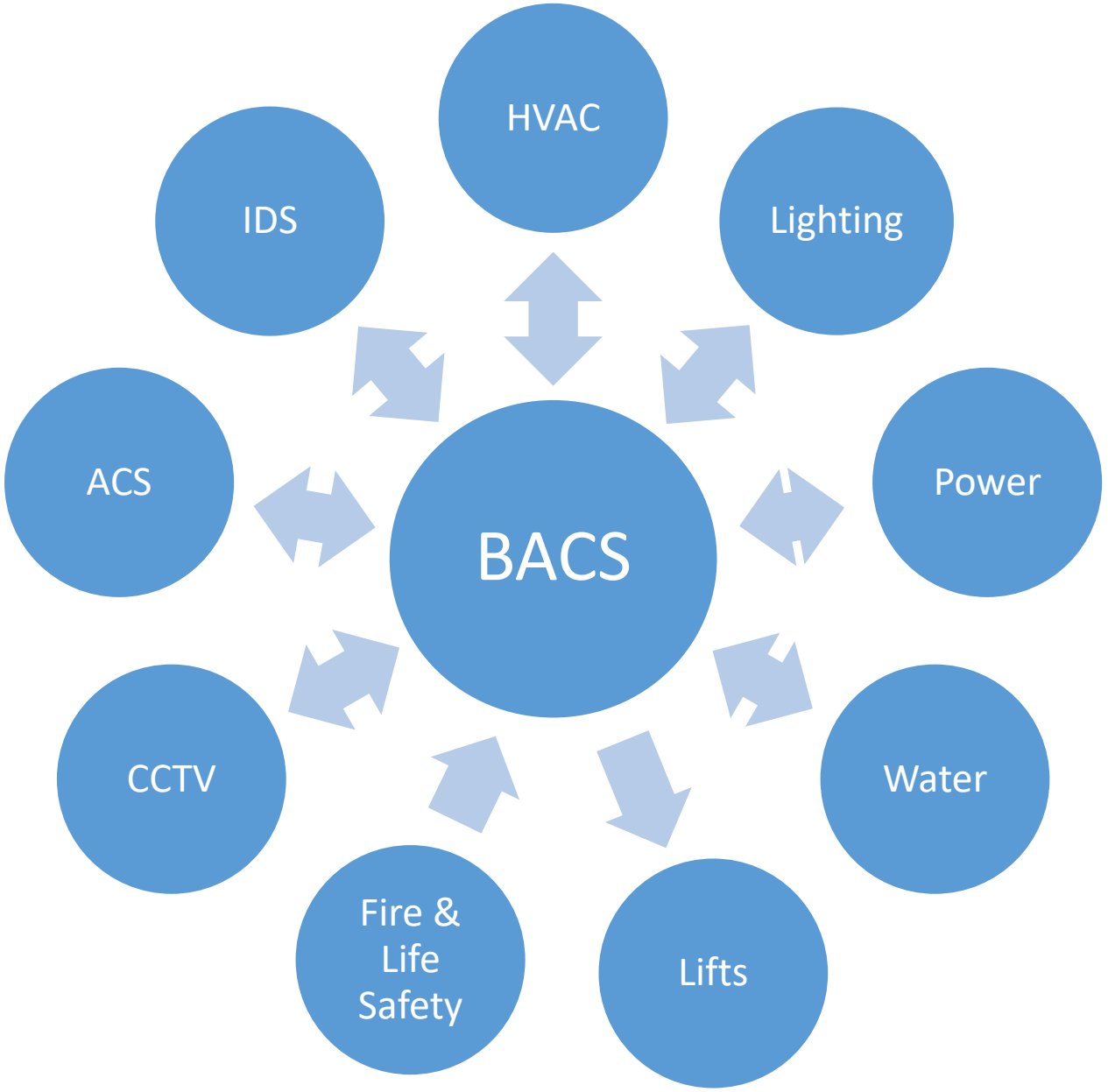
Intelligent Building
Building Automation &
Control Systems (BACS)

Background of Study

- 2010 exploratory study
- Funded & supported by ASIS Foundation, BOMA & SIA
- Objectives:
  - Articulate current BACS vulnerabilities
  - Evidence based understanding of security professionals' BACS awareness & practice
  - BACS Report

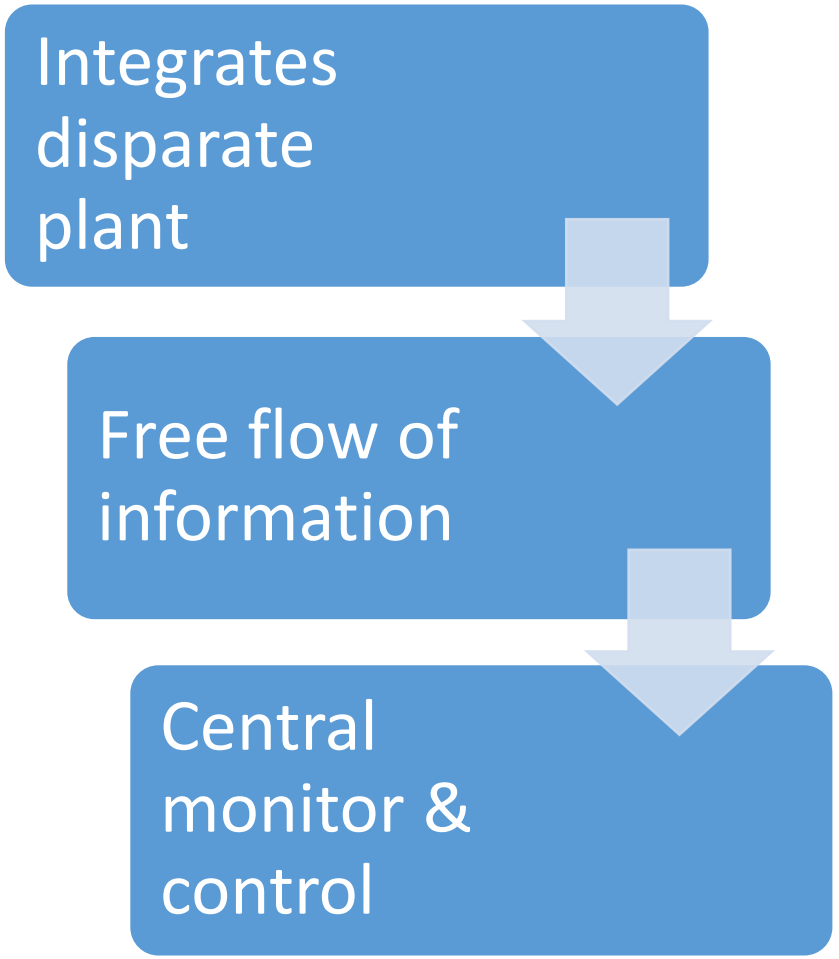
What are BACS?

What are BACS?

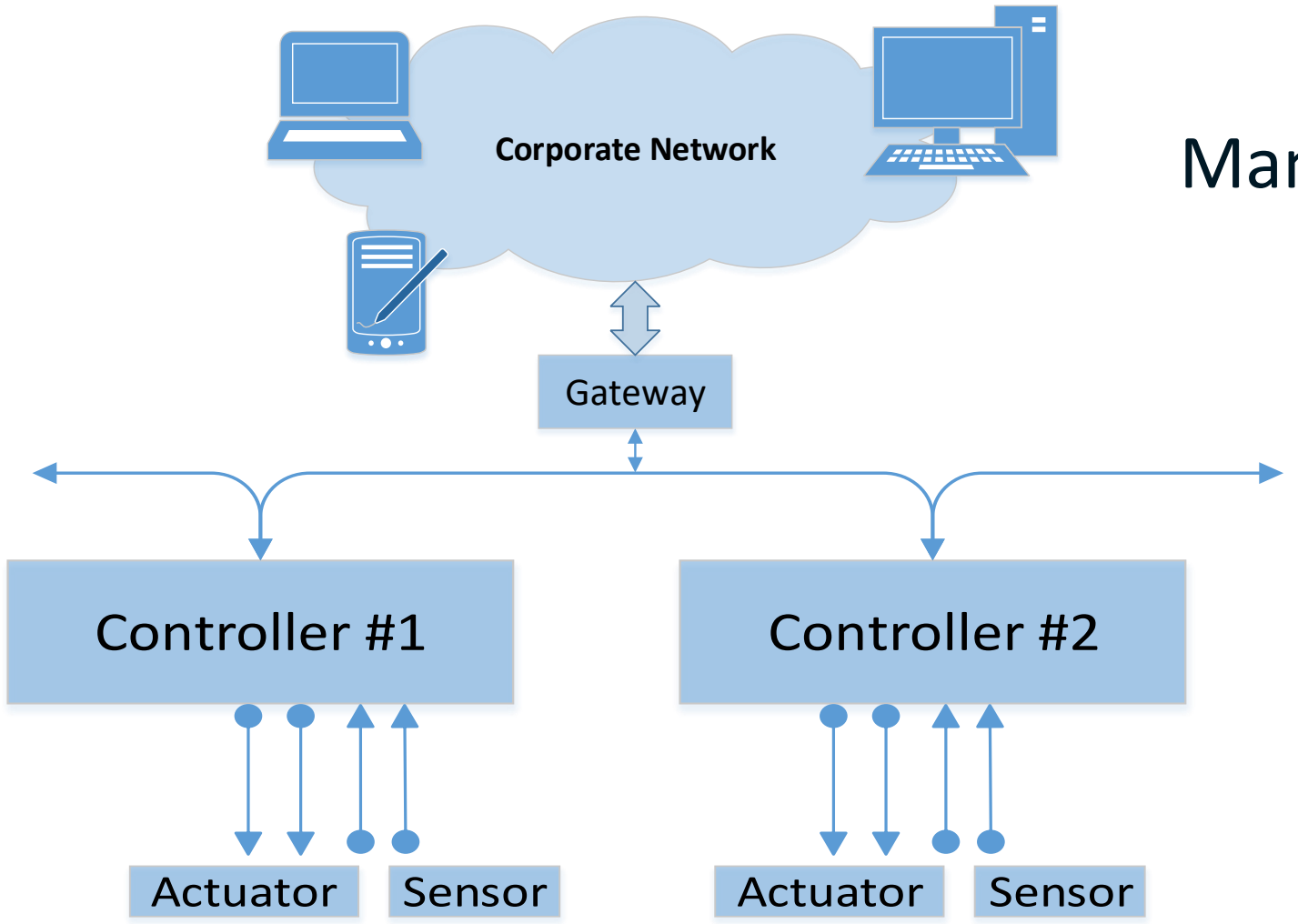


What are BACS?

- 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:
  - EMS, BAS, FMS, BMS, BACS, IB, Smart Building, +++



BACS Architecture?



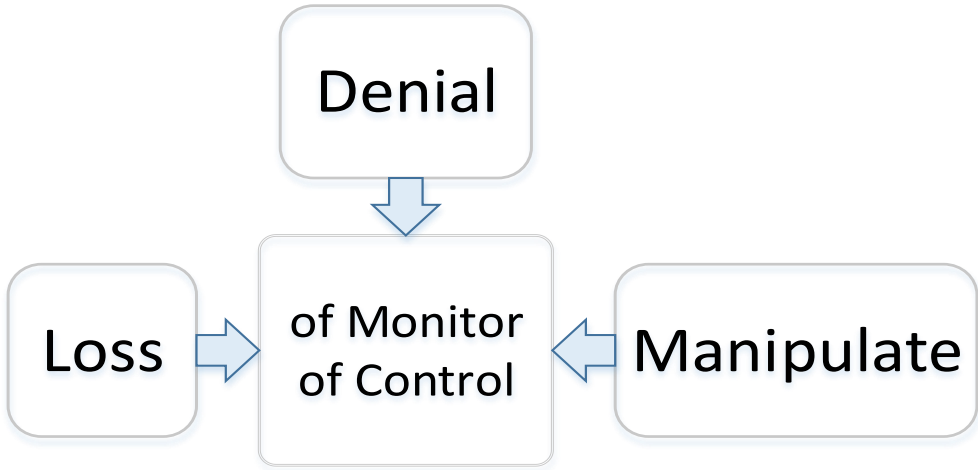
Management

Automation

Field Devices

The Security Problem

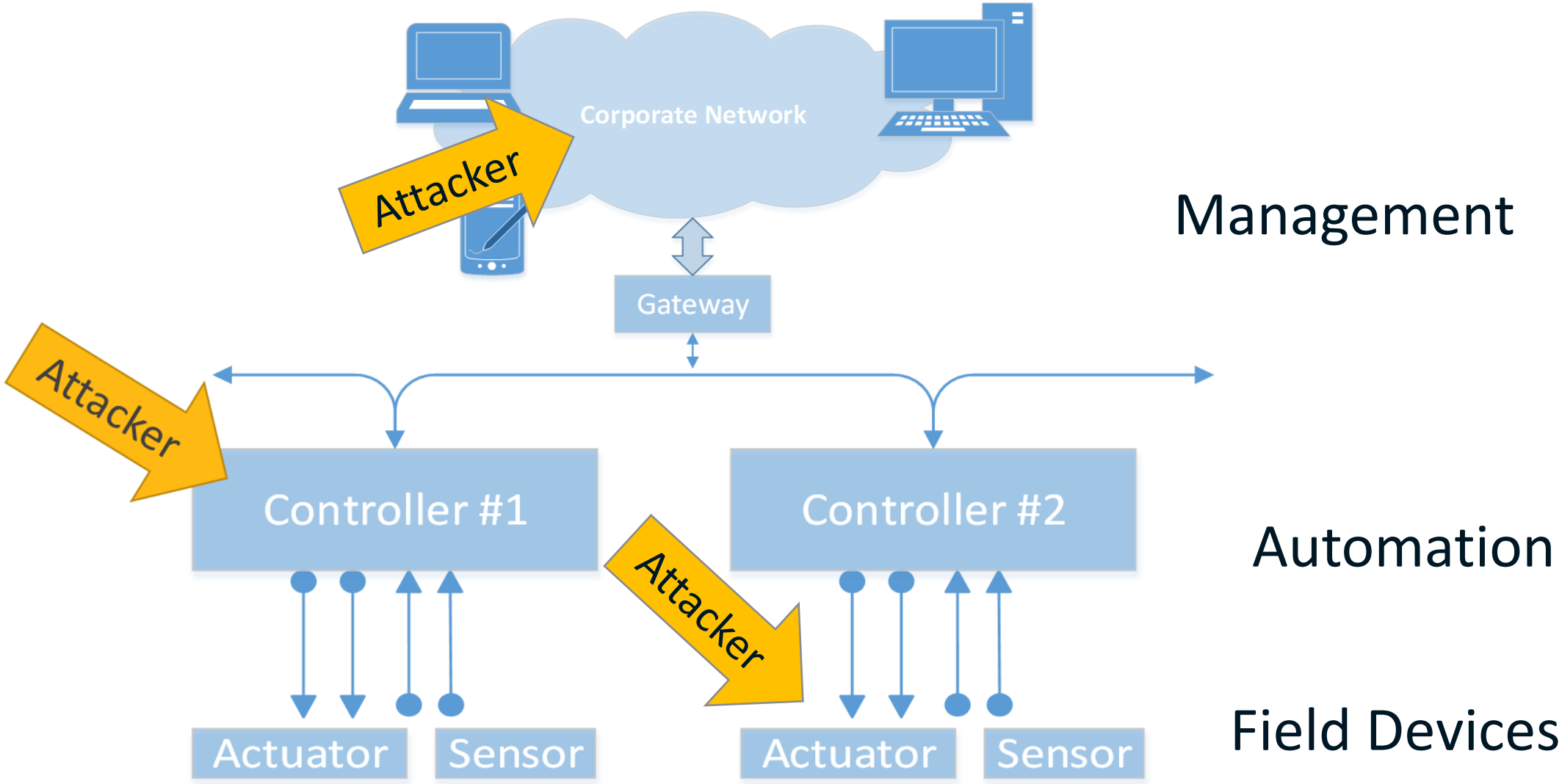
- BACS market value US$54-78 billion, @ annual growth 12-34%
- Converging all building systems
- Converging functionality at enterprise level
- Legacy issues
- Internet of Things
- Who owns & is responsible?
- Whole of building



Marketsandmarkets. (2017). *Building Automation System Market by Communication Technology (Wired, & Wireless), Offering (Facilities Management Systems, Security & Access Control Systems, & Fire Protection Systems), Application, & Region - Global Forecast to 2022* (SE2966).

TMR Analysis. (2017). *Commercial Building Automation Market 2016-2024*.

BACS Security Problem: Attacks



BACS Security Problem: Vulnerabilities

Management Level

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

Field Level

- Device access
  - Manipulation (on/off/alter)
  - Destruction
- Connection access
  - Manipulation
  - Destruction

Automation Level

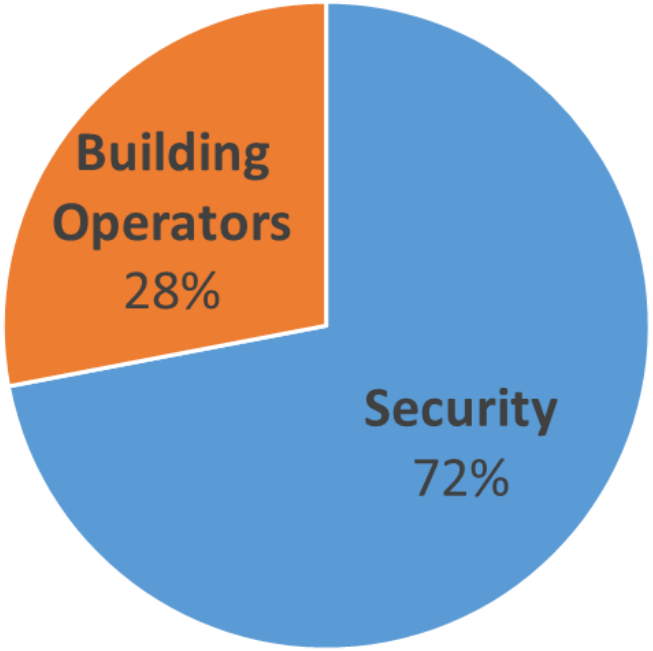
- Controller access
  - Cover
  - Manipulate inputs/outputs
  - Tamper detection
  - Field programmer
  - Embedded functionality
  - Power
- Communication network
  - Wiretapping (sniffing)
  - Monitor & analyze traffic
  - Open source programs
  - Data injection (fabrication)
  - Illegal Controller

	BACS Architectural levels		
	Field	**Automation**	**Management**
Device	Low	Critical	Moderate
Network	Low	High	Moderate
Software (Application)	Very Low	High	Moderate

Practitioners Understanding of BACS

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

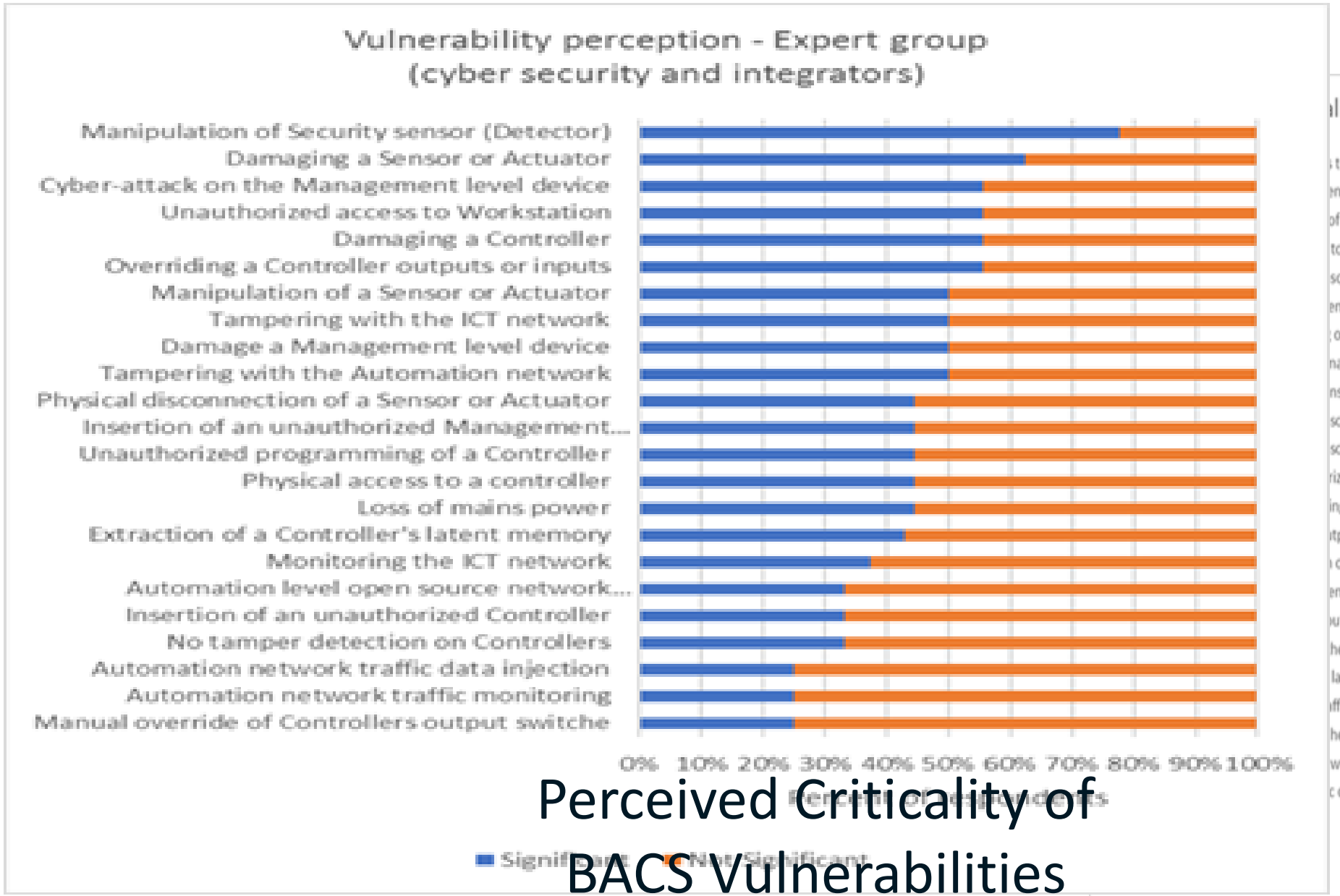
Respondents came from **38** Nations

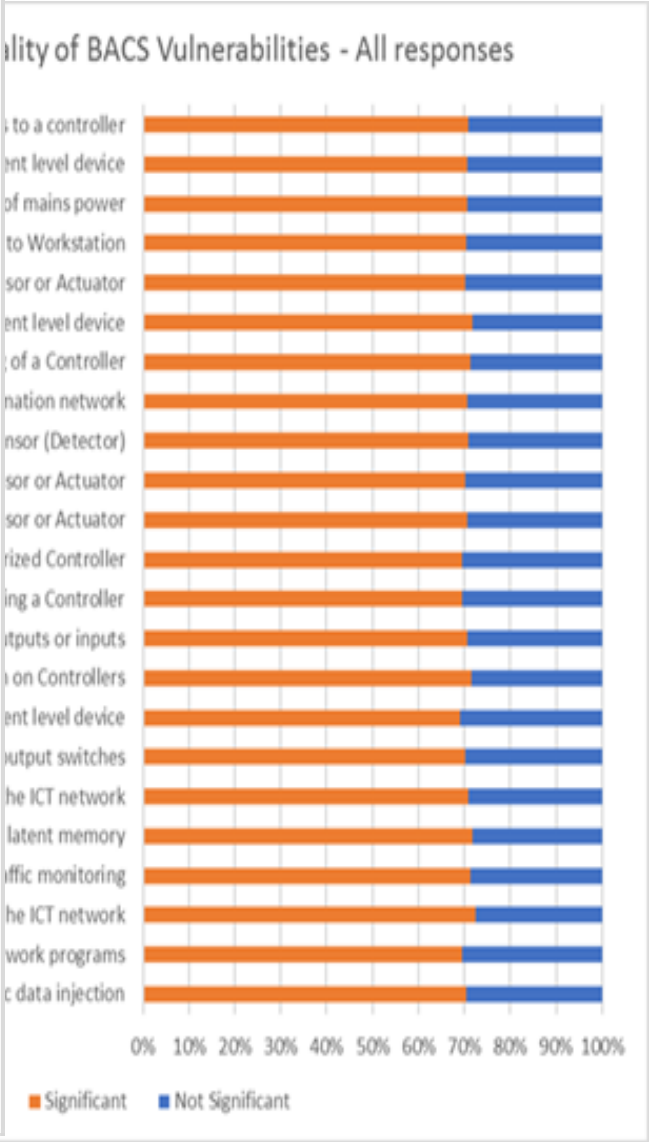


75 The percent of Respondents believed they had an awareness of BACS architecture

48 Percent of Respondents had BACS vulnerabilities in their Risk Register

8 Percent of builder owners & operators have responsibility for BACS





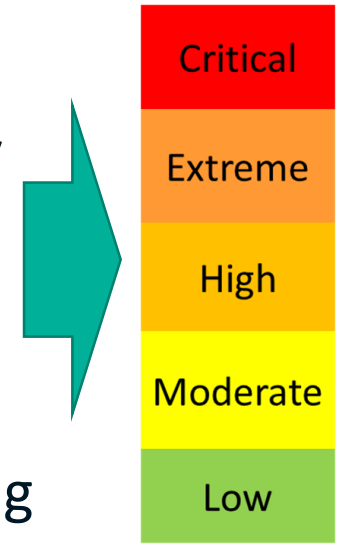
Perceived Criticality of BACS Vulnerabilities

BACS Security Guidance

1. Understand Context

2. Identify Criticality:
   - Operations
   - Occupancy
   - Board
   - Financial
   - Reputation
   - Safety
   - Regulatory
   - Information

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



Security Guidance: Criticality

Level	Operations	Financial	Safety	Regulatory	Information	Occupancy
Critical	Impact across all functions with extreme effect to all operations	Financial loss >10%	Multiple deaths	Loss of statutory accreditation to operate for extended period	Significant commercially sensitive info exposed	Unable to occupy whole facility for extended period
Extreme						
High	Substantial degradation of operations with impact to multiple functions	Financial loss >3%	Injuries or illness that results in hospitalization	Record of non-compliance against statutory accreditation	Restricted commercial info exposed	Unable to occupy major parts for extended period
Moderate						
Low	No measurable operational impact	Financial loss <1%	No resulting lost work	No effect on statutory accreditation	Limited info exposed	Limited effect on occupancy

Security Guidance

Security Level 1 Low

- ❑ Do you have a written & endorsed Security Policy?
- ❑ Is BACS formally assigned to the facility manager's portfolio & if so, who?
- ❑ Do your personnel security practices include pre-employment screening?
- ❑ Do you have an auditable procedure to authorize access to BACS?
- ❑ Are BACS Controllers, routers & network switches physically protected?
- ❑ Do you have a procedure for (mechanical) key control?
- ❑ Do you control your BACS remote and/or external logical access?
- ❑ Are your BACS logical program & configuration details held in a secure off-site location?

Security Guidance

Security Level 1 High

- ❑ Is BACS specifically included in your security policy?
- ❑ Do you undertake & propagate environmental scanning to stay informed on best practice to protect BACS?
- ❑ Are BACS security audits undertaken?
- ❑ Are regular audits of BACS Maintenance personnel status undertaken?
- ❑ Are the BACS Automation level communication network cables protected?
- ❑ During incident response training, are the facility's BACS included in response strategies?
- ❑ Do your BACS have an auditable log of all hardware & software changes & alterations?

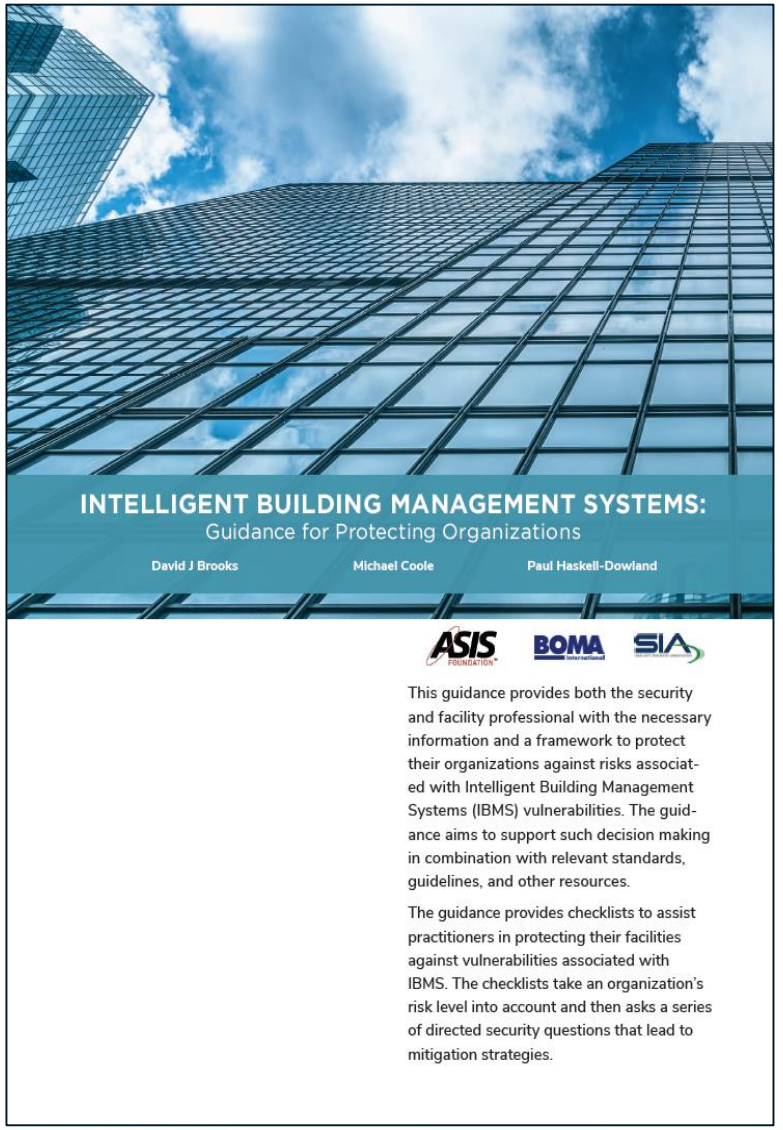
Security Guidance

Security Level 5 Critical

- Do you undertake a BACS specific threat assessment?
- Are BACS equipment or devices security tamper seals audited on a regular basis?
- Does your physical protection of BACS equipment or devices provide evidence of attempted or actual unauthorized access?
- Do you carry out technical surveillance counter measure evaluations 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 maintenance personnel escorted at all times whilst on-site?

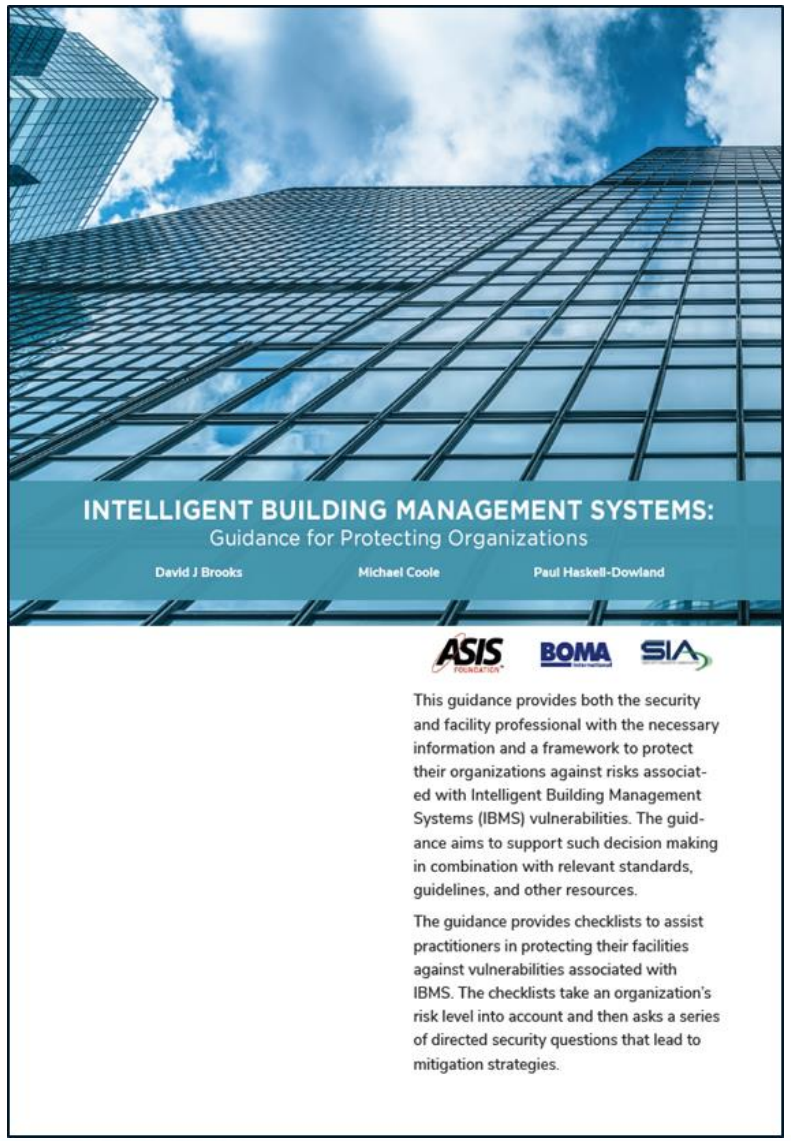
BACS Security Recommendations

- Gain awareness of BACS & it's functionality
- Form a BACS Working Group
- Include BACS in risk management reviews:
  - Criticality register
- Audit BACS
- Collaborate with BACS experts
- ASIS Foundation: *Intelligent Building Management Systems: Guidance for Protecting Organizations*



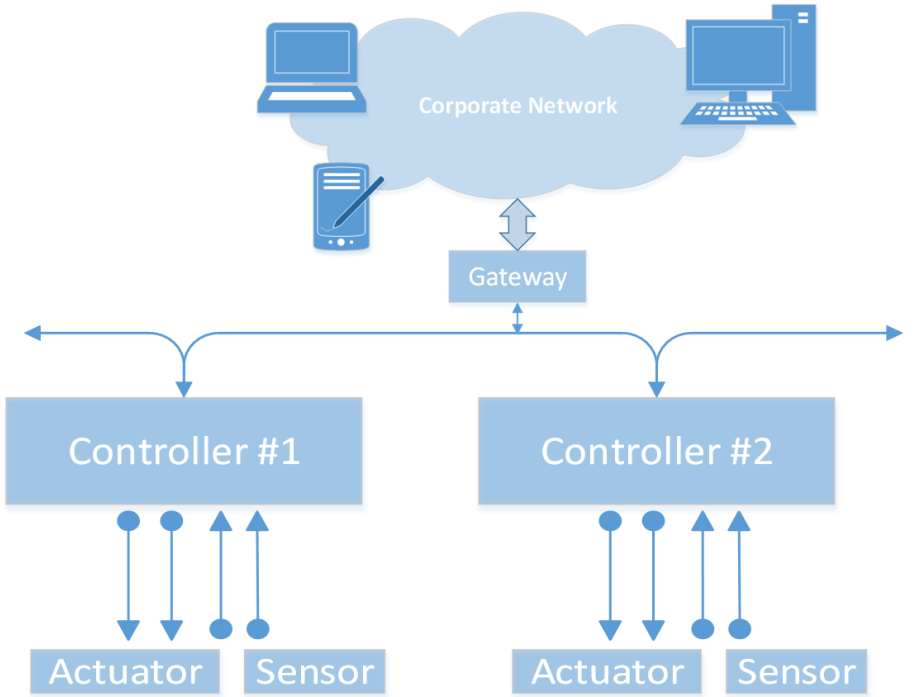
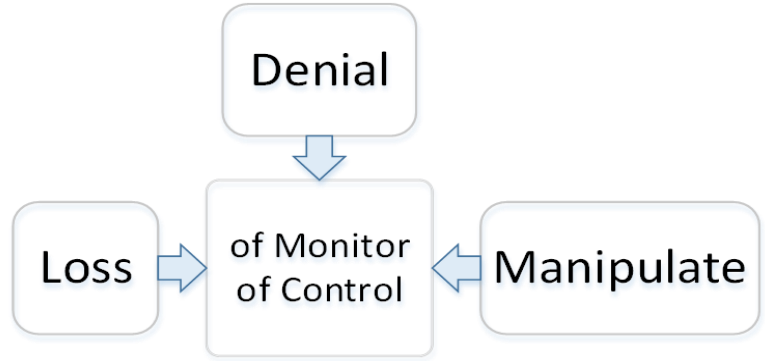
Concluding Remarks

- BACS will continue to grow, converging more building plant & business functions
- Responsibilities lie across multiple groups
- BACS have vulnerabilities & are a security risk
- Generic security strategies mitigation BACS risks
- Be aware & “Ask the Questions”
- https://www.securityindustry.org/wp-content/uploads/2018/08/Intelligent-Building-Management-Systems-Guidance-for-Protecting-Organizations.pdf



- Thank you

Questions?



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