Building Automation & Control Systems

An Investigation into Vulnerabilities, Current Practice & Security Management Best Practice

REPORT

David J Brooks
Michael Coole
Paul Haskell-Dowland
Melvyn Griffiths
Nicola Lockhart

AUSTRALIA ECU EDITH COWAN UNIVERSITY

ASIS FOUNDATION™

BOMA International

SIA SECURITY INDUSTRY ASSOCIATION

ASIS Foundation Project No.: FDN-BMS-2017

This Report was made possible by funding, support, collaborative and membership participation from:

ASIS Foundation

Security Industry Association

Building Owners and Managers Association

The authors would like to acknowledge the contribution and hard work of the many security and facility professionals who participated in this research. Without their contributed and time out of their busy schedules, the research could not have been achieved.

The Edith Cowan University's research team and Report authors comprised of:

David J Brooks, Principal Investigator

Michael Coole, Subject Matter Expert

Paul Haskell-Dowland, Subject Matter Expert

Melvyn Griffiths, Research Analyst

Nicola Lockhart, Research Analyst

Executive Summary

Building Automation and Control Systems (BACS) have become embedded into the contemporary built environment and its facilities. BACS technology and its connectivity extends across all types, sizes and functions of facilities for the purposes of not only automation, but the free flow of information. However, limited organizational awareness and understanding of BACS threats and vulnerabilities remain a concern, and their potentially impact to the organization.

THE PROJECT

The purpose of this project was three-fold. First, to review current and future BACS, including terminology, technical architecture and likely vulnerabilities. Second, to gain an evidence based understanding of security and facility professional's awareness, criticalities and security practice in regard to BACS vulnerabilities; and third, provide guidance to support security and facility professionals in BACS security design and maintenance activities.

The project applied a three-staged mixed methods research approach, to support evidence based findings and outcomes. The process commenced with a meta-literature review (Stage 1), followed by a survey (Stage 2) that was critiqued by focus groups (Stage 3) to garner deeper understanding. The survey (N=331) had responses from 38 different nations and diverse practice areas, with the majority from security (72 percent) and the remainder from facilities. The focus group participants (N=14) reviewed the survey findings and the draft BACS Guideline.

WHAT IS BACS?

Building Automation and Control Systems (BACS) is an automated system that converge, integrates and connects many different facility technologies through information flow to a monitoring point. BACS are modular, formed from the integration of devices, equipment and communication platform networks with open communication protocols. BACS are also known by many other terms, such as a Building Automation System, Building Management System, Intelligent Building, Smart Buildings and even, Smart Cities. With the Internet of Things, BACS will continue to expand into areas of the built environment and everyday life. Nevertheless, regardless of name, the core principles of BACS are the same; to facilitate free information flow and automated decision-making through connectivity.

BACS technical architecture is based on three levels, namely Management, Automation and Field device levels. The Management level contains the human interface, generally on the organization's enterprise network. The Automation level provides the primary control devices, connected via networked Controllers. The Field device level are the physical input sensors and output activators, connected to plant and equipment to monitor and control the environment.

The BACS market is growing between 15 to 34 percent per year, due to the demand for energy and operational efficiency and sustainability, increasing government regulation, and greater monitoring, control and operability. By 2022, the BACS industry will be worth an estimated US$104 billion. With global rises in energy costs and greater government sanctions, BACS is likely to be at the forefront of future facility projects.

PROJECT FINDINGS

Facility professionals manage and operate BACS, with 36 percent of participating building owners and operators indicating they have such a responsibility. Security professionals predominately manage and operate the security systems. Whereas, Information Technology professionals manage and operate the technical elements of networked systems, including the broader BACS architecture. Nevertheless, each professional generally focused only on their areas of practice and responsibility, resulting in silos of responsibilities.

Vulnerabilities in the BACS architecture are diverse, all which can be exploited for nefarious gains. Due to their physical location across all parts of a facility and connectivity with open protocols, BACS are prone to technical and physical attacks at all architectural levels; however, the Automation level is considered the most vulnerable. Generic BACS vulnerabilities were extracted and tabulated (Appendix A). Failure to appreciate such vulnerabilities results in the organization being exposed to security risks unknowingly. Nevertheless, BACS vulnerabilities are diverse and at most times abstract, presented without context or situation and resulting in difficulty for practitioners to understand and mitigate.

There is a significant disconnect between expressed security and facility professionals' perceived understanding of BACS threats and risks, and their actual understanding. Although 75 percent of security and facility professionals had an awareness of BACS architecture and half featured BACS risks in their risk management documentation, the majority of security and facility professionals displayed a limited understanding of BACS technical elements and there resulting critical vulnerabilities.

Security and facility professionals rated BACS criticality of vulnerabilities, at all architectural levels, relatively equal and with limited distinction. Such findings supported the assumption that security and facility professional lack robust understanding of BACS vulnerabilities. In contrast, Integrators (Vender, Installers) and cybersecurity professionals displayed a divergent and more accurate understanding of BACS vulnerabilities and their organizational significance. This group rated higher criticality of attacks against the Automation equipment and its network, demonstrating that they hold a higher level of BACS technical understanding that can be drawn on by organizations to achieve BACS security. Therefore, to manage the security of BACS requires information technology or cybersecurity professionals within, or integrated with, the facilities and security departments. Such professionals may be in-house information technology or cybersecurity professionals, or "third party" contractors, such as Integrators.

Half of the project participants reported BACS had integrated security systems, which is likely to significantly increase in the future. Nevertheless, findings indicate diverse views on the types of integrated security systems, directed by the professional being asked. The understanding of *integration* between security and facility professionals lacks definition or common understanding, leading to misunderstanding and therefore, further siloed view of associated security risks. Integration remains technically and functionally broad and undefined, with diverse views on meaning depending on one's occupational role. There is a lack of common understanding and clarity of language with BACS terms and practices.

BACS risks are contextual, aligned with the facility's threat and their functional criticality. Nevertheless, as with all security vulnerabilities, there are generic mitigation strategies that can be taken to protect these systems. Furthermore, BACS vulnerabilities are abstract and without context, making it difficult for practitioners to understand and mitigate. Therefore, the BACS Guideline (see Appendix I) was developed as a tool to aid professional decision-making. Security and facility professionals can address security related BACS questions to gain a level of assurance in protecting their organization or make informed decisions to accept risk without treatment.

Finally, the security and facility professional's lack of understanding and application of *security zones* was identified. The BACS Guideline has to be applied across many different built environments, with different threats and organizational criticalities and therefore, uses *security* *zones* in its security questions. However, many of the professionals had a limited understanding and practice of designing and applying security zones as a defense in depth method.

RECOMMENDATIONS

Across the security and facility professions, the project identified a number of key recommendations:

- Promote greater awareness of BACS and its threats and risks posed to the organization. However, such awareness has to be sound, easy to read and understandable to non-technical people.
- Improve cross-department liaison, using strategies such as a BACS working group chaired by facilities and with membership from security, cybersecurity and other relevant stakeholders.
- Build partnership with BACS experts, namely Information Technology and cybersecurity professionals, and Integrators. These professionals may be in-house or “third party” contractors.
- Provide a guideline that is simple to read and apply as an aid to security and facility professionals in the security of BACS, achieved via the publication of the proposed BACS Guideline.

The BACS Guideline provides a first-generation guiding document for all professions to address the many and changing threats and risks to BACS and its organization. The BACS Guideline provides a tool to inform and direct relevant professionals, as well as commencing the development of a common BACS language across its many stakeholders.

Contents

Section 1. Security of BACS

1.1 INTRODUCTION

Building Automation and Control Systems (BACS) and more recently, Intelligent Building systems, are becoming embedded and commonplace into much of todays' built environment and its facilities. BACS technology and its connectivity extends beyond just the large high rise commercial building, now adopted by industrial and smaller commercial buildings, and now even domestic residents. Primarily, the application of BACS are driven by the cumulative commercial need for increasing automation functionality and seamless flow of information across the organization, with a focus to reduce operating costs, and provide a more time responsive and safer facility.

The market increase in BACS will further drive greater built environment connectivity, as operators and users seek and demand greater and easier end-user functionality. As BACS become more interconnected throughout the facility and its corporate business network, more complex vulnerabilities become embedded at the corporate level that elevate corporate risk exposure.

BACS are generally owned and operated by facility professionals, with their focus on the primary drivers of cost efficacy and functionality that BACS offers a facility and its organization. However, BACS functionality are also used by many other departments and people in an organization. For example, security systems such as access control and CCTV, amongst others, may be integrated into BACS. Furthermore, the technology of BACS lies across multiple departments of the organization, from the Facilities department to the Information Technology (IT) department, on which the corporate network facilitates the flow of BACS information across the business, to the security department.

The technology of BACS may also be known by many other terms, such as Building Management Systems (BMS), Intelligent Buildings (IB) and increasingly, Smart Buildings and even Smart Cities. However, a more precise term is *Building Automation and Control System* (BACS), which is supported by literature such as the International Organization for Standardization (International Organization for Standardization, 2007a).

The technology of BACS spreads throughout all parts of a facility and with multiple users, leaves these systems open to threats and risks. BACS are designed and operated by building engineers and facility professionals, who may not have an appropriate focus on the broader security risks of the business and its facilities. Yet the security of BACS is a significant business concern and therefore, the security strategies to mitigate the risks against breaches of confidentiality, integrity and availability within the BACS must be embedded in the corporate culture.

Nevertheless, the level of awareness, understanding and practice of the various professionals responsible for protecting BACS is not well known. Therefore, this project set out to achieve various objectives including an evidence based understanding of what is known and practiced with BACS security by the various responsible professionals. Furthermore, to develop guidelines that summarizes these research findings through a hierarchical decision tool. A decision tool that is a functional aide memoir for relevant stakeholders to ensure that the threats that pose a risk from BACS connectivity can be considered and managed accordant with organizational expectations.

1.2 PROJECT OBJECTIVES

Cognizant of the increasing use, functionality and connectivity of BACS and their exploitable vulnerabilities, the security and facility professionals require some understanding of these systems to ensure sound risk mitigation decision-making and governance. Therefore, an increased awareness and understanding enables the professional to provide a more informed and robust advisory service to their organization. Therefore, the purpose of the project was to meet the following Research Objectives:

1. Develop a meta-literature basis of current BACS, including their terminology, architecture and associated vulnerabilities,
2. Gain an evidence based understanding of the security and facility management professional's awareness and comprehension of BACS vulnerabilities, their criticality and associated security practices; and
3. Provide a summary guideline to support security and facility professionals' decision-making when undertaking BACS design, installation and security management activities.

This Report is submitted to meet these three Research Objectives.

1.3 SIGNIFICANCE OF PROFESSIONALS' UNDERSTANDING OF BACS

Building Automation and Control Systems (BACS) are today integral in most large and medium facilities, and will become more so into the future. Gone is the period when only large multi-story or industrial complexes used BACS. Technology connectivity and convergence, driven by the need for improved and easier business functionality and flow of information, will further integrate BACS into the majority of today's facilities. BACS manufacturers continue to strive to integrate all technology within a facility and today, this extends to the functionality of business practice and services that includes the function of security.

The global business of managing and operating facilities indicates a growing reliance on BACS and its service focused industry. The drivers for BACS; a demand for reduced operating and utilities costs, greater sustainability legislation and regulation by governments, increased governance and accountability, and more informed business information to achieve necessary business solutions. These solutions include the use of modern connectivity technologies that provide automated monitoring, control, operating and auditing functions.

Many organizations and their facilities are investing in some form of embedded BACS. Organizational awareness and reduced risk appetites have increased the demand for changes in building design, operation and maintenance that are more cost effective through automation, and today, this includes the function and technologies of security.

Nevertheless, not all operators understand the threats and risk associated with connected and functional BACS, which spans not only the physical facility but also the digital environment. BACS are becoming far more complex than traditional standalone and isolated facility plant, such as Heating and Ventilation Systems, lighting, etc. Furthermore, maintenance personnel must access and operate these multiple systems required for BACS, many with limited security cognizance. These issues leave many BACS prone to exploitable vulnerabilities, and their organizations exposed to significant threats and risks.

In the very near future, the function of security will be fully integrated into BACS. Currently, many BACS devices do not cater to physical security requirements, such as the use of anti-tamper detection, monitored supervised connectivity or even battery backup. Common practice and functionality for intruder alarm systems is not considered or applied in the design and maintenance of BACS. Such a lack of functionality may be due to security designers and managers (along with facility owners and operators), not understanding the extent to which BACS converges with other facility systems.

1.4 INCREASING THE PROFESSIONAL'S BODY OF KNOWLEDGE

The project supports the development and formulation of a body of knowledge in the security design, application and management of BACS. Such a body of knowledge informs security strategies in mitigating BACS threats and risks, enhancing the future security of the built environment and its facilities to reduce corporate risk.

The security body of knowledge has a distinct knowledge category of Physical Security, with embedded technology (Brooks, 2010, p. 12; Coole, et al., 2017) to which this project, in part, will assist in extending into the cybersecurity sub-domain. Such knowledge will include the relationship between facilities and security, vulnerabilities and mitigation strategies, through formal and professional guidance. Finally, the project findings facilitate more directed education and awareness programs, based on what is actually understood, is being practiced and what is required to successfully mitigate the threats that pose a risk.

1.5 The Security Problem

BACS is a progression in the development of technology in response to increasing requirements for a flexible, comfortable, adaptable and sustainable built environment. However, the primary drivers are the need to reduce costs and be more adaptable with fewer resources, while ensuring a safer and more secure environment. The integration of converged infrastructure with facilities and business systems, while creating new business enhancement opportunities, also creates new opportunities for security, both physical and cyber related.

BACS Legacy

Another issue is that of legacy BACS technologies. As King (2016) points out, early generations of automation systems were developed using discrete devices and protocols, lacking the necessary strategic and holistic approach required for facility control. It therefore follows that facilities that are most vulnerable to attack are buildings with legacy BACS that have been built upon and added to, rather than purpose built (Sinopoli, 2012). The vulnerabilities of older systems may be public knowledge through hacker-run searchable websites such as www.shodan.com, which publicizes known BACS vulnerabilities. While King's (2016) focus is on cybersecurity issues, his assertion is that since "these service-based systems were not initially interconnected, they were not designed with logical security as a paramount concern or requirement" (King, 2016). In other words, they remain vulnerable to breaches of confidentiality, integrity and availability by adversaries with intent and capability.

Local and Remote Access

The general view is that the threat to BACS and its facility is from access through an external network. Such remote access is generally amplified when a facility has a large Information and Communications Technology (ICT) infrastructure, with considerable integration with other business systems. Therefore, the "overarching concern is more about network security and less about physical security, although the two are certainly related" (Sinopoli, 2012). However, exploitation through physical localized access remains a robust threat.

The ability to breach BACS locally exposes a facility to not just physical break-in or attack, but also access to those other business systems that may be connected internally to the building automation systems, even if they are "off the grid"(King, 2016). Consequently, the tendency to focus on cybersecurity may create a false sense of protection within the BACS industry. Isolating BACS from external networks may mitigate some remote attacks, but does not address the security vulnerabilities resulting from physical access on the automation network. As Sinopoli (2012) concludes, this type of attack is potentially much more dangerous and difficult to deal with. Furthermore, such a mitigation strategy restricts the business drive for functionality, which in most cases is the reason why BACS was first installed.

BACS Interconnectivity

The inevitable shift in BACS towards greater interconnectivity and all things connected (Hosain, 2016), with the advent of the Internet of Things (IoT) and Building Internet of Things (BIoT), means the ability to physically breach a single system has much greater ramifications. As Wyman (2017, p. 2) suggests, maliciously exploiting vulnerabilities to manipulate the system can cause physical consequences, with cascading impacts in operations, maintenance, process, safety and business. The significance of such attacks is that access into one system potentially means access into all, whether this remains at a local level or extends into external networks, the level of damage to a company and indeed to human life could potentially be catastrophic. Consistent with other office and business information systems, the BACS elements have significant threats that pose a risk to the confidentiality, integrity and availability of their data and other business elements.

With the ever growing use of such technological approaches as the IoT, BACS are becoming more complex. They are spread throughout all parts of a facility, with various levels of communication networks and protocols. To be truly aware and understand the many interrelated exploitable vulnerabilities becomes difficult, especially for non-technical security and facility professionals. This issue is amplified by the diverse applications within BACS, because diversity results in the many sub-systems becoming “owned” or the responsibility of different groups within the organization. Such groups include, but may not be limited too, facility and services, ICT and security. Furthermore, many other business groups use the functionality of BACS, such as human resources, occupational health and safety, etc.

BACS Vulnerabilities

BACS exploitable vulnerabilities can be considered from a number of threat facilitating aspects, namely physical access to devices, network, and software; however, these must be given a context based on the automation’s architectural level. Device and network vulnerabilities include physical access to the automation equipment or hardware, workstations and communication networks. Threats of such access include wiretapping, local and remote connectivity, foreign device insertion and local reprogramming. Software (applications) vulnerabilities include common and open protocols and restricted encryption. Threats of such software access include denial of service, data information theft, covert facility entry or espionage, loss of data confidentiality, integrity or availability, and access to other business packages.

The consequences of realized threats for BACS can be divided into three categories (Table 1.2) of loss, denial or manipulation (Assante & Lee, 2015, p. 11). These consequences pose a significant risk to the confidentiality, integrity and availability of the organizations’ data and other business elements.

Table 1.2

BACS Categories of Consequence

Category	Consequence
Loss	Loss of monitoring
	Loss of control
Denial	Denial of monitoring
	Denial of control
	Denial of safety
Manipulation	Manipulation of monitoring
	Manipulation of control
	Manipulation of sensors or actuators
	Manipulation of safety

BACS Contextual Risks

BACS risks are contextual, aligned with the facility's threat exposure, their criticality of manifestation and environmental situation. Nevertheless, as with all security vulnerabilities there are generic mitigation strategies that can be established to protect these systems. Protection includes situational threat driven security risk management, understanding system architecture and criticalities, integration or closer working relationship between previously segmented departments, a degree of network isolation and greater awareness.

1.7 OVERVIEW OF THE REPORT

The Building Automation and Control Systems (BACS) project Report is divided into a number of discrete, but supporting sections. Some sections align directly to the research and resulting data collection and interpretation, whilst others provide background information.

Section 2. Project Methodology

The BACS project applied a mixed methods research methodology, with both qualitative and quantitative analysis. The intent was to ensure that project findings and resulting outcomes were evidence based. Consequently, Section 2 presents the project's three-staged process, including the meta-literature critique (Stage 1), participant survey process (Stage 2) and focus group interviews (Stage 3). In addition, each stage's underlying sampling, research materials and instruments, data collection and analysis approach, ethical considerations and the project's limitations are discussed.

Section 3. What is BACS?

BACS has become and will continue to be increasingly common in the built environment, converging many diverse building systems as computing technology developed and connectivity became more available. Section 3 introduces the premise of Building Automation and Control Systems (BACS), including the many terms used such as Building Automation Systems (BAS), Building Management Systems (BMS), Building Energy Management System (BEMS), Intelligent Buildings (IB) and increasingly, Smart Buildings and even Smart Cities. Therefore, this section explores and denotes the many types of BACS, with the aim to provide a corroborated categorization of BACS to support current understanding.

Section 4. BACS Fundamentals

BACS are modular in nature, formed from the integration of a number of sub-systems, equipment and devices connected and communicating on a common networked platform. Therefore, Section

4 provides a simplified technology overview of BACS, based on three levels of architecture. BACS architecture levels are Management, Automation and Field levels.

In general, the Management level contains the human interface, operating on servers and through routing devices, and connected via the corporate communication network alongside other corporate applications. The Automation level provides the primary monitoring and control equipment and devices, connected via a dedicated automation network. This automation network connects Controllers and operates via common communications protocol such as BACnet, LonWorks, Transmission Control Protocol (TCP), Internet Protocol (IP), Hypertext Transfer Protocol (HTTP), to name a few. Finally, the Field level includes devices connected to specific plant and equipment as sensors or activators, providing specific functions. Field level devices may be a light switch, temperature gauge, a valve or a Passive Infrared detector (PIR).

Section 5. THE BACS Market

The BACS industry market is a global enterprise, with the driver to extract key business functionalities from facilities. The manufacture and supply market is segmented by geography, end-user typology (government, commercial or residential) and required business solutions. Therefore, Section 5 presents an overview of both the current and future BACS industry, an analysis of the market, and an overview on the size and embedded nature of the automation industry. For example, BACS are growing at approximately 15 to 34 percent per year and by 2022, the BACS industry will be worth an estimated $104 billion. Such predictive growth highlights the current and expected impact that BACS will have in most built environments and its facilities.

Section 6. BACS Industry

Given the current and forecasted BACS market growth, a competitive vendor landscape has developed at both the national and global levels. The BACS market and its manufacturers are dynamic, as major building and today, technology incumbents continue to evolve their offerings, responding with new mergers and acquisitions on both national and global scale. The result is new and innovative types of manufacturers, suppliers and integrators, such as software start-ups, continuing to enter the BACS industry.

Given such a dynamic industry, competitive advantage is likely to result in greater operational and business functionality, broader technical convergence, less expensive platforms and ever greater connectivity. These drivers are likely to increase system vulnerabilities, because one element of the BACS architecture can facilitate unauthorized access to other more critical parts by malicious actors. Therefore, Section 6 identifies the current global BACS manufacturers, and the size and scope of the industry. Such understanding will assist, in-part, raising the awareness of the current and changing threats and vulnerabilities that pose a risk for the security and facility professional.

Section 7. BACS Automation Level Vulnerabilities

Vulnerabilities represent an aspect of the BACS architecture that can be exploited for nefarious gains. Due to their connectivity and common language protocols, BACS are prone to both technical and physical attacks at all architectural levels, although the Automation level is considered the most vulnerable. Consequently, BACS vulnerabilities have been presented (see Appendix A) in the three architectural levels of Automation, Management and Field devices.

Within the BACS architecture, Section 7 presents the Automation level that provides the connectivity between the many field devices and supports the functionality of the Management level. The Automation level typically applies an open industry communications protocol and is in essence an industrial control network, where generated data is distributed across its network to monitor and control.

The Automation level includes both hardware and software system elements, and therefore there are vulnerabilities associated with each of these elements. Given the differing functionality and communication connectivity, vulnerabilities are diverse. Furthermore, as device processing and connectivity capability increase, so do the vulnerability possibilities and consequences when vulnerabilities are realized. Therefore, this section tabulated the literature on BACS Automation level vulnerabilities and associated devices.

Section 8. BACS Management & Field Level Vulnerabilities

The BACS architectural Management level is the human interface, providing systems functionality. The Management level is an information system, with the intent that the facility is operated and maintained as efficiently and effectively as possible (Lowry, 2002). Furthermore, the Management level software is a relatively minor element of the corporate communications network, shared with the many other enterprise operating packages.

In contrast, the Field level provides connectivity from and too the many field devices to the Automation level. The field devices are spread throughout all parts of the facility. Field devices may be a light switch, a temperature sensor or security detector (as system inputs) or a cooling valve or fan drive (as system outputs), just to name a few. Both levels typically apply open industry communications protocols.

As with the Automation level, these levels include both hardware and software elements, and therefore there are vulnerabilities associated with each of these elements. Given the quite different technologies, functionality, processing capability and communications connectivity, vulnerabilities of these levels are diverse. Therefore, this section tabulated the literature on BACS Management and Field level vulnerabilities and associated devices.

Section 9. Stage 2 Survey of Understanding

BACS will continue to become common place in the built environment, which impacts on many departments, groups or persons in an organization. However, there is limited organizational and professional awareness and understanding of BACS and in particular, their vulnerabilities to threats, and resulting risks. Therefore, this section presents a survey of security and facility professionals understanding and awareness of BACS security, including the analysis of the collected data and interpretation in response to the posed project questions and resulting sub-questions.

Primary findings of Section 9 found that security and facility professionals demonstrated limited understanding of the significance of BACS vulnerabilities and therefore, appropriate mitigation strategies required to protect against malicious interference.

Section 10. Stage 3 Focus Groups

Drawing from the previous Stage 2 findings and enhanced through expert panel discourse, this section presents Stage 3. Stage 3 provides a deeper understanding of BACS concerns of security and facility professionals. Findings indicated that for many professionals, they do not understand the security issues associated with BACS. This section presents the focus groups and their participants, the collected data, including key participant statements and analysis, and stage interpretations. More importantly, this section also discusses the critical review and changes to the final BACS Guideline. In addition, how both security and facility professionals can take guidance from cybersecurity and technical integrators in the security of BACS.

Section 11. Project Findings

The project findings respond to the three Research Objectives; however, further findings on security zones developed as a theme during the project. A meta-literature review of BACS identified numerous BACS terminologies, a large commercial manufacturing market that is growing each year, and a list of generic BACS vulnerabilities.

An understanding of security and facility professionals' BACS awareness and practice, security vulnerabilities and their organisational criticality significance was gained, along with associated but generic security mitigation measures. Findings highlighted a lack of robust technical BACS knowledge, along with the associated criticality of technical and procedural vulnerabilities resulting in increased organizational security risks. However, a BACS Guideline was developed and critiqued, to provide an aid to decision-making by security and facility professionals, towards better mitigation and communication of BACS threats and risks. Finally, the concept of security zones was identified as a concept that requires greater understanding, in particular, by security professionals.

Appendix I. BACS Guideline

One of the primary purposes of the project was to support security and facility professionals' decision-making, when undertaking BACS design, installation and security management activities. To provide such support, a BACS guideline was developed and critiqued. The BACS Guideline provides guidance to help ensure that a facility's BACS is, where necessary, protected from foreseeable threats and risks that may impact the organization. The intent of the Guideline is to provide a tool to aid decision-making, whereby security or facility professionals can address relevant security related questions to gain a level of assurance in protecting their organization, or make informed decisions to accept risk without treatment.

1.9 CONCLUSION

Building Automation and Control Systems (BACS) are becoming commonplace, embedded into todays' and the futures built environment and its facilities. The technology and connectivity of BACS extends well beyond just the large or high rise commercial building, now adopted by all facility types, sizes and functions. The drive for BACS is commercial, a need for increased functionality and flow of information across the organization to reduce operating and maintenance costs. In addition, to provide a facility that is more time responsive and safer. BACS are not just a convergence of plant and equipment; rather, they are now a business information system.

BACS are spread throughout all parts of a facility and across all levels of its communication networks. Different departments, groups and people within an organization use or rely on BACS. For example, the function of security and its associated technology is currently and will be more so, subsumed into BACS. However, BACS are designed and operated by building engineers and facility management professionals, who may not have a focus on the security threats and risks of the business and its facilities. Yet the security of BACS is a significant business threat facilitator and therefore concern. Consequently, the security strategies to mitigate such risks against breaches of confidentiality, integrity and availability must be embedded in the corporate culture.

BACS are prone to exploitation. For the security and facility professional, such exploitation places the organization at risks that may ripple throughout the whole business, resulting in substantial and far reaching impacts. Therefore, the security and facility professionals need to have a comparative awareness and understanding of BACS, their vulnerabilities and mitigation strategies.

Nevertheless, the level of awareness, understanding and practice of the various professionals responsible for protecting BACS is not well known. Therefore, this project set out to gain an evidence based understanding of what is known and practiced with BACS security by the various professionals. Furthermore, the project aimed to develop guidelines that summarizes these findings through a hierarchical decision-making tool. This Report addresses each need in the following sections, to be able to manage BACS threats and risks in accordance with organizational expectations.

Section 2. Project Methodology

2.1 INTRODUCTION

The Building Automation and Control Systems (BACS) project applied a mixed methods research methodology, with both qualitative and quantitative analysis to ensure that findings and resulting outcomes were evidence based. Consequently, this section presents the project's three-staged methodology, including the literature critique, participant survey process, focus group interviews, data analysis, research materials, ethical considerations and the project's limitations. In addition, both Stage 2 and 3 methods and materials are presented in detail in support of the proceeding sections.

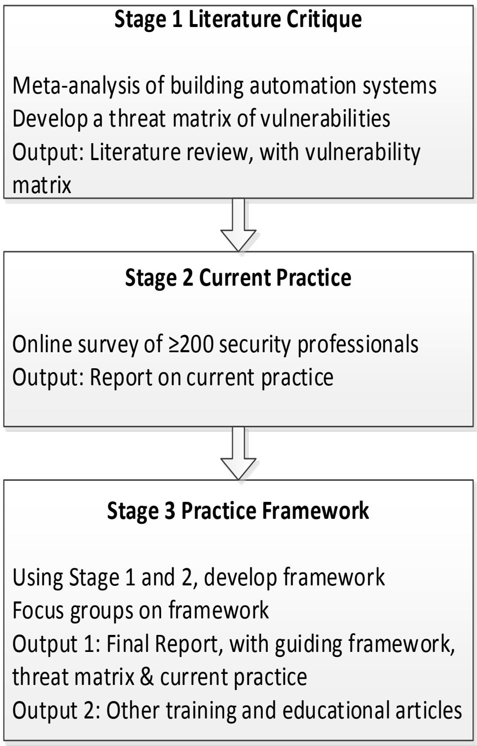
2.2 PROJECT METHODOLOGY

The project applied a three-staged research approach (Figure 2.1), with explicit research objectives and deliverables at each stage.

Stage 1 embodied a critical review of the available literature to present an articulation of BACS technologies, including definitions, roles in the built environment historical and contemporary, system architecture, prevalence in the built environment, the dominant manufacturers and market situation. Following this discussion, the technology of BACS and its exploitable vulnerabilities were evaluated in accordance with the existing research body of literature and an associated threat matrix developed.

Stage 2 assessed current BACS awareness and practices of security and facility professionals when engaged with the management of the built environment. This stage applied an online survey propagated through ASIS International, BOMA and SIA. The survey contained both Likert and semi-structured questions. Likert data was analyzed using measures of central tendency including mean, standard deviation along with various correlation analysis. The open–questions were analyzed using thematic analysis techniques applied to participants' responses.

Stage 3 drew on Stages 1 and 2 findings to develop a BACS Guideline. This stage sought to both interpret the research findings, and also support both the security and facility professional in their understanding and practice of BACS security. In addition, the focus groups critiqued the professional awareness and practice of BACS, garnered from the Stage 2 online survey and also added further refinement to the Guideline to ensure practitioner usability. This process facilitated a deeper understanding of issues encountered by security and building professionals when managing the threats associated with BACS, and their subsequent ability to apply the BACS Guideline to achieve such protection. The focus groups applied semi-structured questions, with responses analyzed using content and thematic analysis techniques.



Stage 1 Literature Critique

Meta-analysis of building automation systems
Develop a threat matrix of vulnerabilities
Output: Literature review, with vulnerability matrix

Stage 2 Current Practice

Online survey of ≥200 security professionals
Output: Report on current practice

Stage 3 Practice Framework

Using Stage 1 and 2, develop framework
Focus groups on framework
Output 1: Final Report, with guiding framework, threat matrix & current practice
Output 2: Other training and educational articles

Figure 2.1 Project Design

2.3 SURVEY OF UNDERSTANDING

The Stage 2 was applied using various association participants via an online survey approach.

2.3.1 Participants

The project drew on a non-probability convenience sample, and applied an online survey of ASIS International, BOMA and SIA members (N=331) which was emailed to potential participants using the respective organisations official data base. This method successfully achieved a statically valid random sample across the three associations. The respondents came from 38 nation states, with the majority from the Unites States (73%), followed by the United Kingdom (5%) and Canada (4%). The assumption was that BOMA and SIA respondents, given their geographical membership, had a higher majority of United States respondents. However, ASIS gained respondents from a broader worldwide sample.

2.3.2 Materials

The survey used Qualtrics survey software to enable respondents to undertake the survey online from any location with web access. The survey (Appendix E) consisted of 18 questions and gathered data on each respondent's role, understanding, knowledge and of BACS vulnerabilities, their criticality and associated mitigation practices. The survey contained mixed questions, including yes/no, Likert and self-response questions. Data was therefore collected in two forms:

1. Quantitative data
2. Self-directed text data

2.3.3 Procedure

The survey followed a logic path (Appendix D), which at certain points removed respondents from having to address contextual questions which they felt they did not understand or were not relevant. This approach provided a number of benefits, such as removing respondents whose poor understanding of a particular question might result in random responses, as well as reducing the time busy respondents needed to complete the survey. It was expected that this would ensure a higher number of respondents across the broad practice areas of security and building operators.

The research procedure involved sending out email invitations to ASIS International, BOMA and SIA members, inviting participation in the online survey. Respondents followed a link in the email to the online Qualtrics survey. Statistical power analysis was used to determine when a sufficient sample size had been achieved.

Respondents to the survey were first asked whether their job function was Security, Building Owner/Operator, Consultant or Other. Depending upon the response to this question, a selection of job roles related to the job function selected were displayed. Respondents were then asked whether they were aware of the different levels of BACS architecture. Those who responded yes were then asked to rate their level of understanding of each of the three architecture levels on a Likert scale from very low to very high. Respondents who indicated that they did not have an understanding of BACS architecture were not asked to rate their level of understanding.

All respondents were then asked whether or not BACS vulnerabilities featured in their group risk register. They were also asked to rate, on a Likert scale (strongly agree to don't know), the positive impact of BACS within the context of their organisation, and to list in a free text field the positive and negative impacts. Respondents were also asked whether or not they were responsible for the management of a BACS. Those that indicated yes were asked further questions about their role in relation to BACS security.

All respondents were finally asked whether within their organisation there was security system integration with the BACS, and which specific systems such integration included. This question was followed by asking respondents to rate the level of criticality on a Likert scale of 23 BACS vulnerabilities; the levels at which they applied different mitigation strategies; and which stakeholder groups they engaged with. The aim of this question was to facilitate a conformational analysis between participant's perceptions of understanding for BACS security and their actual understanding.

2.3.4 Survey Data Analysis

The quantitative data were analysed using various statistical methods. These included measures of central tendency including mean, median, and standard deviation, as well as frequency analysis to compare the response rates across various responses. Following this, a one-way between groups ANOVA was also conducted to compare the effect of role function on perceptions of the criticality of the 23 BACS vulnerabilities. Finally, a Pearson's chi-square test of contingencies was used to evaluate whether role function was related to the BACS architecture level at which each mitigation strategy was applied. The self-directed text data responses were then thematically analysed to enhance the quantitative analysis findings.

Extending from the project's primary questions, sub-questions were developed (Table 2.1) that aligned with sections of the survey. The analysed survey data facilitated a response to these questions and enabled a response to the primary research question.

Table 2.1
Stage 2 Sub-questions

	Project Stage 2 Sub-questions
1	Are security and building owner/operators professionals aware of the threat and risks associated with BACS?
2	What level of responsibility do security and builder owner/operator professionals have with BACS?
3	What is the degree of security systems integration into building automation systems?
4	What type of security systems integrate with building automation systems?
5	What do security and builder owner/operator professionals consider are the most critical building automation system vulnerabilities?
6	What security mitigation strategies do professionals generally apply to protect building automation systems?
7	What are the ideal security measures used by security and building owner/operator professionals for protecting building automation systems?

The Stage 2 survey data analysis and interpretations is presented in a following section (see Section 9 Stage 2 Survey of Understanding).

2.4 FOCUS GROUPS

The Stage 3 of the project used focus groups to further enhance both the Stage 2 findings and BACS Guideline.

2.4.1 Participants

Using a non-probability convenience sample, executive members from ASIS International, BOMA and SIA were sent requests to participate in the BACS focus groups. Each focus group was designated four to five participants, spread across the three participating associations. In addition, during a project presentation on the September 25, 2017, further volunteers were requested to participate to overcome issues of non-attendance.

The focus group participants (n=14) came from a broad range of practice areas, such as corporate security, information technology, public safety, consulting, building engineer, commercial real estate, fire and life safety, and crisis management. The participants' experience ranged from 5 to 35 years individually, with the highest held degree being a Masters (one only), with two degrees and the majority of (security) participants with the ASIS International CPP certification.

2.4.2 Materials

The focus groups used a semi-structured Questionnaire (Appendix H), sent to the volunteering participants a week prior to the sessions. In addition, a draft copy of the BACS Guideline was also supplied. The focus group questionnaire contained three discrete parts, with general participant information, focus group questions to review Stage 2 findings and a BACS Guideline critique questions.

2.4.3 Focus Group Procedure & Analysis

The research procedure involved email invitations to ASIS International, BOMA and SIA executive members, requesting participation in the focus group. Volunteering respondents were assigned a focus group, based on their association and practice area along with a designated time during the ASIS International Conference in Dallas, Texas, United States.

The focus group sessions were assigned a two hour period. At the commencement of the session, participants were briefed on the project, and provided an Information Letter and a Letter of Consent. At that point the focus groups were audio recorded, which commenced with an introduction from each participant. The focus group facilitators then asked the participants the questions from the focus group Questionnaire (Appendix H). The audio recordings were transcribed verbatim.

The transcripts were analyzed, primarily through participants' responses to the posed questions using content and thematic analysis techniques. This approach facilitated the extraction and listing of common themes from the participant's.

The Stage 3 focus groups data analysis and interpretations is presented in a following section (see Section 10 Stage 3 Focus Groups).

2.5 ETHICS

A number of ethical issues were considered to protect the project's participants in all project stages. It was a requirement that participation in the project be voluntary, that there was no published disclosure of identity, that a project overview was presented and that all participants must be at least 18 years of age and be willing participants. It was also highlighted that there was no penalty for refusing to participate and that participants could withdraw at any time once the project commenced.

The project met and was granted Edith Cowan University ethics approval (Appendix C).

For Stage 2 online survey, an invitation email containing the survey link was sent to perspective participants by the associations, stating that by progressing to the survey link that informed consent was given. For Stage 3 focus groups, participants were provided with a Letter of Consent (Appendix G), which gave a project overview and protection of identity assurance. All focus group participants signed the Letter of Consent.

2.6 LIMITATIONS

There were several limitations identified in the project.

The first and most significant limitation for the project related to semantics and definitional issues, which may have impacted on the interpretation of some survey questions. For example, differences in interpretation of the term *integration* between security and builder owner/operator professionals found in the results may stem from a lack of universal nomenclature. This limitations was highlighted in all stages of the project.

Sample sizes also provided some limitations in this project. The Stage 2 survey did not obtain an equal number of respondents in each job function category, and the expert group was limited to 10 respondents. In addition, survey logic resulted in different sample sizes for different questions, and this limitation should be noted when generalising findings. Stage 3 focus groups initially targeted between four and six participant per session, but achieved between three and four participants (Av 3.5).

Finally, during Stage 2 no clear conclusion of what security mitigation strategies professionals apply could be extracted from the data, nor determine the ideal security measures used by security and building owner/operator professionals. These issues were largely due to the homogenous rating of mitigation strategies, which may have been facilitated by the design of the mitigation question. The question asked the respondent whether they apply a particular mitigation strategy, but in their response, allowed them to select one or more BACS architecture level (or alternately, select 'Don't know', although no responded did this). This approach may have given the impression that the question was asking the respondent to list the levels at which they believed the mitigation strategy *should* be applied.

Although this may be a limitation of the project and may have influenced more homogeneous ratings of mitigation strategies, it is also interesting that no respondent used the 'Don't know' option. Nevertheless, this issue was overcome during the Stage 3 focus groups, where the participants were able to interact with greater depth and afforded clarity prior to their responses and were consequently positive towards the draft BCS Guideline questions. In addition, the factor of threat and context (or situation) has to be considered. Without understanding either the context and/or threat to a BACS and its facility, aligning mitigations strategies becomes problematic.

2.7 CONCLUSION

The process of ensuring that the project delivered robust and evidence based findings was vital. Such an outcome could only have been achieved through taking a robust mixed methods research methodology. This approach considered the project process, its instruments, sampling of the populations, data and its analysis, and necessary ethical considerations. The ability to ensure both validity and reliability of the findings could only be achieved by such a structured and staged research driven process, allowing the following sections to proceed.

Section 3: What Is BACS?

3.1 INTRODUCTION

Building Automation and Control Systems (BACS) and later, Intelligent Building systems, developed over an extended period of time, increasing in use and converging as technologies developed and were applied. This section introduces the premise of BACS, commencing with a review of the available literature. The industry in which BACS operate is dynamic in nature; consequently, it is necessary to identify popular terms to provide context. The following sections explore the many types of BACS, denoting IB systems. The aim is to provide a robust and corroborated categorization of BACS to support current understanding.

3.2 BACS: DENOTING COMMON TERMS

The Building Automation and Control System (BACS) and Intelligent Building (IB) developed from earlier rudimentary automation, evolving into the current systems of today, with their likely future being embedded within the Internet of Things (IoT). The following section provides an overview of the many types of BACS.

3.2.1 Automation

Defining automation is the starting point when considering the development of the modern day BACS. Automation, in its most basic form, can be sourced back several hundred years to the development of machines in the industrial age (Autor, 2015), from early textiles machines through to modern day micro level digitization. The human drive for efficiency dictated the development of new and more pervasive automation technologies.

The concept of automation developed for the modern age to mean “the execution by a machine agent (usually a computer) of a function that was previously carried out by a human” (Parasuraman & Riley, 1997). The Oxford English Dictionary defines automation as the “use or introduction of automatic equipment in a manufacturing or other process or facility” (Simpson & Weiner, 1989). Automation is the drive for ever more cost effective, efficient and reliable solutions through the gradual removal of the “weak link” or ongoing expensive element from the process; that of the human. It is widely acknowledged that in repetitive processes the digital or mechanical alternative to human labor is cheaper, more responsive, consistent and less prone to error (Sall, 2017).

Given the attributes of automation, there has been a move from the exclusive focus of manufacturing or process to include broader facets of everyday life and within all parts of the built environment. In contemporary times, the automation of things is thoroughly embedded within our society. Our drive to make life easier, faster and cheaper results in the automation of everyday items. Such items include automated garage doors, home lighting timers that switch lights on at defined times to give the illusion of presence, to automated washing machines designed to take economic advantage of lower cost electricity. To varying degrees, automation is now everywhere in the daily lives of people.

3.2.2 Building Automation Systems

The next stage in the quest for automation was the advent of Building Automation System (BAS). Often treated as an interchangeable name for a Building Management System (BMS), the distinction is slight but nonetheless important.

A Building Automation System (BAS) is where facility services, such as utilities, communicate with each other to exchange digital, analogue or other forms of information, potentially to a central control point. Facility services are utilities and installations that are supplied and distributed within a facility, which may include electricity, gas, heating, cooling, water and communications (International Organization for Standardization, 2004, p. 6). The advance in communication came with software controlled connectivity to control many devices. To facilitate such control, computers and controllers in the BAS can be networked to the Internet or serve as a standalone system for the local peer to peer controller network only. In addition, the BAS Controllers have their own internal processors, so they do not need a central computer to process the control functions (High Performance HVAC, 2017).

BAS is described as a "subset of the management and control system and can be part of a larger BMS [or BACS]" (Control Solutions Inc., 2015). In contrast to BAS, BMS or BACS extends beyond plant and equipment monitoring and control, incorporating the functionality of management. BAS integration may range from small systems where facility lighting is timer controlled to a facility with thousands of automated processes linked to a centralized computer, yet sub-systems can independently carry on according to their programmed functions. Indeed, a facility may have several independent BASs in place; examples being an HVAC system designed to cool a room based on ambient temperature, and a totally separate central surveillance system with movement and heat sensors, again set up and controlled locally but with the potential to be networked.

BAS have advanced from the pneumatic controls of the 1950s through the advent of digitalization and microprocessor control in the 1980s to the present, with remote control of systems through wireless technology (Control Solutions Inc., 2015) and common communication protocols.

A Building Automation System may be denoted as:

> An automated system where building services, such as utilities, communicate with each other to exchange digital, analogue or other forms of information, potentially to a central control point.

2.2.3 Building Automation and Control System

Given the organic and context driven developmental nature of the building automation industry, there exist a number of nuanced names and resulting definitions. Depending on the scale of the system—from a small residential home to a high-rise facility—a BACS may be known in the industry as a Facilities Management System (FMS), Building Automation System (BAS), Building Management System (BMS), an Intelligent Building (IB) or a Building Energy Management System (BEMS). This list is not exhaustive, because the scope and focus of the individual system dictates its label.

Building Automation and Control Systems (BACS) are known by many terms, such as a Facilities Management System (FMS), Building Automation System (BAS), Building Automation and Control System (BACS), an Intelligent Building (IB) or a Building Energy Management System (BEMS).

At its core, the principle of a BACS remains the same. Due to the automation of systems within facilities, the development of a central control has been necessary to ensure smooth and efficient cohesion between all automated sub-systems. A BACS could be considered a system that converges at a central point to integrate technology and processes to create a facility that is safer, more comfortable and productive for its occupants, and more operationally efficient for its owners and operators.

Smaller scale examples of a BACS include residential home automation systems providing control for services such as automated heating, lighting and audio visual systems. At its most basic level, a BMS consists of software, a server with a database and sensors connected to a network. This falls under the same broad definition, even though the scale is entirely different, to a commercial or industrial BACS.

At the other end of the scale, a BACS can integrate multiple facility services and their sub-systems beyond utilities, such as elevators, lighting, fire and life safety, emergency warning and intercommunication (EWIS), and security systems. The BMS is designed to operate automatically, with restricted human intervention. The ability to monitor and manage a wide range of facility service systems across multiple protocols and platforms can provide the facilities team with a single shared view of the operations within a facility, and more importantly, control.

By 2002, the concept of modern integrated BACS were beginning to receive widespread acceptance in the facility and real estate marketplace, and were generically defined as a "computer-based control building automation systems predominate in most commercial and industrial buildings, reducing energy costs while improving system performance, operability and reliability" (Langston & Lauge-Kristensen, 2002, p. 75).

A Building Automation and Control System (BACS) may be denoted as:

> An automated system, where building services and processes, communicate with each other to exchange digital, analogue or other forms of information, to a central control point.

3.2.3 Intelligent Building (or Smart Building)

The next level of building automation and integration is becoming known as an Intelligent Building (IB) system. While the term IB has been used in the industry since the early 1980s, a standard industry wide accepted definition does not exist. Nevertheless one of the earliest definitions of IB comes from the European Intelligent Buildings Institute, which described it as being one that "creates a new environment which maximizes the effectiveness of the facility occupants while at the same time enabling efficient management of resources with minimum life-time costs of hardware and facilities" (cited in Sherbini & Krawczyk, 2004, p. 137). The focus on facility services in a BACS moves in IB to the needs of the occupants.

The Asian Institute of Intelligent Buildings (AIIB) extends this explanation, adopting a definition for IB as the inclusion of nine functions, being environmental friendliness, space management, human comfort, working efficacy, culture, image of high technology, safety and security, construction and structure process and finally, life cycle cost. These elements resulted in a definition that:

> An Intelligent Building is designed and constructed on an appropriate selection of quality environment modules to meet the users' requirements by mapping with the appropriate facilities to achieve long-term building value. (So & Wong, 2002, pp. 288-289)

The evident shift in the IB industry was felt in the late 1990s, with the increasing focus on energy efficiency and sustainability. For example, the term "Bright Green Buildings" was introduced to indicate that a facility was both environmentally friendly and intelligent in its output, with sustainability at its core (Frost & Sullivan, 2008).

According to Smart Accelerate (n.d), an Intelligent Building is one that incorporates available concepts, materials, systems and technologies, and by integrating these, meets or exceeds the performance requirements of the facility stakeholders including the owners, managers, occupants and users. Therefore, the facility's environment should be productive, safe, healthy, and thermally, aurally and visually comfortable. These can be achieved through optimizing a facility's four basic components, namely its structure, systems, services and management. However, these views do not provide an explicit definition of IB.

To address the ever broader technical and business functions in defining IB, Kujuro (1990) summarized that an IB comprises of three key elements:

a. Highly sophisticated office automation functions relying on a facility LAN and augmented by diverse office automation equipment

b. Advanced communications capabilities achieved through effective introduction of digital technologies

c. Sophisticated building automation capabilities realised through effective integration of facility management, security and energy saving systems (Kujuro, 1990)

There is no standard consensual definition of what constitutes an IB; however, most explanations have several things in common:

a. Integrates disparate facility service systems so they can be controlled by a single and centralized common user interface

b. Maximizes facility performance and efficiency by integrating facility service systems such as lighting, HVAC, safety, power management, security, etc.

c. Uses a shared network for all facility-system communications

d. Provides significant benefits to facility owners, property and facility management professionals, and its users.

e. Uses technology and strategies that add long-term, sustainable value to the property

An Intelligent Building system may be denoted as:

> An automated system where building services and corporate processes, communicate with each other to exchange digital, analogue or other forms of information, to a central control point to manage the environment.

3.2.4 Internet of Things (IoT) and Building Internet of Things (BIoT)

In more recent years, the "Internet of Things" has had to be considered. Morgan defines the IoT as "the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other)" (2014, p. 1). The list of everyday items that can be connected to the Internet is limitless; through the IoT it is possible to remotely and wirelessly control washing machines, switch on or off air conditioning, record television programs while abroad and programme the coffee pot for our arrival home from work. Such connectivity also applies to the non-domestic world. The basic premise to the IoT is that anything that can be connected to the Internet, will be connected (Hosain, 2016).

As a relatively recent phenomenon, the IoT is highly relevant to the IB discussion as a system that connects all "things". At the core of the IB is the concept of connectivity and central control by the individual, through various physical electronics or engineering methods. The IoT provides the same capability of connectivity, but uses the Internet or wifi connectivity (Young, 2014). The result is the ability to move away from the use of a dedicated network and protocols, which is a more efficient and less costly means of delivering building automation.

The IoT is already having an impact on building automation, with the convergence of the IoT and IB. For example, Young defined the Building IoT (BIoT) as "the overlaying of an Internet Protocal (IP) network, connecting all the facility services monitoring, analyzing and controlling without the intervention of humans" (2014, p. 1). There are already cloud and application based solutions using IoT, such as BuildingIQ, SkyFoundary, Mios, which provide functionality not previously available (BSRIA Institution, 2015).

Facility professionals are concerned with improved efficiency and reduced costs that can be achieved by the IB. However, the age of the Internet has brought about a level of cheaper and easier connectivity that takes building automation into a different realm. It is predicted that the traditional building automation will transform itself over the next technological generation into a BIoT (BSRIA Institution, 2015; Young, 2014).

3.3 BACS: A DEVELOPMENTAL HISTORY

As the above discussions have highlighted, the development of Building Automation and Control System (BACS) is the drive for faster, more efficient and more stress-free ways of conducting business. With time and the development of technologies, there have always been improving methods to automate and integrate almost all areas of industry, business, and, indeed, personal lives.

Unlike automation, which originates in the early industrial era, BACS has roots in the 1970s industrial sector, from the systems and controls used to automate production processes and to optimize plant performances. The concepts and applications were then adapted, developed and modularized during the 1980s, supported by more powerful and cheaper microprocessors, enabling transferability of the technology and systems to the residential and commercial sectors.

BACS systems developed alongside other facility service systems, such as energy management and process control. However today, energy and sustainability systems are integrated and integral to BACS, and not seen as separate systems. Such a view is likely to increase in the future, as are other facility functions; whereas, process control systems remain primarily a domain of production and factory control. Both energy management systems and process control systems are discussed in greater detail.

3.3.1 Energy Management Systems

The history of energy management systems (EMS) started after World War II, when a need to monitor the growing number of pneumatic controls and electrical switches arose (Chan & So, 1999). It soon became apparent that servicing a great number of panels mounted near equipment controlled areas was expensive and centralization became one of the key topics.

In the 1950s, engineers introduced the first generation pneumatic sensor transmitters that allowed remote monitoring and local adjustment from the pneumatic controller. Pneumatic controllers functioned by varying the amount of compressed air powering a device attached to that unit (Nardone, 1999). The system consists of air chambers, springs, linkages, orifices, diaphragms, nozzles and internal valves to regulate air pressures. According to Nardone (1999), centralizing these controllers resulted in lots of pneumatic tubing and a large display board with gauges and control switches. An operator monitored these gauges and when abnormal values were detected, a mechanic could be sent to the endpoint to resolve the problem. While pneumatic controls were primarily used at the beginning of the 1950s, electric and electronic controls were increasingly introduced towards the end of the decade. The commencement of electric and electronic controls marked the second generation of energy management systems (Panke, 2001).

The third generation, in the 1960s, used electromechanical multiplexing systems (Chan & So, 1999). Controllers were aggregated in local system panels, directly wired to a central console (Panke, 2001). This EMS technology decreased the response times, because scanning was done electronically, and lowered installation and maintenance costs. The greatest drawback of this type of system was the dependency on the central processor. An error in the central processor led to a whole system blackout.

Parallel to the electromechanical evolution, minicomputers and Programmable Logic Controllers (PLCs) were improved and adapted to the requirements of control systems. Due to the high energy costs during the 1970s oil crisis the need for energy saving systems became more crucial. Increasing computerized systems improved and optimized the control of system elements. In addition, fire and life safety systems from the emerging market of BACS were integrated into the already existing EMS.

Due to lower hardware costs and improved microprocessing capacity in the 1980s, microcontroller based control panels replaced the conventional pneumatic control systems. Therefore, remote panels became increasingly smarter and could carry out most of the functions that had formerly been controlled centrally. These remote intelligent nodes were connected with the central console by a proprietary Local Area Network (LAN).

Around the 1980s, the current generation introduced the concept of Direct Digital Control (DDC) and used small programmable microprocessors on remote nodes, controlled centrally by a Personal Computer (PC) (McGowan, 1995). The distributed intelligence in the field nodes led to improved speed of response and increased system reliability. In addition, it was possible to monitor the EMS from multiple remote locations. Therefore, besides on-site operators, energy managers, manufacturers and facility operators could access the data. Furthermore, the usage of software-based controllers made it possible to change system operation without changing the underlying hardware.

3.3.2 Process Control Systems

Process Control Systems (PCS) are used to monitor and control processes in industrial plant and equipment to a centralized location, using a defined communications standard (language). The centralized location became the operators console, a human-machine interface (HMI) to monitor the values of the Remote Terminal Units (RTUs) that were regularly polled by the central host processor. However, due to the lack of common communication standards, proprietary systems were extensively used and this resulted in systems that could not communicate with each other (Shaw, 2006).

During the 1970s microcontrollers were introduced, where simple process steps could be programmed into these controllers. Mainframe computers were used as a central host computer to poll the remote controllers. To poll is a communication process in which the computer or controller interrogates the status of its connected external devices on a communication line to find whether it has data to transmit (Takagi, 1991, p. 193) or receive. A disadvantage of the centralization process was the increasing risk of a failure in the central systems, leading to a system blackout. However, low-cost 8-bit and 16-bit microprocessors slowly replaced the conventional Remote Terminal Units and provided the first so-called smart remotes.

In the 1980s more decentralized systems were introduced with intelligent field nodes that were connected to the central console by a bus system. Local Area Network (LAN) technologies and Ethernet found its way into PCS. Redundant dedicated front-end processors were used to poll the

RTUs, while more advanced systems performed special application and backup tasks. This approach reduced costs in contrast to pure mainframe applications and improved system reliability. Such technology development led to the Supervisory Control and Data Acquisition (SCADA) systems.

Due to the broad acceptance of PCs and decreasing hardware costs in the 1990s, overall costs for PCSs decreased. PCSs were comparable to corporate IT networks and the client server concept evolved into SCADA systems. Past monolithic programs were rewritten and new programs distributed to dedicated computers. Another step was the introduction of a set of communication standards for data exchange, for example the Object Linking and Embedding for Process Control (OPC). In terms of cutting costs and creating a standardized environment, the evolution of LANs, WANs, TCP/IP networking, communication standards and protocols, and Ethernet resulted.

3.4 THE MODERN BACS

Building Automation and Control System (BACS) evolved from the merging of different areas of automation, for example EMS and PCS. Integrating these systems into one Distributed Control System (DCS) for facility's takes advantage of both systems in managing the challenges in modern ' management. BACS systems are technically focused and can be integrated into facility management that joins BMS and Maintenance Management Systems (MMS), focused on work scheduling, maintenance planning, inventory control and accounting (Boed, 1999).

Modern BACS automates, controls and manages the services, environment and business functions within a facility. Facility services include utilities and its subsystems such as Heating, Ventilation and Air-Conditioning (HVAC), lighting, blinds, elevators, life safety (such as fire detection, fire suppression, emergency warning and intercom), and security (such as intruder alarm systems and CCTV) into one integrated facility communication system. Many manufacturers, using common connectivity protocols like Bacnet and LonWorks, offer "plug and play" products for managing or controlling end nodes, specifically taking advantage of common language standards. Furthermore, the modern IB is now connected to existing enterprise management software such as SAP or OpenView.

3.5 CONCLUSION

Building Automation and Control Systems (BACS) and later, Intelligent Buildings, developed over an extended period of time as demand required more cost effective facilities and improved information flow across the business. BACS developed from industry control systems, to what is today a computerized control and monitoring system embedded into a facility. Today, facility automation systems may be known by many terms such as a BACS, Intelligent Building or Smart Building, and more recently, Smart Cities. The industry in which building automation operate is dynamic; consequently, these terms are at times interchangeable, as there are no single consensus that defines these systems, whether a BACS, Intelligent Building or Smart Building.

Section 4: BACS Fundamentals

4.1 INTRODUCTION

Building Automation and Control Systems (BACS) are modular in nature, formed from the integration of a number of devices connected and communicating on a common platform. Therefore, this section provides an overview of BACS, based on three levels of architecture. The aim of this section is to provide the basic technical background and understanding of BACS hardware, software and communication techniques to understanding their vulnerabilities.

4.2 THE FUNDAMENTALS OF A BUILDING AUTOMATION SYSTEM

Building Automation and Control Systems (BACS) architecture is based on three levels, considered the 1) Management level, 2) Automation level and 3) Field level. However, in contrast to this model some consider there to be a fourth level labelled Service. In general, the Management level contains the human interface (workstation), server and routing devices, all connected via an appropriate communication medium. The Automation level provides the various primary control technology devices and secondary facility automation, connected via networked controllers and operating via BACnet, LonWorks, etc. communication protocols. The Field level includes devices connected to specific plant and equipment sensor or activators. The Service level generally embodies remote access connectivity for service and maintenance use. The following sections present a general discussion for each level, providing a deeper understanding of these devices and their interrelationship.

4.2.1 Automation Control System Basics

A simple control system consists of three component functions and associated parts: a sensor providing input function, a controller providing decision functions and a controlled device providing a defined system output function (Figure 4.1). The sensor [S] measures a variable, for example the controlled medium of temperature in the duct, and sends that information to the controller [C]. Dependent on configuration, the controller calculates the necessary output value to adjust the controlled device [CD]. Adjusting the controlled device alters the amount of heated water supply and ultimately, the duct temperature at the sensor.

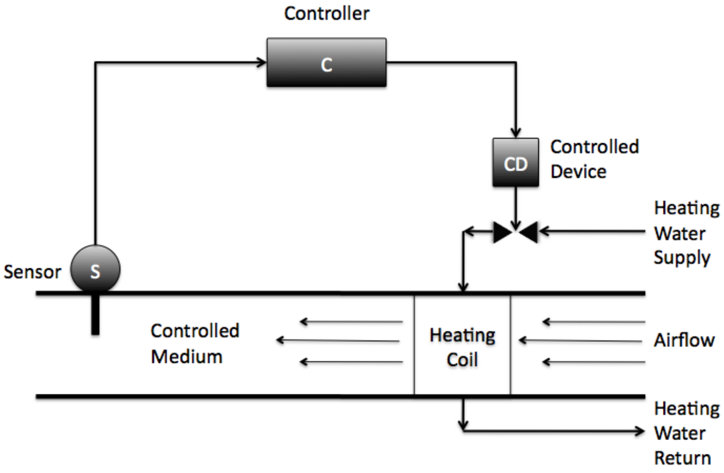


Figure 4.1. Control system

(CIBSE, 2000)

There are two general types of control systems: open-loop and closed-loop control. A closed loop operating modality is closed because the effect of the control system device is used as input for the sensor. Figure 4.2 shows how the temperature detected in the room is used as a continuous input for the processing controller, which compares against preset functions to adjust the heating output through a radiator. In other words, a control system where the "output acts upon the process in such a way as to reduce the difference between the measured value and the desired set-point" (International Organization for Standardization, 2004, p. 7).

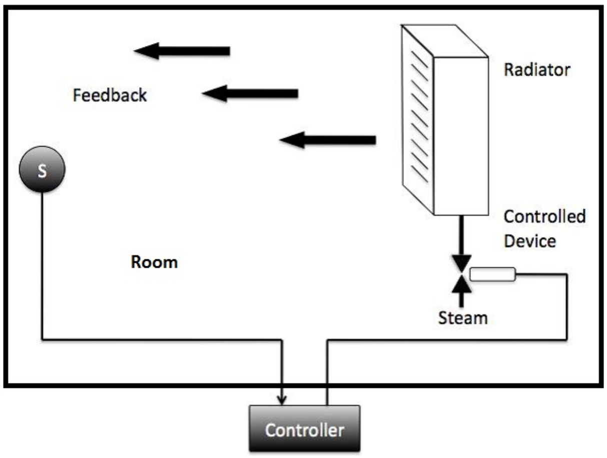


Figure 4.2. Closed loop control

(Adjusted from CIBSE, 2000)

In contrast, open-loop circuits embody a system where the sensor measures a completely independent variable. In other words, a control system where "one or more measured inputs controls the output without any influence from the process" (International Organization for Standardization, 2004, p. 20). For example, Figure 4.3 shows that the measurement of the temperature that occurs outside the building and controls the internal radiator.

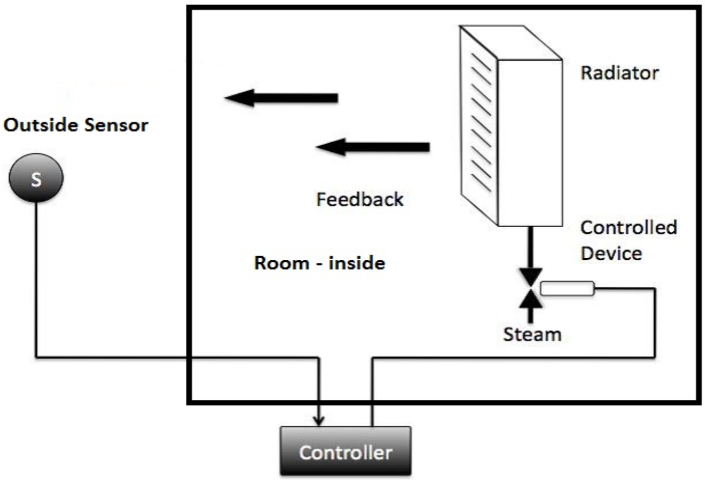


Figure 4.3. Open-loop Circuit

(Adjusted from CIBSE, 2000)

4.2.2 Automation Control Logic

Two formats of information or logic are used to exchange or inputs into automation, digital and analogueue data. Digital (binary) information communicates through two distinct states, namely on [logic 1] or off [logic 0]. For example, this is used to monitor whether an engine is running or not. In contrast, analogueue information is represented as a floating value, for example from 0 to 5 volts, and is used to measure continuously changing or modulating environments.

In earlier automation systems, the controller logic was hard-wired and more representative of analogueue technologies, whereas current systems use software to calculate values and is digital in nature. However, some basic types of building automation controllers can still be distinguished: two-position, floating, proportional, proportional plus integral and proportional plus integral plus derivative (PID) controllers.

The two-position control, also known as digital or on/off control, defines a set-point and a differential value to this set-point. The controlled device is switched to on when it reaches the set-point and switched to off when it leaves the differential area to the set-point. In Figure 4.4, a radiator is activated when reaching 20 degrees and turns off again when reaching 23 degrees.

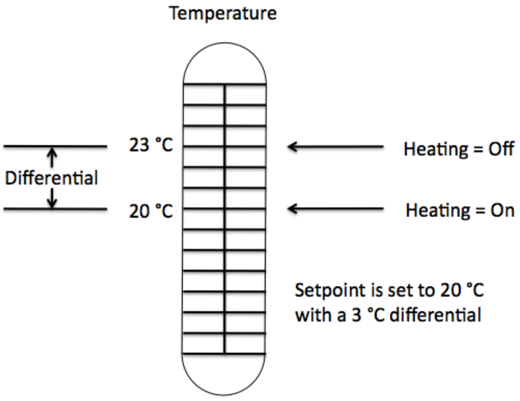


Figure 4.4. Two-position Control Configuration

(DDC Online, n/a)

Floating control is a type of two-position control and defines three states: increasing, decreasing or off. An example is a controlled device such as a valve for mixing hot with cold water. When the water is too hot, the controller signals to close the valve and stops when the valve reaches its mid-position.

Proportional controllers adjust the output proportional to the input signal, used for example, to correct deviation to the defined set-point. The output signal is proportional to the difference of the set-point and is off when the set-point is reached. When an integral is added to the proportional controller the divergence to the set-point is integrated over time. Hence, the proportional plus integral (PI) controller combines the advantages of proportional control and integration, and is; therefore, one of the most widely used controls in HVAC (CIBSE, 2000). A proportional plus integral and proportional plus integral plus derivative (PID) control adds derivation to the calculation of outputs. For example, when controlling a valve, the speed of closing or opening the valve is dependent on how large the difference between the measured value and the set-point are.

4.3 BACS HARDWARE ARCHITECTURE

The European Committee for Standardization (CIBSE, 2000), in their International Standard for Building Automation (2004), divides building automation architecture and communications into three distinct layers or levels of Management, Automation and Field devices (Figure 4.5). The advantage of such architecture is that there is a clear separation of duties and a reduction of network traffic in the management level; however, for smaller systems a separation of networks can be expensive.

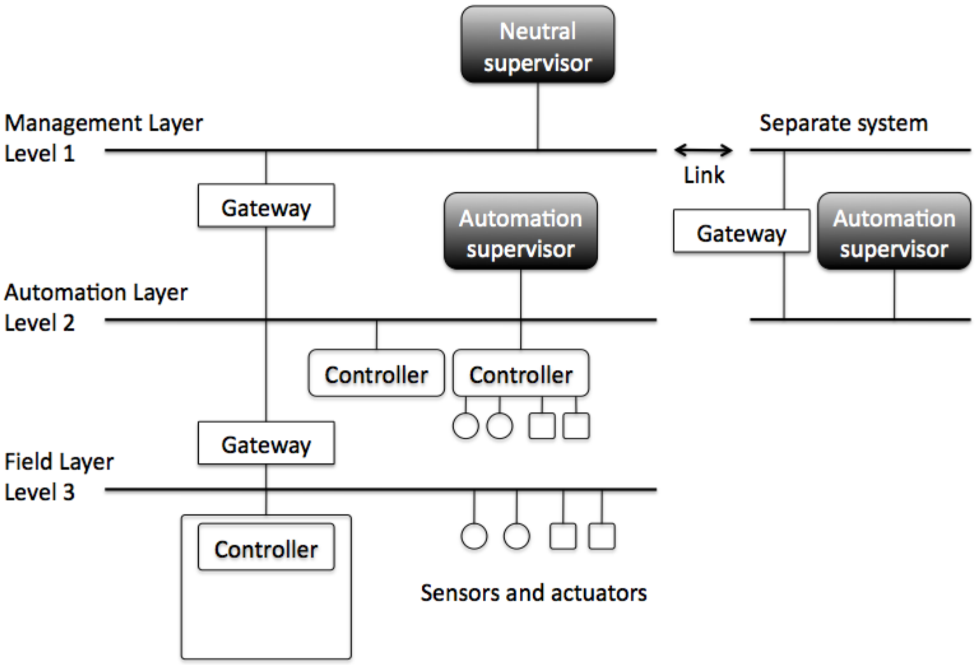


Figure 4.5. Three-layer BACS Architecture

The Management Level

The Management level is generally the company's Information Technology and Communications (ITC) network.

The Management level comprises "operator stations, monitoring and operator units, programming units and other peripheral computer devices connected to a data processing device i.e., a server" (International Organization for Standardization, 2004, p. 53) to support the information exchange monitoring and management of the automation system. For example, a personal workstation that has dedicated automation software installed. Several autonomous systems can be connected to support the human interface for monitoring and management purposes.

The Automation Level

The Automation level is generally a dedicated communications network for the sole purpose of building device connectivity, communication and control (automation).

The Automation level comprises "control devices and monitoring and operator units, programming units, operator stations or panels and/or programming units connected to a data processing device i.e., a server" (International Organization for Standardization, 2004, p. 53). This level is associated with controllers that serve main plant, such as the air handling units, chillers and boiler units, etc.

The Field Level

The Field level comprises devices that are generally self-contained physical units.

Field level devices are connected to automation level controllers, either application specific or generic controllers. Application specific controllers operate using communications protocols such as M-bus or other proprietary protocols.

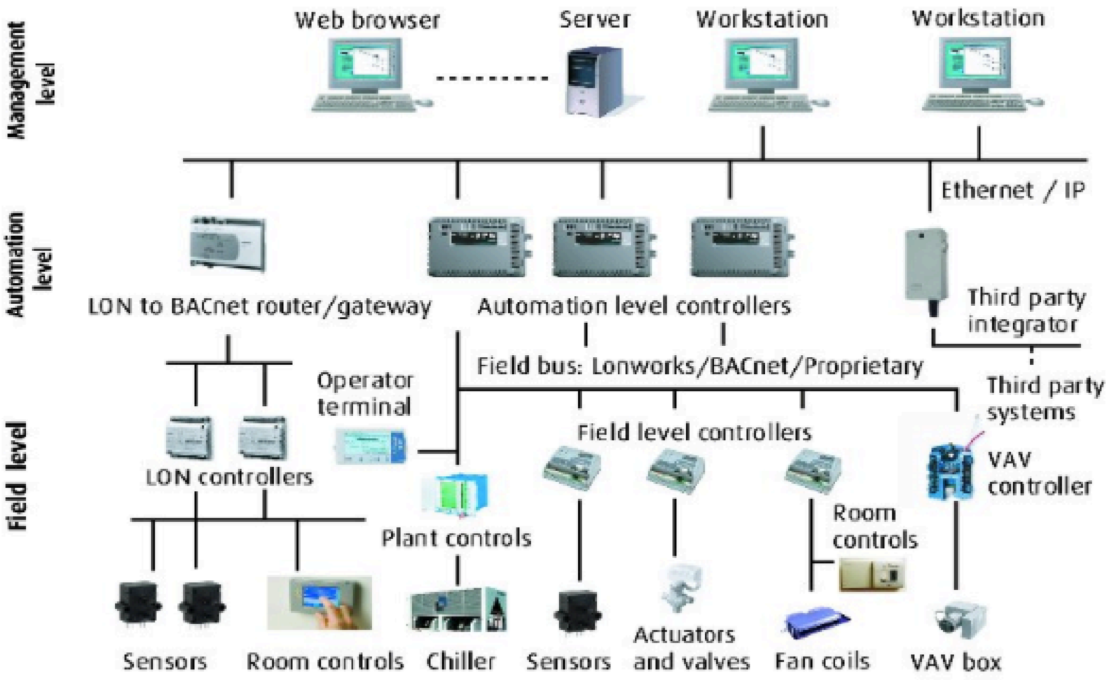


Figure 4.6. Illustration of BACS Three-layer Architecture

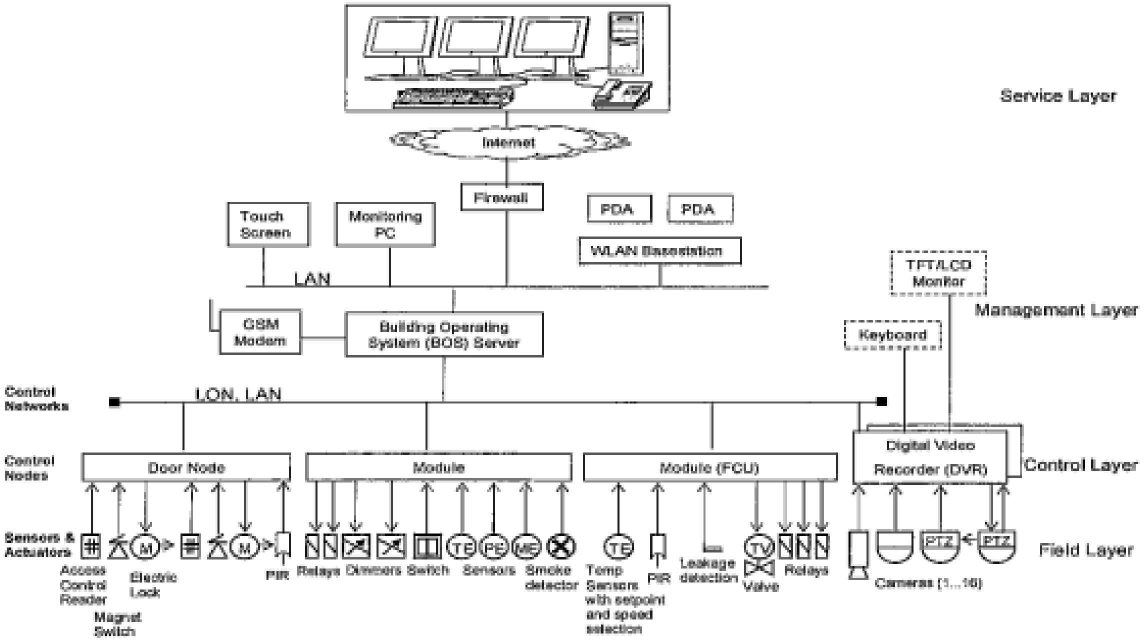


Figure 4.7. Typical BACS, with security functionality (Lonix Building Connectivity, n.d., p. 26)

4.4 BACS SOFTWARE ARCHITECTURE

As with BACS hardware, the International Standard for Building Automation (2004) divides its software architecture and communication networks into three distinct levels of Management, Automation and Field (see Figure 4.5). The following sections provide a background and overview of the more commonly used automation protocols, such as BACnet and LonWorks.

4.4.1 BACS Industry Standards and Protocols

For BACS to function, there is a requirement for connectivity and common language communication. Connectivity is achieved through via various communication networks that link and integrate the many discrete devices. Communication is achieved through standardized logic code. Such a requirement has led to a number of building automation network and communication protocols (Table 4.1) being established.

Table 4.1

BACS Industry Standards and Protocols

Standards and Protocols		
BACnet	KNX	OpenTherm
C-Bus	LonTalk	OpenWebNet
CEBus	LonWorks	S-Bus
CIBSE[1]	M-Bus	VSCP
DALI	Midac	WebService
DSI	Modbus	X10
Dynet	oBIX	ZigBee
EnOcean	OPC	

Note: CIBSE (Chartered Institute of Building Services Engineers)

The more applicable and current standards of automation operating protocols can be further defined with their key attributes (Table 4.2).

Table 4.2

BACS Key Industry Standards and Protocols Attributes

BACS Standard	Attributes
BACnet	American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) standard, modelled on the Open Systems Interconnection (OSI) reference that shields BACnet from obsolesce with respect to networking. Adopted worldwide as ISO 16484-5:2003
CAN	Developed by Bosch for the automotive industry
CEBus	Electronics Industry Association (EIA) standard, covers devices that communicate through mains power cabling, low voltage twisted pair, coaxial cable, infrared, RF and fiber optics
DALI	Digital Addressable Lighting Interface. Network-based systems that control lighting in buildings
Dynet	Dynalite network and protocol
EHSA	European Home Systems Association (EHSA) allows connection to a network using any collection of media and therefore supports an open systems
EnOcean	Battery-less, interoperable and wireless standard
KNX	System for local device control
LonTalk	Part of the LonWorks platform. Created by Echelon Corporation for networking devices. ISO standard numbers for building automation worldwide are ISO/IEC 14908-1, ISO/IEC 14908-2, ISO/IEC 14908-3, and ISO/IEC 14908-4
LonWorks	Local Operating NetWork that was designed for automation control. A worldwide standard that includes a communication media similar to CEBus. Focus of LonWorks is the "Neuron" chip, which acts as the network node and communication protocol
NEST	Novell Embedded Systems Technology, aimed to be used everywhere for devices in offices, homes, cars, etc
OPC	Standard used widely in manufacturing, process control, and building automation. The open standard transfers, values, historical data, and alarms and events
S-Bus	Smart-BUS, SBUS, an open protocol, open source
X10	Oldest available technology, allowing limited control of devices via power reticulation
ZigBee	Short range, low-powered wireless communication standard

(Adjusted from Schneider Electric, 2015; Sharples, Callaghan, & Clarke, 1999, p. 136)

4.4.2 BACS Operating Protocols

The more commonly applied BACS automation protocols include BACnet, LonWoks, KNX and Modbus. However, application, region and the market dictates which protocol is more likely used.

BACnet

The ASHRAE BACnet (Building Automation and Control Networks) protocol was developed specifically to address the needs of building automation and control systems in various capacities. Created in 1987 at Cornell University, it became an ANSI standard under the auspices of the American Society of Heating, Refrigerating and Air Conditioning Engineers (ASHRAE) (Schneider Electric, 2015, p. 7). BACnet was modeled on the Open Systems Interconnection (OSI) reference model.

The focus of BACnet was to ensure a high level of inter-operability in an environment that involved many vendors and multiple types of building plant, equipment and systems. In 1995, BACnet became ASHRAE1/ANSI2 Standard 135 and was published as International Standard ISO

3/IEC416484-5:2003. Since January 2006, BACnet International is the official initiative for promoting and developing BACnet.

LonWorks

Local Operating NetWork (LonWorks) is a widely used standard for many types of automation and control applications. It was created by the manufacturer Echelon around 1989, and in 1999 it was accepted as a standard by ANSI for control networking (ANSI/CEA-709.1-B) (Schneider Electric, 2015, p. 8). Echelon had the goal to design a microprocessor that possessed a standardized communications interface, where each device was able to “talk and work” with every other device, regardless of manufacturer and to carry out its specific task as decentralized intelligence within a network (TROX GmbH, n.d.). LonWorks is part of the BACnet MAC layer.

In 2008, the Joint Technical Committee (JTC 1) of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) formally approved LonWorks control networking technology as ISO/IEC 14908, Parts 1, 2, 3, and 4 (LonMark International, 2017).

KNX

KNX is a worldwide communication standard for home and building control, using OSI-based (Open Systems Interconnection) network communications protocol. The protocol was created in 1999 by Konnex Association (now KNX Association). It is a combination of three previous standards, namely the European Home Systems Protocol (EHS), BatiBUS and European Installation Bus (EIB or Instabus). KNX has been standardized through EN 50090 and ISO/IEC 14543).

Modbus

Modbus is a serial communications protocol, developed in 1979 by Modicon (now Schneider Electric). Originally created as part of the programmable logic controllers (PLCs) market, it was released as an open protocol in 2004.

The Modbus protocol uses a client/server architecture to manage communication between a host and device. In building automation, it is used to control equipment such as chillers, boilers and fans. The protocol continues to be used at the application device level because it is easy to understand, is an open system and can be used royalty-free. However, Modbus is not restricted to just building automation, and can be found in numerous diverse automation industries including industrial control automation.

4.4.3 BACS Architecture of Operating Protocols

The many types of protocols provide connectivity at the various BACS automation levels. As with its hardware, automation protocols can be divided into levels (Figure 4.8), although typically software straddles levels.

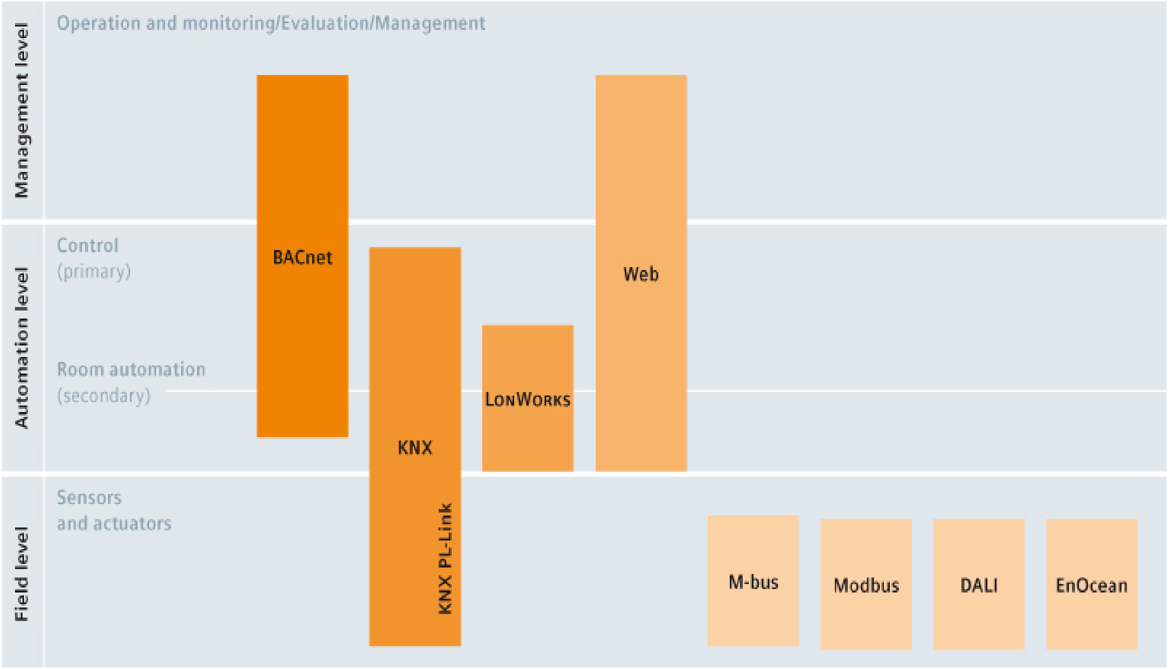


Figure 4.8. BACS Software Architecture (Siemens, 2017)

In general, the Management level contains the human interface (workstations), server and routing devices, all connected via an appropriate communication medium such as LAN/WAN using TCP/IP/BACnet. The Automation level provides the various primary control and secondary room automation, connected via networked controllers using twisted pair cables and operating BACnet, LonWorks or KNX. Finally, at the Field level, devices are connected to specific plant and equipment sensor or activators operating M-bus, KNX or their own proprietary protocol.

4.5 AUTOMATION LEVEL DEVICES

In this section, BACS automation levels are discussed to provide an oversight of the typical parts within the automation architecture. Typical physical devices for the levels of Management, Automation and Field are discussed.

4.5.1 Field Level Devices

Field level devices are physical equipment that connects the BACS to its physical environment, providing the system with information and the means to adjust the building environment. These are generally self-contained physical units, either as actuators or sensors. Typical field devices are light switches, PIRs, fan motors, air volume boxes, temperature sensors, etc.

Actuators

Actuators allow control of plant process, and operate electrically, pneumatically or hydraulically, to influence the flow of mass or energy (International Organization for Standardization, 2004, p. 3). They are typically motorized electromechanical devices for the control of valves or dampers.

A typical actuator is the Schneider Electric TAC M310, which is an electromechanical actuator for the control of two-way and three-way plug valves for hot water, heating and air handling systems (Schneider Electric TAC, 2004, p. 112). This device is controlled by either an increase/decrease signal or by a modulating 0 to 10V control signal.

Sensors

A sensor is a device or instrument designed to detect or measure a variable. Typical sensors may be a switch (binary), thermostat (binary) or temperature gauge (analogueue) (International Organization for Standardization, 2004, p. 25). For example, a typical sensor is an electronic average transmitter that converts data from four duct air temperature sensors into one averaged signal (Schneider Electric TAC, 2004, p. 126).

4.5.2 Automation Level Devices

The Automation level devices generally comprise Controllers that provides an interface between the system's field and management levels, and which contain some distributed decision intelligence. Controllers are typically designed to provide either specific application functionality or generic functionality, although most provide a degree of both (multi-functionality).

Controllers are generally compact, DIN mounted, may be used in standalone or in network mode and are freely programmable. They include inputs and outputs, from 6 to 40 inputs/outputs (Table 4.3). Controllers may be programmed for defined functions using the management level's workstation, by a directly connected laptop or locally connected handheld programmer. In addition, some may be expanded using input/output expansion modules.

Table 4.3

Typical Controller Inputs and Outputs

Type of Input / Output	Typ. number
Digital Inputs	2-4
Thermistor Inputs	2-4
Universal Inputs	4
Analogueue Outputs	3
Digital Outputs (Relay)	3-6
Digital Outputs (Triac)	0-6

Typical operating parameters (Table 4.4) are similar across most manufacturers.

Table 4.4

Typical Controller Operating Parameters

Input / Output	Requirements
Operating voltage	24 V AC/DC ±20%, 50/60 Hz
Power consumption	Max. 5 W
Operating temperature	0 to +50°C
Data backup in event of power failure	72 h RAM-Backup
Dimensions incl. base	180mm x 110mm x 77.4 mm
Transceiver Protocol	FTT-10, LonTalk
Transmission rate	78 kbits/s, TP/FT-10
External LonWorks data points	
Input variable	Max. 15 Network variables
Output variable	Max. 30 Network variables
Interfaces	
Serial connection	RS232, RJ45
Operator Panel	Modular jack, LonTalk Protocol

Application Specific Controllers

Application specific Controllers are devices for controlling secondary plant and equipment systems, such as HVAC, elevators, etc. These controllers can be adapted to individual requirements using a degree of flexible configuration settings.

A typical application specific controller is the Schneider Electric TAC Xenta 102 Variable Air Volume (VAV) Controller (Schneider Electric TAC, 2004, p. 53), which is a room controller for HVAC applications. The Controller keeps a constant temperature in the zone by controlling the air flow, heating stages and fan-in sequence. With a carbon dioxide sensor, the air quality can be zone controlled.

4.5.3 Management Level Devices

The Management level device primarily consists of the information technology and communications (ITC) network, with connected "operator stations, monitoring and operator units, programming units and other peripheral computer devices connected to a data processing device i.e., a server" (International Organization for Standardization, 2004, p. 53). In addition, one or a number of data and information processing (software) packages that allows human system interface such as a Graphical User Interface (GUI). Manufacturers provide such software packages in various modules, allowing designers and users to select what most suits their building.

Software packages range from simple information processing systems that control a single room via the Internet to complex whole of building services function, running not only the building plant and equipment, but also security, energy management, lighting, etc.

4.6 CONCLUSION

This section has provided an overview of the underlying BACS architecture and technology. The discussion presented the architecture of BACS, based on the three-level model of Field, Automation and Management levels, and where appropriate the fourth level of Service for maintenance. A preliminary discussion of control systems provided various control techniques and approaches. More pertinent to this section, was the presentation of BACS hardware and software, and their connectivity.

Connectivity forms the platform and resulting functionality of BACS, hence the significance. The technical architecture facilitates connectivity, which in turn facilitates communication and decision-making and automated control functions. The many BACS vulnerabilities lie in this architecture of connectivity and common communication protocols. Consequently security and facility professionals must understand this architecture to understand BACS vulnerabilities, as well as mitigation strategies and techniques.

Section 5. The BACS Market

5.1 INTRODUCTION

The Building Automation and Control System (BACS) industry market is a global enterprise, based on the pan-cultural need to extract key business functionalities from the built environment and its facilities. Consequently, the market is segmented on the basis of geography, end-user typology (government, commercial and residential facilities) and required business solutions. Therefore, this section presents an overview of both the current and future BACS industry and the respective market values.

The aim is to provide a descriptive analysis of the market, to achieve a greater understanding of the size and embedded nature of the BACS industry within the built environment. Such an understanding will highlight the impact that BACS is likely to have in future building, the effect on the security industry and the ever increasing exposure of building vulnerabilities.

5.2 GENERAL MARKET SIZE AND FORECAST

The Building Automation and Control Systems (BACS) market is considered from a top-down approach, to gain a better understanding of the industry and its products. The issue of cross-over definitions is raised, which may cause distortion in the market values.

5.2.1 BACS Market

Marketsandmarkets (2017) placed the 2016 global BACS business market value at US$53.66 billion, with an expected compound annual growth rate (CAGR) of 10.73 percent to reach a financial estimate of US$99.11 billion in 2022. Such growth is supported by other market analysts, as TMR Analysis (2017) estimates the CAGR to be 4.3 percent to 2024, but projects a rise from the current 2016 value of US$77.63 billion to US$108.49 billion in this period. Interestingly, TMR analysis placed the 2016 financial market value in excess of US$24 billion more than Marketsandmarkets (2016). Regardless of the final business values the financial figures highlight that BACS represent a significant component of the modern built environment.

In 2016 the global BACS market was valued at between US$54-78 billion, increasing in 2022 to an estimated US$104 billion.

Such variations in indicative market figures possibly results from the many and varied definitions of connected BACS systems (see Section 3), with the global BACS market encompassing all automation processes within the built environment. Such automation includes BACS, BAS, BMS, BEMS, IB and importantly, those not generally considered “smart” automation such as industrial automation systems.

5.2.2 Intelligent Building Market

According to Technavio (2016), the global Intelligent Building (IB) business market was financially valued in 2016 at US$12.50 billion, with a compound annual growth rate (CAGR) forecast of over 12 percent to reach a business market value of US$22.5 billion by 2021. In contrast, Marketsandmarkets (2016) valued the 2016 IB/BMS market at US$5.73 billion, with an anticipated CAGR of 34 percent to a 2021 value of US$24.73 billion.

In 2016 the global IB market was valued at between US$6-13 billion, increasing in 2021 to an estimated US$24 billion.

Within the growing business market expansion of Intelligent Building (IB) is the life safety and security systems segment, which is also poised to undergo continued growth. Such forecasts owe, in part, to the existence of several programmable business enabling features including emergency service response and communication functions during a facility's emergency conditions, such as fire and earthquake hazards. Functionaries also include facilitating responses to human centered threats including violence and terrorism events with the changing security posture in many parts of the world. According to Persistence Market Research (2016), due to the current global security climate, by 2026 the security segment is likely to overshadow the more traditional drivers of environmental and energy conservation segments.

> The BACS security systems integration will continue to grow, overshadowing the traditional system drivers of environmental and energy conservation segments by 2026.

5.2.3 Building Energy Management Systems Market

BSRIA (2016) placed the growth emphasis of automation on the drive for energy-efficiency, with their forecast that the Building Energy Management Systems (BEMS) market sector would have a global growth rate of over 13 to 15 percent per annum. Within this growth, 45 percent is accounted for by the European market, 33 percent is predicted to take place in the USA, with the rest of the world accounting for 22 percent (Lawson, 2014). The relative CAGR for 2009 to 2014 was 10 percent in Europe, 11 percent in the USA and 36 percent in the rest of the world (Lawson, 2014). In contrast, the growth in the whole building automation sector was forecasted to grow at a lesser rate (Lawson, 2014). Navigant went further, with a suggested 2015 BEMS growth from US$2.4 billion to US$10.8 billion by 2024, a CAGR of 18.2 percent (Martin & Talon, 2015).

A review of market data suggests that the Asia-Pacific region is forecast to have the fastest business market growth for building automation services (Marketsandmarkets, 2017; Technavio, 2016; TMR Analysis, 2017). Such expected growth is attributed to the high economic expansion of major Asia-Pacific countries and the subsequent construction industry growth projections. Such rapid modernization and willingness to adopt and adapt to Smart Cities within the Asia-Pacific is further feeding the automation market. Some of the larger industry manufacturers such as Schneider Electric and Honeywell Automation are amongst the investors in the deployment of integration solutions to India in particular.

5.2.4 BACS Market Growth

Regardless of the specifics of BACS systems, it is evident that this market will continue to grow for many years. According to the cited market research companies (Marketsandmarkets, 2017; Technavio, 2016; TMR Analysis, 2017), the global built environment automation system market will register steady growth due to business demands for energy-efficient systems, the need for ease of control and operability to reduce operational and maintenance costs, and governance with the increasing integration of life safety and security sub-systems.

> The global BACS market will achieve steady growth of between 12 to 34 percent due to the demand for energy-efficient systems, reduced maintenance and the need for control and operability.

5.3 GEOGRAPHICAL MARKET

Geographically, the global market is segmented into Europe, Asia-Pacific (including China and India), North America, and the rest of the World.

5.3.1 World Market Share

According to a 2017 BSRIA report, North America had the largest share (37%), followed closely by Europe (34%) and the rest of the world (23%) of the total BACS market share (Kaparthy, 2016). Such a market share is corroborated by several market research reports (Marketsandmarkets, 2017; Technavio, 2016; TMR Analysis, 2017) and is expected to remain consistent until 2024 (TMR Analysis, 2017). The Asia-Pacific is still in its nascent stage.

Based on type of service or product offered (Figure 5.1), Europe (34%) and North America (29%) have the largest total business market in BACS. It is suggested that North America is driven by services and maintenance, and the value-add element of the systems (Kaparthy, 2016). An assumption can be made that such a drive can also be transposed to Europe and parts of the Asia-Pacific. The rest of the world is still involved in heavy investment in physical infrastructure when compared against North America.

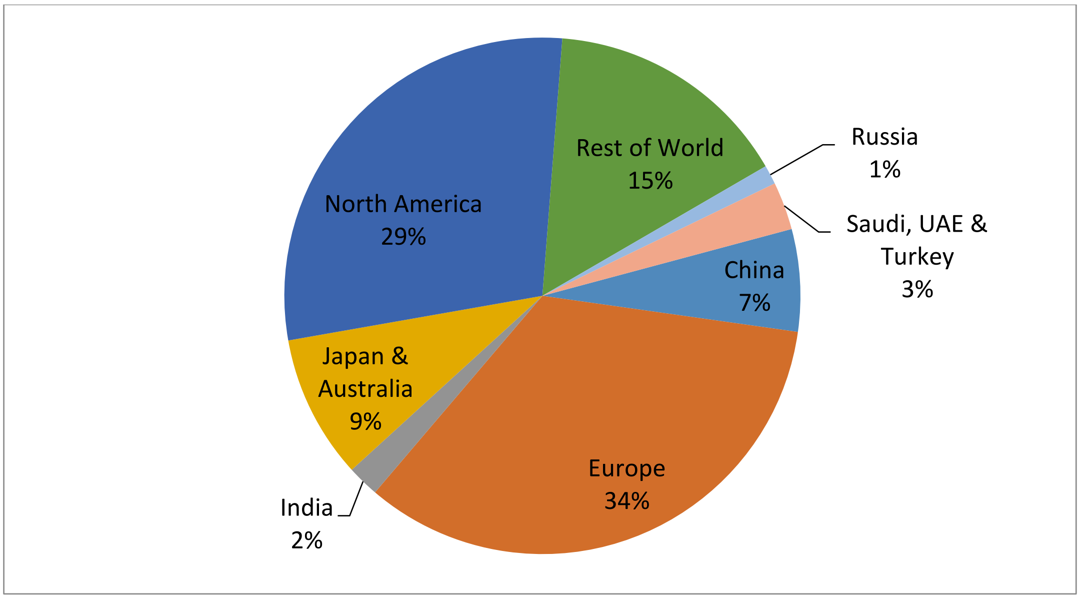


Figure 5.1. BACS World Product Market Share (Adjusted from Kaparthy, 2016)

5.3.2 The North America Market

The market in North America has been driven by several contributing factors:

1. Economic Slump 2008–2009: The USA showed a more robust response to the worldwide economic slump of 2008-2009. In 2010, the USA had a GDP rate increase of 2.5 percent (Elwell, 2013), compared with the European Union of 1 percent (Trading Economics, 2017). It is considered that North American companies had more money to invest in infrastructure improvements and innovations, with the focus being on return on investment.

2. IB/BMS Manufacturers: A considerable proportion of the global automation manufacturers are based in the USA, for example Honeywell International Inc., Cisco Systems Inc., Hubbell Inc., Johnson Controls International Plc., and United Technologies Corp. The growing competition within this market is considered to drive innovation (Lawson, 2014).

3. Smart Grid: Increasing usage of smart grid within the USA national electricity network overhaul (Smart Grid Interoperability Panel, 2010).

4. Rising Energy Costs: Concerns over raising energy costs have driven market strength in greener systems. For example, a year-long trial conducted by the US Department of Energy's Northwest

National Laboratory showed that commercial buildings could cut their heating and cooling costs by 57 percent (Lawson, 2014).

5. Security Concerns: Increased security concerns following the 2011 Twin Towers, resulted in reassessment of regulations. In addition, the more recent threat of local born and imported terrorism events has altered the view of building security, particularly public buildings. Organizational awareness and reduced risk appetites have increased the demand for changes in building design, secure technologies along with enhanced operating procedures.

6. Government Regulations and Targets: Gradual increase in regulations and government targets due to environmental concerns. While the USA did not remain signatories to the Kyoto Agreement, they did ratify the Paris Agreement in November 2016 – a global response to climate change and commitment to take measures to slow global warming. The Paris Agreement was considered an alternative, involving the USA, Australia, China, Japan, India and South-Korea. However, in August 2017, the USA informed the United Nations that they intend to leave the Agreement, although they cannot completely withdraw until 2020 and will remain in negotiations on current and future climate change deals (ABC News, 2017 Aug). These issues may still impact on future USA policies, with some examples of current policies:

> a. Regulation of Commercial Building Initiatives (CBI) to make commercial buildings completely energy independent by 2025.
>
> b. Energy Policy Act (2005) established tax deduction for energy-efficient commercial buildings, subsequently extended several times and expired in 2016.
>
> c. ENERGY STAR program, a joint initiative of the Department of Energy and Environmental Protection Agency, to increase implementation of energy-efficient equipment and techniques (Lawson, 2014; US Department of Energy, 2017).
>
> d. Advanced Energy Manufacturing Tax Credit (MTC) awards tax credits to new, expanded or re-equipped domestic manufacturing facilities that support clean energy development.

5.3.3 The European Market

The European market has similar driving factors to those driving the USA market:

1. European Energy Price: Between 2005 and 2013, European gas prices almost doubled, while major economies such as Germany became increasingly dependent upon politically sensitive and unstable countries such as Russia and the Gulf states for their imported gas supplies. The reliance upon uncertain supplies is a key driver in the EU member state governments pushing ambitious energy conservation targets.

2. Government Regulations and Targets: The EU signed the Kyoto Protocol in 1998 and subsequently, the Paris Agreement in 2016, making ambitious commitments to reduce greenhouse gas emissions by 8 percent below the levels of 1990 by 2012. This target was met and revised in 2008, when the EU adopted their Climate and Energy package, with a reduction target of 20 percent of the 1990 level by the year 2020. According to the BSRIA, this is in-part an explanation of the 10 percent CAGR between 2009 and 2014 (Lawson, 2014). Some examples of how the EU and its member states have put in place new legislation that has driven the building automation market:

> a. The Energy Performance of Buildings Directive (EPBD, directive 2002/91/EC), required member states to issue energy performance certificates to buildings. The directive 2010/31/EU, amended 2002/91/EC, makes member states place minimum

mandatory requirements for new or renovated buildings. The objective that by 2020, new buildings will have almost zero energy consumption.

b. Through the French Environment and Energy Management Agency (ADEME), since 2012, France has constructed low energy consumption and energy positive buildings. Existing buildings should lower their energy consumption by 38 percent by 2020.

c. In Spain, Indoor Heating and Air-conditioning Systems (RITE) regulation forms a framework for energy efficiency.

d. In Germany, a non-monetary but informative measure is the Guide to Sustainable Construction, published in 2001. It describes how to implement sustainability measures in construction, and recommends certain building equipment, energy supply technologies, etc.

3. BACS manufacturers: There are several major manufacturers and service providers based in the European Union. These include Ingersoll Rand (Ireland), ABB Ltd., (Switzerland), Schneider Electric SE (France), Robert Bosch GmbH (Germany) and Siemens AG (Germany).

4. The adoption of the public private partnership model to assist public companies to obtain finance to fund smart buildings (EY Ltd., 2015).

5.3.4 Rest of the World Market

Within the rest of the world, the global drive for financial and environmental gains is the main factor for growth in the BACS market. The market is heavily dependent upon the attitude within each country towards the greener side of the built environment and its facilities.

In China, the national five year plan from 2011 to 2016 included comprehensive strategies for improving energy efficiency in new builds. Given the high rate and size of construction within China, the adoption of financially attractive and efficient systems that comply with these plans has driven the building automation market.

Within the United Arab Emirates, the return of investor confidence after the financial crisis of 2008/09 resulted in an automation growth from 2013, with construction plans in both the private and public sector. Significant investments in the rail system, public schools and hospitals throughout the region has meant an increase in demand for integrated and IT convergent systems, particularly in the security and surveillance sectors (Fritsch, 2013).

In India, a slightly nuanced attitude is driving the market for building innovations. While elsewhere in the world the concern over price rises in energy are driving the need for efficiencies, in India, a more pressing public concern has been pollution caused by the burning of fossil fuels (BSRIA Institution, 2016). Regardless of motivation, the Indian government has responded, issuing the Energy Conservation Building Code (ECBC) that applies to commercial buildings and is therefore driving the demand for energy efficient BACS (Lawson, 2014).

In Australia, a new framework regulating minimum performance standards has been introduced as part of its National Strategy on Energy Efficiency. This framework has driven the demand for building automation and services to meet Australia's new built environment energy consumption standards. However, subsequently the Building Code of Australia (Australian Building Codes Board, 2016) was introduced, which is considered a soft approach for buildings to meet the compliance regulations without having to make too many infrastructure changes (Lawson, 2014).

5.4 BREAKDOWN BY END USER

On the basis of end-user, the global BACS market is segmented into government, commercial and some residential facilities. The Commercial and Residential facilities sector accounts for 37 percent of the global BACS market (Technavio, 2016). The increased rate of adoption of large scale BACS in shopping centres, hotel complexes, hospitals and transport areas including airports and railway infrastructures is driving the market within the commercial sector (Marketsandmarkets, 2017).

5.5 BREAKDOWN BY SOLUTION

The BACS market is attributed to a number of goods and services (Figure 5.2). BSRIA reported that the global market is broken into the physical automation product (33%), the value-add of automation in an organization (44%), and service and maintenance (24%) (Kaparthy, 2016).

1. The functions associated with the physical automation product, which may include utilities automation, etc., extending to security specific automation of entry control, fire life safety, intrusion detection and security lighting.

2. The value-add functions of BACS, which may include smart lighting for energy efficiency while maintaining fit for purpose, work comfort and safety; human resources single entry processing from recruitment to security access card, etc.

3. The service maintenance product refers to software as a service (see Section 5.5.1 Software as a Service), such as 24-hour service diagnostics and response, maintenance management, compliance, etc.

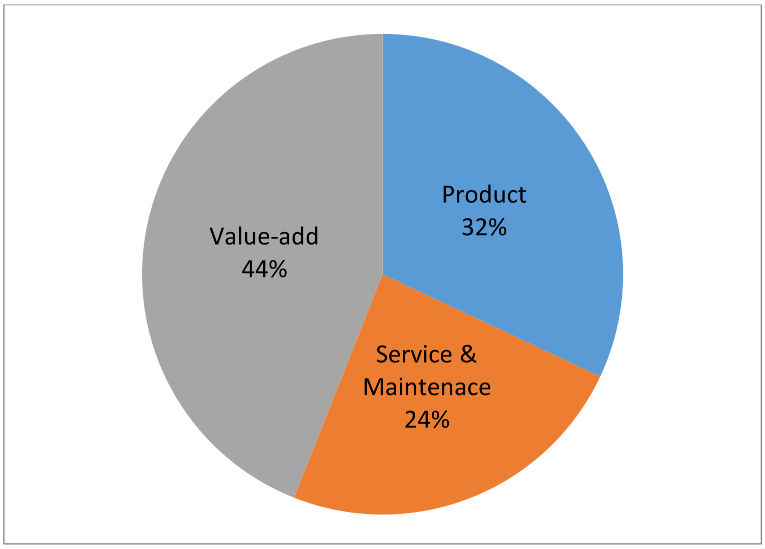


Figure 5.2. BACS 2016 Market Breakdown (Kaparthy, 2016)

5.5.1 Software as a Service

The majority of BACS service and maintenance offerings are sold in the “software as a service” (SaaS) model, with monthly to multiyear service contract agreements. Service configurations range from no-touch software modelling performance algorithms against estimated energy use from utility bills to fully integrated solutions that push automated system changes for operational and energy improvements.

The one unifying aspect of the building automation and its software is that solutions are designed to be open and technology agnostic in order to support customers with diverse building portfolios in terms of size and technology infrastructure. More specifically, common elements of building automation architecture include:

1. Integration via common communication protocol such as BacNet
2. Supplemental data collection and wireless or cellular communication devices including sensors, meters and gateways
3. Cloud-based software and analytics, accessible via Web or mobile applications
4. Network operations center for orchestrating managed services

These elements are delivered in a variety of ways. Large building technology incumbents like Schneider Electric, Siemens, Honeywell, and Johnson Controls may offer an end-to-end solution for large enterprise customers. Other smaller companies may partner to deliver comprehensive solutions. The customer's goals for implementing BACS can influence the appropriate configuration (Talon & Gartner, 2016).

5.6 CONCLUSION

The global built environment business model indicates a growing reliance on the BACS service industry. Demand for reduced operating costs, increased governance and accountability, along with security, is increasing the prevalence of connectivity within the built environment to achieve the necessary business solutions. These solutions include the use of modern connectivity technologies that provide automated operational, monitoring, control and auditing functions. Many organizations and facilities are investing in some form of embedded BACS automation. Organizational awareness and reduced risk appetites have increased the demand for changes in facility design that are more cost effective through automation.

The reviewed data highlights significant growth over the following decades in the BACS industry. Such growth will result in many more facilities, including critical infrastructures, operating through connectivity to the digital world. BACS is currently skewed towards larger commercial facilities, but this will change as smaller commercial and residential buildings are automated. Such a change will impact on the security industry, in both providing protection and integrating with the BACS industry.

The growth in technology uptake based on business market share indicates that the threats and vulnerabilities associated with BASCS will affect all modern organizations. The monetary value of the BACS industry, along with indicative growth, provides support for inclusion of enhanced features that protect the connectivity of the built environment in its drive to achieve business solutions. However, such features come at additional financial cost to organizations; consequently, business decisions need to be made regarding the necessity and priorities of such costs. Such decisions are best made through a risk decision where embedded security can be balanced against threat significance. The available BACS market data provides evidence that industry participants will respond to consumer needs within the built environment and therefore, higher security requirements based on contextual risk can be justified and mitigated.

Section 6. BACS Industry

6.1 INTRODUCTION

The global Building Automation and Control System (BACS) market is growing at an average Compound Annual Growth Rate (CAGR) of 12 percent (Technavio, 2016). Given the current and forecasted market growth, a competitive vendor landscape has developed at both national and global levels. The BACS market is dynamic, as major building technology incumbents continue to evolve their offerings, responding with new mergers and acquisitions on a national and global scale. The result is that new types of manufactures, suppliers and integrators, such as software start-ups, continue to enter the BACS market (Talon & Gartner, 2016).

Such a dynamic BACS market means that competitive advantage can result in greater functionality, broader technical integration, less expensive platforms and perhaps broader business value. However, such developments should not come at the cost of security, because vulnerabilities in one component of the BACS architecture can facilitate unauthorized access to other more critical parts by malicious actors.

The aim of this section is to identify the current global BACS manufacturers, demonstrating the size and scope of this dynamic market. Such understanding, in-part, will assist in understanding the current and changing threats that pose a risk for the security and facility professional.

6.2 GLOBAL MARKET PARTICIPANTS

The global BACS market is considered highly fragmented by region, with the presence of a number of international, national and local vendors. International vendors generally operate as Original Equipment Manufacturers (OEMs), distributing through national and local level dealers and system integrators (Technavio, 2016). Smaller companies, normally at a national or local level, may partner with similar companies to deliver comprehensive solutions (Talon & Gartner, 2016).

With the advent of the Internet of Things (IoT) and the Building Internet of Things (BIoT), continued integration is drawing large companies such as IBM and CISCO into the BACS market. In the past, the market was traditional dominated by more specialist global technology suppliers, such as Johnson Controls, Honeywell and Schneider. Nevertheless, as technology converges and connectivity continues to develop, many other innovative companies both large and small are likely to enter the BACS market. As shown by IBM and CISCO, such new companies entering this market are coming from more traditional information technology and communications (ITC) fields. However, it is not suggested that these fields are the only areas that new companies will be drawn from, as innovative software developers will likely have the greatest impact across the IB business market.

> As technology converges and connectivity continues to progress, other innovative companies will enter the BACS market. Innovation will initially come from information technology and communications (ITC), although the greatest change is likely to come from creative software solutions.

6.2.1 List of Market Participants

Geographically, the global BACS manufacturers market is segmented into North America (Table 6.1), Europe, the Middle East and Africa (EMEA) (Table 6.2) and Asia-Pacific (including China and India) (Table 6.3). Given the dynamic nature of this market, new manufacturers are likely to enter over time. The following regional tables of manufacturers are not a definitive or in any way an exhaustive list, rather indicative at the time of the study.

Table 6.1

North America Manufacturers

North America Manufacturers and Integrators		
Advantech	Creston Electronics Inc	Lonix Inc
Alerton Technologies Inc	Danfoss Inc	Lutron Electronics Inc
American Auto-Matrix Inc	Delta Controls Inc	McQuay International
Andover Controls Corp	Distech Controls Inc	Novar Controls Corp
Automated Logic Corp	Eaton Cutler-Hammer	Phoenix Energy Technologies
Barrington Systems	Ebtron Inc	Reliable Controls Corp
Bosch Security	Emerson Electric	Siemens Building Technology
Building IQ	General Electric Co	Solidyne Corp
Building Logix	H I Solutions Inc	Square D Co
Carrier Corp	Honeywell Inc	TAC Americas
Cimetrics Inc	Hubbell Inc	TCS Basys Controls
Circon Systems Corp	Innovex Technologies Inc	Teletrol Systems Inc
Computrols Inc	Integrated Building Solutions Inc	Temsco Inc
Contemporary Controls Inc	International Systems Inc	The Trane Co
Control Pak International	Invensys Building Systems	Tridium Inc
Control4	Johnson Controls	
Convergentz	KMC Controls	

Table 6.2

Europe, the Middle East and Africa (EMEA) Manufacturers

EMEA Manufacturers and Integrators		
ABB Ltd	Centraline	Legrand SA
ABEC Ltd	Chartwell Controls	Next Control Systems Ltd
Advanced Control Solutions	Cyclon	Priva
AES Control Systems	Demont Engineering	Robert Bosch GmbH
Alerton Technologies	Distech Controls SAS	Sauter
AMB	Eagle Technology	Schneider Electric TAC
Armiti Trading	Giza Systems	Siemens Building Technology
Atrina	Honeywell Inc	Trane
Avanceon	Ingersoll-Rand Plc	Trend
Beckhoff	Johnson Controls	Tridium Inc
Building Maintenance Services	Kieback and Peter	

Table 6.3

Asia-Pacific & Australasia Manufacturers

Asia-Pacific & Australasia Manufacturers and Integrators		
3S Technologies & Automation	Cyclon	KMC Controls
Alerton Technologies Inc	Distech Controls Inc	MS Group
AllGreen Ecotech	General Electric Co	NEC
Andover Controls Corp	Honeywell Inc	Novar Controls Corp
Automated Logic Corp	Innotech Control Systems	Oberix
Azbil Corporation	Innovex Technologies Inc	Schneider Electric TAC
Bajaj Electricals	Integrated Building Solutions Inc	Siemens Building Technology
Circon Systems Corp	Invensys Building Systems	United Technologies
Computrols Inc	Jardine Engineering Corporation	
Contemporary Controls	Johnson Controls	

6.3 MANUFACTURER PROFILES

According to market research (Technavio, 2016; TMR Analysis, 2017) the leading vendors in the BACS market are Cisco, Honeywell, Johnson Controls, Schneider Electric, Siemens Building Technology and United Technologies. Therefore, these manufacturers' are profiled, providing an overview of each company and its relevance to the building automation industry.

The BACS market is dominated by a relatively small number of large multinational companies. New innovative products, either hardware or software, that impact on the building automation market, will often result in one of the larger multinational companies acquiring (via purchase or product licence) the developing company.

The continued drive for single functional business solutions is likely to come from innovative software development using improved connectivity.

6.3.1 Cisco

Profile

Cisco Systems, Inc., (known as Cisco), is headquartered in California and is an American multinational technology company that develops, manufactures and sells networking hardware, telecommunications equipment and other high technology services and products.

Cisco has around 71,500 employees in 380 global sites in more than 160 countries.

OpenDNS, WedEX and Jasper are some of the 170 acquired subsidiary companies through which Cisco has become known as a market specialist company in technology areas such as IoT, DNS security and energy management.

In 2000, at the height of the dot.com bubble, Cisco became the most valued company in the world, with a market capitalization of more than US$500 billion (CBS.MarketWatch.com, 2000). Cisco was listed 54th in the 2016 Fortune 500 and 183rd in the Global Fortune 500, with revenue of US$49 billion.

Cisco is considered the largest networking company in the world (Network World, 2003).

Products

For the BACS market, Cisco specializes in the design and engineering of networking products, including routers, interfaces and servers. The company's strategy is to pursue alliances and create new channel partners to exploit the potential market of cloud services, Internet and network related technologies.

Through their acquisition of Jasper in February 2016, a deal worth US$1.4 billion, Cisco moved further into the IoT market. With the purchase of Vivint, a control center automation system, Cisco also entered the home and business automation markets.

One of Cisco BACS product is the Smart+Connected Real Estate Solution, which "converge building, safety, and communications networks onto the open Internet Protocol (IP) standard, streamlining processes by providing a single connection for building management and IT systems [and] helping transform physical space into service offerings. The network forms the foundation for an intelligent building infrastructure that adds value to every kind of real estate project" (Cisco, 2017).

6.3.2 Honeywell

Profile

Honeywell is one of the leading engineering technology and manufacturing companies that provides products, software and services for BACS control and management systems. Honeywell is headquartered in New Jersey, USA, operating three business units; Honeywell Aerospace, Honeywell Automation and Control Solutions and Honeywell Performance Materials and Technologies.

Honeywell was a 2016 Fortune 100 company, listed 75th in the Fortune 500 and 256th in the Global Fortune 500, with revenue of US$38.5 billion.

Products

Honeywell entered the BACS market in the 1980s and continued to be one of the largest companies throughout this period, after several acquisitions and mergers. Honeywell provides solutions to the retail, transportation and logistics, and healthcare markets. It sells its products through a global distributions network and local reseller partnerships.

In May 2016, Honeywell set up a new business unit offering platforms aimed at improving management controls, data analysis, and safety and efficiency using a range of industrial IoT applications. These products include DynAMo alarm and operations management, Industrial Cyber Security Risk Manager, Assurance 360 and Honeywell Pulse (Pieri, 2016), which facilitate operator functionality across broad network architecture.

In June 2016, Honeywell announced the release of its BACS system, Enterprise Buildings Integrator (EBI), to support the Middle East region's smart facility and cities ambitions. Honeywell stated that EBI leverages the connectivity of today's buildings to help make them more strategic assets that are green, safe and productive (Dey, 2016). According to Talon and Gartner (2016), the strength of Honeywell's business lies in their breadth of products and services, from installation, through services, controls and software management.

6.3.3 Johnson Controls

Profile

An American multinational, Johnson Controls designs, engineers and sells BACS systems. Johnson Controls also offers an installation and after sales service. Consultancy and technical services are also offered within the Johnson Controls commercial building segment.

Headquartered in Wisconsin, USA, it employs 170,000 staff in more than 1300 locations across six continents.

In September 2016, Johnson and Irish company, Tyco International merged to form Johnson Controls International plc.

Johnson Controls International was listed 70th in the 2016 Fortune 50, with revenue of US$40.2 billion.

Products

Under the Building Efficiency Business Unit, Johnson Controls designs, produces, installs and services ventilation, HVAC, facility management systems, fire and security systems, refrigeration for industrial and commercial units, and mechanical equipment for commercial and residential buildings. Their products and solutions in BACS are produced under the brand name Metasys.

6.3.4 Schneider Electric SE

Profile

Schneider Electric SE is a French multinational company that specializes in energy management and built environment BACS solutions. The products on offer include hardware (architecture), software (platforms) and services.

Headquartered in Rueil-Malmaison, Paris, France, Schneider employs 160,000 staff in approximately 100 countries across the globe.

Schneider's acquisition of companies such as Lexel in 1999 (installations and control systems), TAC in 2003 (power systems automation), Andover Controls in 2004 (building automation and security) and SCADAgroup in 2010 (SCADA and control systems), positioned the company into the global automation, and particularly, the energy management markets.

Schneider Electric was listed 354th in the 2016 Global Fortune 500, with revenue of US$29.6 billion.

Products

Schneider entered the BACS market in 2011 with their acquisition of Summit Energy and its SmartStruxure (Talon & Gartner, 2016), offering hardware, software and services for the BACS automation industry.

Life is On was launched by Schneider in 2015, which embodied the company strategy to capitalize on the digital transformation and IoT. The integration of this system with the SmartStruxure platform allows building system control for energy management through data analysis from electrical distribution, power use, HVAC, lighting, and fire and life safety systems.

6.3.5 Siemens Building Technology

Profile

Siemens Building Technologies is an operating division of Siemens AG, one of Europe's largest industrial companies. Siemens is a global electronics and IT company based in Munich, Germany. The Building Technologies Division manages the automation business and is based in Zug, Switzerland.

In 2016, Siemens had 351,000 employees in more than 200 countries, operating in 289 major production and manufacturing plants worldwide.

Siemens was listed 71st in the 2016 Global Fortune 500, with revenue of US$87.7 billion.

Products

Siemens offers the integrated HVAC system Synco and a scalable BACS system Desigo. In BACS and energy management, Siemens offers the APOGEE and TALON systems. Within the building energy management market, Siemens launched the Advantage Navigator BEMS in 2014.

6.3.6 United Technologies Corporation

Profile

United Technologies Corporation (UTC) is an American multinational company headquartered in Connecticut, USA, developing BACS solutions that include system architecture and software products. UTC researches and develops technology products in markets such as aviation, aerospace, HVAC, elevators and escalators (OTIS), fire and security, building systems and industrial products. UTC is a large military contractor, with around 10 percent of its revenue originating from USA government contracts.

In 2016, UTC had approximately 201,600 employees across the globe.

UTC was listed 45th in the 2016 Fortune 500 and 136th in the Global Fortune 500, with revenue of US$61 billion.

Products

In the BACS market, UTS offers Automated Logic. In addition, UTS has developed and produced the WebCTRL system, a Web based BACS system that can connect and control all automated systems installed within a facility.

6.4 CONCLUSIONS

The global BACS market has had significant growth over the last decade and this is likely to continue to grow. Industry demand has seen major international companies, with a strong technology and industry focus, operating in the BACS automation market, delivering hardware, software and maintenance services. These international companies will continue to both grow and dominate the BACS market, given their size, market share, business models of service, and continued solution driven approach.

The continued drive for single functional business solutions is likely to come from new software developments and improving connectivity. Such developments may impact on these BACS companies, but as they have shown, they will acquire companies if they feel a product will support their business. However, as technology converges, and connectivity continues to develop, new innovative companies will enter the BACS market. Innovation will initially come from information technology and communications (ITC) organizations, although the greatest change is likely to come from software solutions.

In the BACS business market, the organizations involved are all leading technological innovators or investors with research and development capabilities. They develop and seek product commercialisation. Such large organizations have the financial capital and business will to respond to market desires; therefore, as the commercial market demands more connectivity, ease of use and efficiency, they will respond in-kind. However, such response should not include compromises on security.

Security concerns exist in the BACS architecture, at the Management, Automation and Field levels. Therefore, it is essential that industry end users demand security across such connectivity accordingly. The size of the BACS market and its organizations involved means if it is required by the end user, then market participants will meet such demands as standard deliverables. Nonetheless, it must be acknowledged that due to such connectivity, vulnerabilities across the levels will never be eliminated regardless of manufacturer, therefore they must be managed.

Section 7: Automation Level Vulnerabilities

7.1 INTRODUCTION

The Automation level, within the Building Automation and Control Systems (BACS) architecture, provides the connectivity between the many field devices and supports the functionality of the Management level. The Automation level bridges the Field devices input/outputs and the Management level cyber domain (Wyman, 2017). The Automation level typically applies an open industry communications protocol, such as BACnet, LonWorks or Modbus (Shang, Ding, Marianantoni, Burke, & Zhang, 2014, p. 51) and today, Hypertext Transfer Protocol (HTTP), Transmission Control Protocol (TCP) and Internet Protocol (IP), etc. Furthermore, the Automation level is in essence an industrial control network, where generated data is distributed across its network to monitor and control.

The Automation level includes both hardware and software system elements, and therefore there are associated vulnerabilities. Given the differing functionality and communication connectivity, vulnerabilities are diverse. Furthermore, as device processing and connectivity capabilities increase, so do the vulnerabilities and realized consequences.

This section evaluates BACS vulnerabilities and their associated devices at the Automation level. In addition, provides a brief description of the underlying BACS automation device or network, before introducing suitable generic mitigation strategies.

7.2 AUTOMATION LEVEL

The BACS Automation level has vulnerabilities ranging from physical access to devices to what may be considered highly technical remote cyber-attacks. Table 7.1 provides an overview of the vulnerabilities, extracted from the critical meta-literature review.

Table 7.1

Automation Level Vulnerabilities

Section	Evaluation Description	Vulnerability
7.2.1	Device Access (Physical)	Device cover allows easy access to internal circuitry No anti-tamper detection to Device cover or mount Manual service switches Covert control of outputs Covert control of inputs Damaging the Devices, such as Controller
7.2.2	Network Access (Physical)	Network tamper, allowing communication access Traffic monitoring and analysis Network traffic injection Open source and free network programs and code Rogue device insertions
7.2.3	Wiretapping	Network wiretap
7.2.4	Electromagnetic Emanation	Network information extraction
7.2.5	Remote Connect Workstation	Unauthorized access Traffic monitoring and analysis
7.2.6	Foreign Device Replacement	Insertion of an unauthorized or rogue device
7.2.7	Internal & External Memory	Extraction of latent memory
7.2.8	Device Programmer	Unauthorized programming at Controller, using secondary device

7.2.9	Embedded Functionality	Unknown or unauthorized dormant device capability
7.2.10	Power Supply	Loss of main power No uninterruptable power supply capability

The meta-literature evaluation considered BACS automation basics, the vulnerabilities and possible mitigation strategies. "Basics" provides an overview of the fundamentals of the Automation level functionality, while the description is a narrative of exploitable vulnerabilities.

7.2.1 Device Access Vulnerabilities (Physical)

Basics: BACS Automation level devices, generally Controllers, are located throughout a facility. These devices are located alongside what could be considered non-critical devices, such as HVAC and lighting controllers. Many of these devices are located in electrical enclosures, close to the plant and equipment. They are generally mounted on DIN type rails, together with other electrical devices and connected to the Automation level network. Controllers may also be located in electrical risers, plant and equipment rooms, and ceiling spaces. In the past, these have only been secured due to safety reasons and to protect against minor misuse or nuisance issues. As Grand states "design of secure hardware is often overlooked ... leaving many devices vulnerable to hackers" (2004, p. 1). Physical access to such a device can facilitate exploitation, thereby breaching the security of the built environment.

Evaluation Description: Physical access to the Automation level (the Controller) results in various vulnerabilities being open to exploitation, including the use of the service switches or through covert means (magnet) to change output states, having no physical anti-tamper detection on the Controller covers to detect internal access, and denial of service through destruction. The security vulnerability arises once an attacker has physical access to a Controller, enabling changes to any output or input state at will. For example, a magnet can be used when placed onto a relay to force and hold in an output state.

Automation level access allows an attacker entry to a BACS network. Automation level hardware devices include routers, generic Controllers, specific Controllers, switches, etc. Access to the physical devices results in access to communication ports (Advantech, n.d.), which can facilitate broader system exploitation.

Device Cover

Device Controllers are generally provided with a plastic cover to protect the internal electronic circuits (Figure 7.1). These are generally fixed into place by a simple clip mechanism or common screw. Once the cover is unclipped, access to the internal circuitry is possible. Once access is gained, other vulnerabilities are exploitable, such as the ability to covertly change output states.

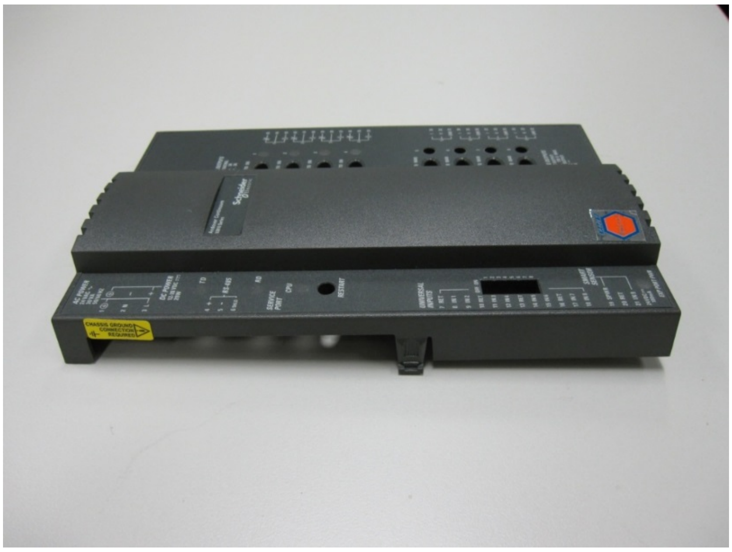


Figure 7.1. Typical AHU Controller Cover

Device Cover Anti-tamper

Generally, devices such as Controllers do not contain any form of cover anti-tamper switch to detect entry. A lack of anti-tamper allows interference in an intentional, unauthorized or undeclared manner (Garcia, 2007, p. 339) to the internal circuitry by unclipping or unscrewing the cover. Device covers, such as Figure 7.1, are installed to protect against safety or misuse. Such an approach may be suitable for standard plant and equipment Controllers; however, covers provide an opportunity for exploitation by skilled adversaries. Once physical access is gained, other vulnerabilities are accessible for exploitation, such as the ability to covertly change output states (see Service Switches).

Anti-tamper detectors should provide protection against unauthorized entry into or removal of the Controllers cover and other electrical enclosures. Anti-tamper detectors may be a micro-switch, bias-magnet or optical switch (Garcia, 2007, p. 339). Nevertheless, anti-tamper detectors may be vulnerable to attack from poor design of the detector and/or enclosure, by-pass or reconfiguration.

A bias-magnet anti-tamper detector bypass may be achieved through the use of additional magnets to spoof the detector, whereas reconfiguration may occur through the re-fixing of the anti-tamper secondary magnetic from the actual door to the devices. Such a reconfiguration will allow the door to be opened and closed without detection. In addition, some enclosures have not been designed to physically resist a determined attack, resulting in the potential to gain side access through cable entry points, bending part of the door back or general flex in the enclosure.

Service Switches

In general, Controllers provide the user with manual override of its digital and analogue outputs. These outputs are controlled by a switch that can be used to change the state of output, from on, off or auto. The intent of these switches is to allow the user to active or de-active the outputs locally, when maintaining the Controller and its connected Field level devices.

The “auto” position of the switch places control of the output with the BACS program. The switch “on” position turns the output to a permanent on state, while the “off” position turns the output to an off state. Once physical access to the Controller is gained, these switches can be manipulated to covertly change output states and affect field devices.

Covert Control of Outputs

On some Controller output switches, a magnet can be used on the digital output power relays to change their state covertly. In testing, this has been confirmed by observing the digital output states, while a magnet was attached to a power relay (Brooks, 2012), where the Management or Automation levels did not identify such covert changes in output state. Change of state included the Controller's output indicator and connected field device. However, not all output switches are prone to such vulnerabilities, depending on the technology used.

Covert Control of Inputs

Signal inputs are generally not supervised or end-of-line supervised, allowing short circuit (electrical closed circuit), by-pass or removal (electrical open circuit) of inputs. The Management or Automation levels do not generally have the capability to identify such covert change in input states. Note: New (high security) Controllers are now coming onto the BACS market with anti-tamper connectivity (dual end of line supervision) functionality to overcome this vulnerability.

Damaging the Device

Destroying or damaging devices, such as a Controller, will deny an authorized user from monitoring or controlling connected inputs or outputs. Such damage creates a denial of service attack (Wyman, 2017, p. 8), although the loss of the Controller should be noted at the Management level. The Management level software polling function will trigger some response on detecting the loss of communication due to damage. Another factor may be a loss of automated GUI monitoring from the localized Controller.

Summary

Physical access to the Controller is a significant localized threat that is poorly understood. Once an attacker gains entry to a Controller, they can change any input or output state at will using manual overrides, although in some systems this may inform the Management level. The majority of Controllers are housed in a plastic cover to protect its internal electronic, without anti-tamper cover or mount detection. A lack of a physical protection and tamper detection enables a covert attacker to access the Controller and manipulate the inputs and outputs, pus gain access to the Automation level network. Finally, the attacker can destroy the Controller for a denial of service, although this will likely inform the Management level via loss of communication. Where Controllers or other BACS device enclosures and covers lack physical robustness, it may be necessary to install them in more secure mounted containers.

7.2.2 Network Access Vulnerabilities (Physical)

Basics: The BACS Automation communication network is generally located throughout the facility, linking the automation devices such as Controllers, switches and routers. Like the Controllers, this network may be located in electrical risers, cable trays in the ceiling space, and plant and equipment rooms. Physical access to the Automation level network may therefore result in various exploitable vulnerabilities.

Evaluation Description: Automation level communication network access may give the attacker access to the BACS system. The intent of manufacturers, at this level, is to reduce network traffic for efficiency, whereas "security mechanisms (especially cryptographic algorithms) are computationally intensive and must not exceed available device resources" (Granzer, Praus, & Kastner, 2009).

Network Tamper

The Automation level communication network contains no anti-tamper cyber-detection capability, allowing wiretapping, cutting and splicing, etc., as well as methods to link to, monitor or insert control data onto the automation network. Once access is gained other vulnerabilities are exposed, such as the ability to covertly change output states.

Traffic Monitoring and Analysis

The ability to access the network enables access to the communication traffic. With most BACS automation "protocols, such as BACnet, it is common to name devices (and the data they generate) to reflect their physical location" (Shang et al., 2014, p. 53). By monitoring this network traffic, which is also generally in "plain English", an intruder could note building name, floor level, function of office, etc., allowing a "picture" of the facility and its operating modus to be developed. As Wyman states, "an observer … may glean context on the process by viewing process graphic displays, reading point description and examining the programs for the controller" (2017, p. 8). In real time, an understanding can be gained by the attacker as to when certain areas may be accessed or empty via the activation of building services. For example, a card reader is swiped, a door lock released, a reed switch bypassed and a light sensor senses movement turning on a light.

Open and Free Source Code

Packet analyzing or packet sniffing involves using an appropriate software and network connectivity to intercept and log traffic passing over the network. There are many open source free software programs and coding that enables network analysis and programming (see Section 7.2.5). By capturing and reading the data transmitted between Controllers, it is also possible to inject data back into the network with false commands. Such false commands may enable access to the system or change outputs, such as opening a door or bypass an alarm sensor.

Unauthorized keys; where the secret keys are known to an attacker and they can craft a new Update-Key-Set message to add a second set of authentication keys to network devices. This addition enables an attacker to send messages without others being able to decrypt or view their contents, reducing the discovery of their target. Once a network's secret key pairs (that enable the BACnet security to work) are known to an attacker, the network message security can be removed and the messages themselves read and manipulated.

Device Insertion

Physically inserting an unauthorized device, such as a Portable BACnet to MS/TP Router connected to an unauthorized computer can facilitate nefarious actions within the BACS system. Insertion of such devices, through physical connection or via wireless means, can result in rogue devices being connected to a vulnerable point of the physical communication network, exposing network traffic for exploitation.

Such devices could be connected anywhere on the physical BACS Automation network, for example in a ceiling space, plant room or service duct.

7.2.3 Wiretapping

Basics: Wiretapping is used for accessing communication data without permission and detection. Formerly, this was done by installing "wiretaps" to read information from telephone lines. With the emergence of the Internet, mobile phones and Voice Over IP (VoIP), wiretapping techniques have evolved. Today, wiretapping vulnerabilities should consider all forms of media transfer methods.

The Internet Engineering Task Force (IETF) defined wiretapping (2000) as information that is passed across the Internet from one party to one or more other parties, but is delivered to an additional unauthorized third party. The third party receives this information without the knowledge of the sender or receiver, when the normal expectation of the sender or receiver is that the transmitted information will only be seen by the receiver. Furthermore, when the third party acts deliberately to target the transmission of information, because of their interest (IETF, 2000).

There are three steps involved in wiretapping: accessing, collecting and filtering the signal (Diffie & Landau, 2009). Data is accessed by using devices that are directly connected to the wires, to receivers of electromagnetic emanation or a computer program. Data is then filtered, and the information recorded and processed accordingly.

Evaluation Description: There are a variety of methods available to wiretap a communication network, depending on the network communication medium. Listening devices or software for interception can be installed on any one of the three BACS levels, the communication medium or devices used in connecting the level, such as routers, etc. Taps can be installed just before the transceiver or directly on the network cable, using mediums such as twisted pair cabling or fiber-optic cables.

The Automation level communication network operates using such protocols as BACnet, LonWorks, etc. Most BACS manufacturers attempt to reduce network traffic for efficiency. As devices become more specific in plant and equipment functionality and locality, less vulnerability would be expected. In general, the Automation level network is physically cabled throughout a facility, with restricted cognizance of its security vulnerabilities and potential for covert misuse. Such a network could be prone to covert misuse with a foreign signal being embedded into the network as a vehicle to activate covert devices or exfiltration.

Due to the nature of the Automation level communication network, physical access to the “buss” can be gained from many internal and external parts of the facility. Once accessed, wiretapping is relatively simple. Access is gained using devices such as a RS-485 to USB converter, which does not interrupt the network and therefore minimizes detection. For example, there are a number of ways to wiretap an Ethernet cable. These include physically cutting the cable and re-crimping, accessing a router switch and plugging in a remote workstation or covertly using insulation-displacement connectors and an Ethernet card (Figure 7.2). Cutting and crimping will result in the communication link failing briefly, which may alert an authorized user. The use of insulation-displacement connectors allows connectivity without cutting the network cable, hence no loss of the communication link.

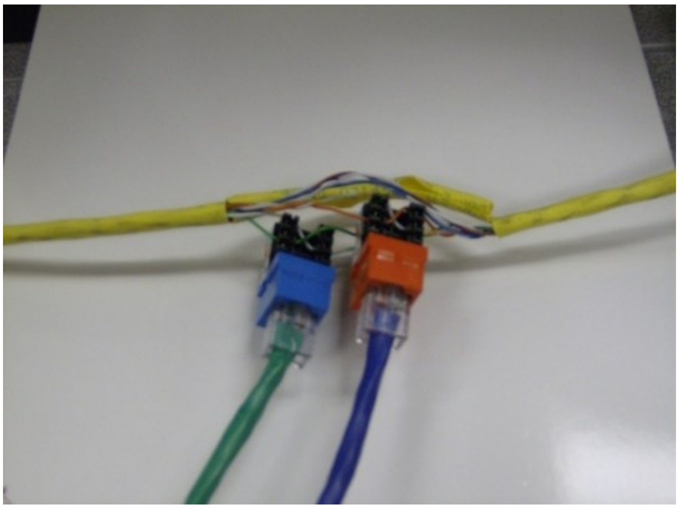


Figure 7.2. Covert Wiretap using Insulation-displacement Connectors

Once the tap has been established, free packet analyzing software such as Wireshark or the BACnet specific program (BACnet4Linux) can be used to dissect and analyze the data in transit.

7.2.4 Electromagnetic Emanation Attack

Basics: An electromagnetic (EM) emanation attack, often referred to as TEMPEST, is a technique to intercept and analyze electromagnetic emanations for restricted data. Electrons flowing through wires generate an electromagnetic wave with a magnetic vector, which are propagated along the cable. The emanations can cause electromagnetic interference (EMI), for example the noise of a radio when placed besides a CRT display.

The first well known scientific article about TEMPEST was titled "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?" (Van Eck & Laborato, 1985). Further research was done on CRT displays and flat-panel displays; however, TEMPEST is not limited to emanation of displays. There are different kinds of emanations from electric, electronic, electromechanical or electro-optical equipment that can be captured, measured, and boosted including optical, acoustic and electromagnetic emanations (Auddy & Sahu, 2008).

Evaluation Description: Electrical power is used in all parts of BACS, resulting in many possible attack points. For example, in 2009 at the Las Vegas Black Hat Conference an attack by keystroke interception was presented. In this case, attackers were able to read the keystrokes typed onto an operator's keyboard via the mains power as emanations from the data wire of PS/2 keyboard influenced the cable ground wire (Barisani & Bianco, 2009). The ground wire from the PS/2 keyboard is directly connected to the power adapter. Therefore, extracting the necessary information was accomplished by using an oscilloscope and subtracting the standard wire noise (Figure 7.3).

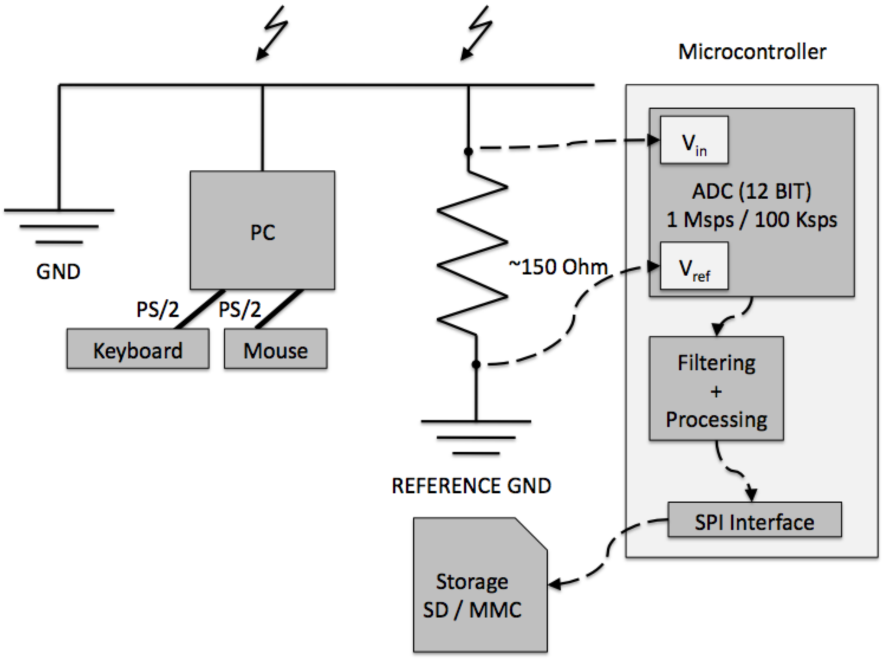


Figure 7.3. Electromagnetic Emanation Attack of PS/2 Keyboards over Power

(Barisani & Bianco, 2009)

Literature suggests that EM attacks are possible on communication media such as telephone lines, coax cables, twisted pair cabling or power lines. Automation level devices are all connected to both mains power and a communication network, resulting in the technical possibility that an attacker could exploit this vulnerability.

To prevent wiretapping, all devices such as routers, switches and communication media must be protected from unauthorized physical access. In addition, all cables should be shielded to suppress electromagnetic emanation. However, such a tactic is virtually impossible and expensive, and consequently encryption algorithms above layer 1 should be used to protect the transmitted traffic from this type of attack.

Furthermore, it is technically possible to induce a malicious signal into a cable running in parallel to an automation level network cable. However, there are technical limitations such as cable length, induced cable noise, etc., but vulnerabilities such as denial of service, data disruption and traffic monitoring are quite feasible.

7.2.5 Remote Connected Workstation

Basics: Through physical access to the BACS Automation network, an additional device configured on an unauthorized workstation may be connected.

Evaluation Description: The Automation level network is spread throughout the facility, where access could result in an unauthorized workstation being connected. Issues ranging from denial of service to traffic monitoring. Analysis of the BACS system is also possible.

Gaining physical access to a Controller that contains a router (switch) on the BACS Automation network enables an unauthorized computer to be plugged into the network. For example, using the freeware BACnet4Linux program can enable an unauthorized computer to monitor a BACS inputs and outputs. Ettercap can be used to undertake an Address Resolution Protocol (ARP) attack and create a whole of system denial of service. Professional BACnet programming software could result in a greater vulnerability.

BACnet has been of some interest to the Internet community for some time, therefore many open source programs are available to operate specifically with this protocol. These open source and free programs include, but are not limited to:

- BACnet4Linux: Linux specific program designed to read and write to BACnet devices over Ethernet.
- Yabe: Graphical explorer program for BACnet devices, written in C# for browsing BACnet devices. Currently supports BACnet/IP, BACnet MSTP and BACnet PTP. Basic functions for ReadProperty, WriteProperty, ReadPropertyMultiple, WritePropertyMultiple, I-Am, Who-Is, SubscribeCOV, Notify, AtomicWriteFile and AtomicReadFile.
- VTS: Visual test shell for Win32, used for testing a BACnet implementation. Includes a network sniffer for BACnet messages and the ability to send any BACnet services.
- Wireshark: Cross platform protocol analyzer with BACnet support.
- BACnet Firewall Router: Combines BACnet routing capability with traffic management functions to carefully control access to BACS networks.
- BACpypes: BACnet stack written in Python.
- BACsharp: BACnet/IP stack written in C#.
- BACnet4J: BACnet/IP stack in Java that serves as the BACnet layer for Mango.
- Mango is a machine-to-machine software for industrial control, SCADA, HMI or domotics (Karg, 2015).

7.2.6 Foreign Device Replacement

Basics: The BACS Automation level firmware and software protocol do not always require new device authentication when installed onto its network.

Evaluation Description: Some form of physical access to the network or a device could lead to foreign devices being installed onto the network, which may allow many types of attack. A similar, but foreign, Controller connected to the Automation network could potentially be reconfigured to be recognized by the BACS system.

7.2.7 Internal and External Memory

Basics: Devices will either be replaced due to failure or during upgrades; however, most BACS devices contain some degree of on-board RAM or non-volatile memory function. In addition, expandable memory using MMC cards or other portable memory devices are often embedded. Typically with devices such as Controllers, this may be 8Mbyte of RAM, expandable up to 128Mbyte (Schneider Electric TAC, 2004, pp. 67-71).

Evaluation Description: It has been shown that it is difficult to fully erase data, such as network data, encryption keys and other core data that will remain after the device has been memory erased and power removed (Gutmann, 2001).

7.2.8 Device Programmer (Handheld)

Basics: Most BACS have the functionality to locally program an Automation level device, such as a Controller. This function allows Integrators, installers or maintainers to commission and repair a system without the added complexity and sometime remote nature of accessing the Management level workstation. Using a manufacturer's handheld BACS programmer enables functions to be programmed on devices, which are typical connected direct to the device.

Evaluation Description: There is little control or restriction in the sale and supply of BACS specific programming devices, enabling persons to purchase these from a specific supplier. For such an attack, physical access to a device is required; however, the "proliferation of field-upgradeable hardware has given adversaries opportunities to attack" (Grand, 2004, p. 21).

Most Controllers contain a service port which a readily available Service Tool can be connected. The Service Tool allows local access to the Controller and ability to change its programming.

7.2.9 Embedded Functionality

Basics: BACS manufacturers provide many functions to increase ease of use and connectivity, with the intention of making products more appealing to customers and thus increasing sales. In today's competitive manufacturing environment, it is often less expensive to mass produce a single device with all functions embedded for all markets, rather than customize different devices. The same view can be applied to BACS devices at all levels of its system.

Functionality of devices include embedded capability that can be up-sold or activated depending on customers' expectations and building requirements, which is characteristic of the contemporary electronics environment. One such direction is the increase in wireless connectivity, as this provides installer/integrators and facility professionals with significant infrastructure savings. Many of these embedded functions may be dormant (software disabled) and only activated when the function is required. Some typical embedded functions may include:

- Wireless or TCP/IP connectivity
- Memory expansion
- Types of input or outputs

Dormant functionality may provide the opportunity for a capable threat to gain unauthorized system access.

Evaluation Description: BACS users, maintainers and some Integrators, being second tier to the manufacturers, may not have full transparency or understanding of embedded device functionality. In addition, installers and integrators may draw upon some of these functions to support the user's facility requirements, such as Human Resource (HR) functionality, facilitating a more responsive service to building issues. Consequently, a lack of understanding of such embedded functionality, coupled with the ability to software enable such functionality, may lead to system compromise such as denial of services or automation control being gained through remote system access facilitators.

7.2.10 Power Supply

Basics: A BACS and its devices require power to maintain monitoring and control capabilities. In general, power requirements are mains power (110V/240VAC) for such devices as workstations and low voltage (12/24VAC/DC) for its Automation and Field level devices. BACS are not, in general, provided with uninterruptible power supplies (battery back-up) and the loss of mains power will result in a loss of system capability.

Evaluation Description: Loss of mains power or local device power will result in either the loss of the whole or part of BACS. When mains power is lost, other facility plant and equipment fail such as HVAC, non-emergency lighting, elevators, etc. It is not practical to provide uninterruptible mains power to plant and equipment, such as HVAC. Therefore, it has not been common practice to provide BACS with uninterruptible mains power. In contrast, critical life safety systems such as fire detection, annunciation and suppression are provided with uninterruptible power supplies.

7.4 CONCLUSION

The BACS Automation level provides the necessary connectivity and communications between the many Field devices (for example, the light, temperature or security detector) to the Management level (for example, how and when was that device used). This BACS level typically applies an open industry communications protocol, such as BACnet, LonWorks (Shang et al., 2014, p. 51), Hypertext Transfer Protocol (HTTP), Transmission Control Protocol (TCP) and Internet Protocol (IP) between devices and higher gateways. In practice, the Automation level is an industrial control network; designed, installed and maintained by engineers or Integrators, where data generated at this level is distributed across its entire system network.

The Automation communications network is the core of a Building Automation and Control System (BACS), providing facility and device-wide connectivity. However, such connectivity, including embedded data entry access points, results in a degree of embedded vulnerability that can be exploited by interlopers. The most significant vulnerabilities are considered to be physical access to the Automation level devices and its communications network. Evaluated vulnerabilities are spread across physical devices, communications network access, wiretapping, electromagnetic attacks, remote connectivity, foreign device placement, embedded and remote memory, device programming, and embedded functionality and power supplies. The vulnerabilities identified and summarized in Table 7.2 were presented using a traffic light system (see Appendix A) to highlight the vulnerabilities in terms of threat levels.

Section 8: Management & Field Level Vulnerabilities

8.1 INTRODUCTION

The Building Automation and Control Systems (BACS) Management architectural level is the human interface, providing systems output functionality. The Management level is an information system, with the intent that the facility is operated and maintained as efficiently and cost effectively as possible (Lowry, 2002, p. 695). The Field level provides connectivity from the many field devices to the Automation level. The field devices are spread throughout all parts of the facility. Field devices may be a light switch, a temperature sensor or security detector (as system inputs) or a cooling valve or fan drive (as system outputs). Both levels typically apply open industry communications protocols, such as BACnet or Modbus (Shang et al., 2014, p. 51).

As with the Automation level, both of these levels include hardware and software elements, and therefore associated access vulnerabilities. While acknowledging the Management level software as a relatively minor element of the corporate communications network. Consistent with other office and business software packages and information technology platforms, the BACS elements have significant threats that pose a risk to the confidentiality, integrity and availability of their data elements.

Given the quite different technologies, functionality, processing capability and communications connectivity, vulnerabilities of these elements are diverse. This section presents these vulnerabilities and their associated devices at both the Management and Field levels. In addition, provides an overview of underlying BACS generic mitigation strategies.

8.2 MANAGEMENT AND FIELD LEVELS

The BACS Management level vulnerabilities range from physical access to workstations to remote technical "hacking" via the corporate network. Table 8.1 provides an overview of the vulnerabilities, extracted from the critical meta-literature review.

Table 8.1

Management Level Vulnerabilities

Section	Evaluation Description	Vulnerability
8.3.1	Device Access (Physical)	Device access to workstations, etc. Cyberattack of devices through insertion Destruction of devices
8.3.2	Network Access (Physical)	Monitor and analyze network connections Wiretapping of the network to monitor and analyze the network and its systems Insertion of illegal or unauthorized device
8.3.3	Device Access (Digital)	Cyberattack of devices via network
8.3.4	Electromagnetic Emanation	Monitor and analyze network connections

The Field level vulnerabilities range from physical access to manipulate of the device, with Table 8.2 providing an overview of the evaluated vulnerabilities.

Table 8.2

Field level vulnerabilities

Section	Evaluation Description	Vulnerability
8.4.1	Device Access (Physical)	Manipulation of device input/outputs Physical disconnection of devices Destruction of device Security sensors (detectors) tamper detection
8.4.2	Connectivity Access (Physical)	Loss of function Monitoring of the connection Control (remote) of devices via connection Spoofing device outputs Security sensors (detectors) tamper detection
8.4.3	Electromagnetic Emanation	Monitor and analyze network connections

The meta-literature evaluation considered BACS automation basics, the vulnerability and possible mitigation strategies. "Basics" provides an overview of the fundamentals of the Management and Filed levels functionalities, while the description is a narrative of exploitable vulnerabilities.

8.3 MANAGEMENT LEVEL

8.3.1 Device Access Vulnerabilities (Physical)

Basics: The Management level devices include the corporate Information and Communication Technology (ICT) network, workstations, routers and network switches. Physical access to the Management level devices results in various vulnerabilities being open to exploitation.

Evaluation Description: Unauthorized physical access to the Management level devices allows an attacker access to the BACS network, leading to a level of greater corporate network access. Once access is gained at this level, other non-building automation networks and systems are exposed to some degree.

Device Access

Physical access to a human interface device, such as a workstation, which does not apply appropriate or effective physical, ICT or cybersecurity protection strategies, could result in the BACS being exposed to a critical level of attack. For example, hijacking an operator's workstation allows the issuing of unauthorized control commands (Wyman, 2017, p. 8). When access is gained at this level, other non-building automation systems and applications may be exposed to threats against data confidentiality, integrity and availability. The range of threats at this level are substantial.

Once access at the Management level is gained, the BACS is vulnerable to the embedding of covert program, changes to bypass protection strategies, real time remote control of doors and other facility sub-systems, approving unauthorized system access from a remote or local zone, activating embedded software, firmware or hardware such as wireless connectivity, along with the possibility of installing additional covert automation devices.

Consistent with the confidentiality, integrity and availability model of information security, various types of software are available for use by interlopers to attack the BACS, resulting in attacks of accessing and copying (Confidentiality) the automation database program. Once copied, the management database can be loaded onto an external workstation for later manipulation and/or remote monitoring and control (Integrity and Availability).

Cyberattack

While the threat of cyberattack is not new, cyberattacks are likely to increase in 2017 (OSAC, 2017, p. 1) with such attacks predicted to continue to increase each year for the foreseeable future. A trusted employer may insert an infected storage device into their corporate network connected workstation that downloads malicious code. Malicious code may be in the form of viruses or worms enabling attacks against the confidentiality, integrity and availability of the BACS software and data, facilitating unauthorized access through back-door, password cracks, brute force attacks, dictionary attacks, denial of service attacks, spoofing, man in the middle attacks, sniffing programs, key loggers, etc. These vulnerabilities may range between denial of service to the ability to remotely reprogram the BACS to allow non-authorized entry without detection.

Destruction of Devices

Physical device access vulnerabilities may result in the destruction of management devices, such as workstations, switches, etc. This attack creates a denial of service and lack of system oversight.

8.3.2 Network Access Vulnerabilities (Physical)

Basics: The Management level is generally the corporate Information and Communication Technology (ICT) network. This network is supported by devices, such as routers and network switches. The Management communication network is generally located throughout the facility, using network transport medium such as copper twisted pair cables for Ethernet (Cat5 or similar) fiber-optic cables, coax cables, radio frequency (RF), and infrared or wireless technology (LonWorks Americas, n.d.). As with the Automation level network, this network may be located in office spaces, server rooms, electrical risers, cable trays in the ceiling space, and plant and equipment rooms.

General office spaces have a multitude of network connection points, designed to allow general workstations, phones and other office equipment such as printers to be connected into the corporate network. Therefore, physical access to this corporate network may result in various vulnerabilities being exploited through connectivity.

Evaluation Description: Unauthorized physical access to the BACS Management level network may allow access to the wider facility network and to the corporate network (i.e., finance systems). Such access could prove a significant threat, as access may allow intrusion into the many other applications that operate within the corporate environment. Once access is gained at this level, other non-building automation networks and systems may be exposed to some degree of unauthorized access, disclosure, alteration or availability.

Network Connections

A corporate network will have many possible connection points, physically and wirelessly. Physical connection opportunities include offices, server rooms, electrical enclosures or plant rooms. A standard Ethernet connector (RJ45 or similar), if not disabled or removed, enables foreign devices to be connected. Foreign network connections may enable traffic monitoring and analysis of the network. To overcome this, corporate networks should be secured against foreign device connectivity and capable of detecting foreign devices on the network.

Wiretapping

Basics: Wiretapping is used for accessing communication data without permission and detection. Formerly, this was done by installing "wiretaps" to read information from telephone lines. The emergence of the Internet, mobile phones, etc., has resulted in wiretapping techniques evolving to facilitate exploitation of connectivity. Today, wiretapping should consider all forms of media transfer methods (see Section 6.2.3 Wiretapping). The Management level (corporate) communication network operates using such protocols as Internet Protocol (IP), BACnet, etc., and is extensive throughout a facility.

Evaluation Description: The methods to wiretap a corporate network are many and depend on the network communication medium, such as copper or fiber-optic cables. Wiretapping the corporate network cable allows traffic monitoring and analysis of the network and its systems, and potentially injecting traffic or introducing malicious code. There are many ways to wiretap a communication medium. These include physically cutting the cable and re-crimping, accessing a router switch and plugging in a remote workstation or covertly using insulation-displacement connectors and an Ethernet card. However, some forms are more easily detected than others. For instance, cutting and crimping will result in the communication link failing briefly, which may alert an authorized user. Wiretapping to monitor and analyze may compromise of the confidentiality, integrity and availability of the network traffic and programs.

Listening devices or software can be installed on the Management level medium or its connected devices, such as routers, etc., to enable nefarious monitoring and control. Taps can be installed just before the transceiver or directly on the network cable.

Device Insertion

Physically inserting an unauthorized device could result in devices, such as a Portable BACnet Router with a laptop computer, being connected to a vulnerable (unprotected) corporate network point. These devices could be connected anywhere on the physical corporate network, facilitating further exploitation of the organizational communication network. Such holistic connectivity means unauthorized access can be gained via the BACS network where the confidentiality, integrity and availability of information in other business networks can be at risk.

8.3.3 Device and Network Access Vulnerabilities (Digital)

Basics: The Management level devices include corporate Information and Communication Technology (ICT) network, workstations, routers and network switches. Digital access to the Management level devices results in various vulnerabilities being open to exploitation.

Evaluation Description: Unauthorized digital access to the Management level devices allows an attacker access to the BACS network, leading to a level of greater corporate network access. Once access is gained at this level, other non-building automation networks and systems are exposed to some degree.

Cyberattack

Cyberattacks are likely to increase in 2017 (OSAC, 2017, p. 1), with such attacks predicted to continue to increase for the foreseeable future. For these attacks to occur, interlopers do not require physical access to the network; rather, remote network cyberattack may deliver malicious code. For example, a trusted employer may unintentionally download a malicious code via their email. Malicious code may be in the form of viruses or worms enabling attacks against the confidentiality, integrity and availability of the BACS software and data, facilitating unauthorized access through back-door, password cracks, brute force attacks, dictionary attacks, denial of service attacks, spoofing, man in the middle attacks, sniffing programs, key loggers, etc. These vulnerabilities may range between denial of service to the ability to remotely reprogram the BACS to allow non-authorized entry without detection.

8.3.4 Electromagnetic Emanation Attack

Basics: An electromagnetic (EM) emanation attack (see Section 7.2.4 Electromagnetic Emanation Attack) is a technique to intercept and analyze electromagnetic emanations to gather restricted data. As electrons flow through wires they generate electromagnetic waves, with a magnetic vector that propagates along the cable. The emanations can cause electromagnetic interferences (EMI), for example the noise of a radio when placed besides a main power cable. There are different kinds of emanations from electric, electronic, electromechanical or electro-optical equipment that can be measured, including optical, acoustic and electromagnetic emanations (Auddy & Sahu, 2008).

Evaluation Description: Electrical power is used in all parts of a building automated system, resulting in many possible points of electromagnetic (EM) emanation attack. For example, in recent years attackers have read keystrokes from hard-wired computer keyboards from the mains power source (Barisani & Bianco, 2009).

The Management level network is an Ethernet or fiber-optic cable. It is generally considered that EM attacks on Ethernet cabling (Cat5, etc.) are most limited. Nevertheless, it is likely that given physical access to such a cable that it is possible to extract transmitted data; however, if the cable is in close proximity it would be far more practical to physically wiretap.

8.4 DEVICE LEVEL

8.4.1 Device Access Vulnerabilities (Physical)

Basics: The Field level and its devices are “monitoring” sensors (inputs) and “control” actuators (outputs). The Automation level Controller inputs and outputs bridge the gap between the physical field devices and the cyber domain (Wyman, 2017, p. 7). Field devices are spread throughout the facility, such as plant rooms, electrical enclosures, and within plant and equipment, generally connected via a twisted pair copper cable to the Automation level device Controller. Activators are generally Direct Drive Control (DDC) devices that control solenoids, valves, motors, fans, vents, etc. Sensors are generally system input devices that measure defined variables from their environment and transmit collected data to the Automation level devices such as temperature gauges, air pressure, etc., for decision-making.

Evaluation Description: The vulnerability of physical access to the Field level device will vary depending on the device and its environment. Actuators and valves will result in restricted vulnerabilities, because these are, in general, relatively simply devices controlling localized plant or equipment. Nevertheless, some electrical, gas, heating/cooling or process control activators could cause the loss of a utility, depending on the device and plant function. Issues such a denial of service of some building utilities should be considered.

Anand et al., stated that “sensor devices are typically vulnerable to physical comprise” (2005, p. 3). Such a view is appropriate, given that sensors are generally located across and within all parts of the facility. However, given their relatively isolated function, sensors will also result in restricted vulnerabilities. Again, these devices are in general relatively simple devices controlling localized facility plant or equipment; however, their inputs are transmitted to the Automation level.

Manipulation of Devices

Field devices may be both accessed and manipulated. For examples, sensor manipulation using components such as resistors to alter the value of a system input signal, resulting in a change to the monitored temperature may assist in the manifestation of an attack. Another may be the use of an independent power source, such as a battery, connected across an actuator valve to artificially increase an area's temperature, resulting in an incorrect value recorded at the Automation level.

Physically Disconnect

Another vulnerability is physically severing (disconnecting) the device from the Automation level Controller. Disconnection will result in the field device a) not providing an input signal (data) to the Automation level Controller and any resulting systems affect or b) the field device not receiving an output control signal. The Management level will generally not detect such disconnection, only shown as a loss to a device input. For most BACS to lose an individual sensor is not a significant vulnerability, but from a security perspective may be indicative of some form of developing threat event.

Destruction of Device

Physical access to a device could result in its damage or destruction. Therefore, the Automation level may lose inputs, such as a sensor, to detect intrusion or outputs, such as an actuating control valve for cooling. Removing the sensor's Automation level input degrades situational awareness across the building. This attack prevents the operator from issuing control command, resulting in denial of service (Wyman, 2017, p. 8) and lack of system oversight.

Security Sensor

Manipulation, disconnection or destruction for most sensors is not a significant vulnerability given their general isolated functionality. However, security sensors such as a passive infrared detector PIR), microwave, reed switches, etc., are now being connected as field device sensors into the Automation level. Automation level Controllers and the connection to field devices do not use tamper-indicating circuitry, as required by most intrusion detection systems. A tamper-indicating circuit provides a supervisory circuit on the connection point that detects and notifies a loss of alarm capability (Garcia, 2007, p. 339), such as an open, closed or bypass circuit attempt. Non-tamper or supervised connection points enable a low level technical defeat of sensors (security detectors) when connected via the BACS.

8.4.2 Connectivity Access Vulnerabilities (Physical)

Basics: The Field level devices are monitoring sensors and control actuators, directly connected to the Automation level Controller typically via twisted pair copper cable. Their connection is a simple control signal and low voltage power cable.

Evaluation Description: The vulnerability of physical access at the Field level device connectivity will vary between devices, from actuators to sensors. As with physical access to these devices (see 8.4.1 Physical Access), there are restricted vulnerabilities because these are relatively simply devices that control localized plant or equipment. However, some electrical, gas, heating/cooling or process control activators could cause the loss of a utility, depending on the device and plant function, or trigger actions to facilitate a more elaborate threat vector.

For example, the malicious code Stuxnet targeted specific industrial automation Programmable Logic Controllers (PLC), infecting files of the PLC program when running in Microsoft Windows (Karnouskos, 2011, p. 4491). A widely reported case was the attack on Iran's Nuclear plant that "destroyed roughly a fifth of Iran's nuclear centrifuges by causing them to spin out of control" (Kelley, 2013, p. 1), while outputting normal readings to monitoring equipment. PLCs are similar in application and function as Automation level Controllers.

Loss of Function

Disconnection, manipulation or destruction of both actuators and sensors will result in restricted vulnerabilities, because these have limited connectivity to the greater BACS. However, at the Field level some connectivity attacks could result in the loss of utilities, depending on the situation.

Monitoring

The connection between the Automation level Controller inputs or outputs and the Field device can be monitored. One such example is the application of a clamp meter, which displays whether there is a signal that determines which digital outputs are currently active. In addition, by stripping back the connection wiring, wiretapping of Field level devices can easily be gained. Connections between the Automation level Controller and the field device do not require authentication or have line monitoring (detection) capability. However, given the isolated nature of monitoring a field device, the data extracted will be limited.

Remote Control

Once a field device connection is wiretapped, it would be relatively simple to be able to control the device via the wiretap. For example, an actuator such as a valve could be driven "open" or "closed" with an additional power or control source. Nevertheless, as with monitoring, given the isolated nature of most field devices the ability to affect the greater BACS, plant or equipment is limited.

Spoofing Device

Field devices may be accessed and spoofed. The output and/or input of a device may be bypassed to spoof the actual device. Spoofing the device signal may use various methods, such as resistors or independent power source (battery). Spoofing will enable the manipulation of the value of the system's input signal, for example to alter the monitored temperature.

Security Sensor

Loss of function and spoofing for most sensors is not a significant vulnerability given their general isolated functionality. However, security sensors such as PIR, microwave, magnet reed switches, etc., are now being connected as field devices into the Automation level. In contrast to rated intruder alarm systems, Automation level Controllers and the connection to field devices do not use tamper-indicating circuitry. A tamper-indicating circuit provides a supervisory circuit on the connection line that detects and notifies a loss of alarm capability (Garcia, 2007, p. 339), such as an open, closed or bypass circuit attempt. Non-tamper or supervised connections enables a low level technical defeat of sensors (security detectors) when connected via the BACS.

8.4.3 Electromagnetic Emanation Attack

Basics: Field devices are generally connected to the BACS Automation level Controller by copper twisted cable, enabling an electromagnetic (EM) emanation attack (see Section 7.2.4 Electromagnetic Emanation Attack).

Evaluation Description: Field devices are generally connected to the Automation level device, Controller, by copper twisted cable that carries an electrical current. This medium could be vulnerable to EM attack, at its simplest if the device is on or off. Nevertheless, it is likely that given physical access to the device cable, it would be far more practical to physically wiretap. In addition, the device's functionality and locality will further reduce the threat.

8.5 GENERIC BACS MITIGATION STRATEGIES

Across the literature, BACS vulnerabilities are broad and at times abstract, presented without context (situation). Such abstraction results in vulnerabilities being difficult for practitioners to understand and mitigate against. Therefore, without context of the built environment and its facility, understanding the threat context and organizational functional criticality, mitigation strategies can only be generic (Table 8.3).

Table 8.3

Mitigation Strategies Overview

Mitigation Strategies
Management
Security Risk Management
Personnel Security
Procedural Security
Physical Security
Cybersecurity
Incident Response
Continuity Planning
Maintenance

The following generic mitigations strategies (Table 8.4) were tabulated to begin the development to achieve a risk approach, cognizant of the assessed threats and risks, and contextual considerations. It should be noted that these strategies are not presented in any order of importance or application.

Table 8.4

Mitigation Strategies

Category	Mitigation Strategy	Mitigation Strategy Description
Management	Security Policy	General Statement of Principle or Security Charter of overall intentions and directions expressed by the Board and Executive Management.
	Guideline	Guide or Basis for Design document that defines the expectation and strategies of security, and the processes that forms the function of security.
Security Risk Management	Security Risk Management Plan	Documented security risk management function that defines the risk principles, framework and processes, including roles, responsibilities, assessment, communication, and monitoring.
	Threat Assessment	Documented assessment to inform the security risk assessment through understanding the intent and capability of the attacker.
	Criticality Assessment	Documented assessment to inform the security risk assessment through identifying critical BACS functionality and equipment.
	Vulnerability Assessment	Documented assessment to inform the security risk assessment through identifying security weakness in the BACS protection system.
	Risk Assessment	Documented risk assessment of the security risk consequence and likelihood, informed by threat, criticality and vulnerability assessments.
Personnel Security	Personnel Security Program	Personnel security addresses the security program roles and responsibilities implemented from position recruitment to termination.

	Position Categorization	Assigns a risk designation to all positions that interact with BACS.
	Pre-employment Screening	Individuals are pre-screened prior to BACS access using a consistent vetting process, aligned with the risk designation of the assigned position. Screening may commence with Police and general background checks, to drug testing and federal checks.
	Personnel Roles	Employees, contractors and third-parties are provided with and accept expectations of conduct, duties, terms and conditions of employment, legal rights and responsibilities.
	Access Agreements	BACS authorization is gained prior to access being granted, including third-parties and contractors. Access is for a predetermined period only, requiring renewal on a defined frequency.
	Personnel Transfer	Review physical and logical access permissions to facilities and BACS, when individuals are reassigned or transferred to other positions within the organization.
	Personnel Termination and Exit Interviews	When an employee is terminated, their physical and logical access to facilities and BACS are revoked. Exit interviews ensure that individuals understand security constraints imposed by being a former employee and that proper accountability is achieved for all BACS related property.
	Contractors	Third-party and contractors shall meet all Personnel Security requirements as per employees to gain and maintain BACS access.
Procedural Security	Security Awareness and Training Program	Provide basic security awareness and training of general information to relevant users, operators and maintainers of BACS.
	Security Awareness and Training Records	Maintain a record of awareness and training for each user.
	Security Testing	Regularly test the knowledge of personnel on security policies and procedures, based on their roles and responsibilities, to ensure that they understand their responsibilities in securing the BACS, with a record of testing.
	Continuity restoration	Undertake practical exercises in security awareness briefings to simulate an actual BACS attack on a regular basis.
	Security Groups and Associations	Establish and maintain contact with external security groups and associations to stay informed with the latest security practices, techniques and technologies, and to share current security-related information including threats, vulnerabilities and incidents.
	Security Procedures	Detailed implementation instructions for carrying out security policy, presented as forms or list of steps to be taken prior to, during or after a security threat or incident.
	Access Control Procedure	Documented procedures in the control of authorized persons and objects into protected zones, Includes both physical and logical control access with the use and display of badges, access hours and levels of access, challenging non-badged persons, credential tampering and replacement.
	Incident Response Procedure	Documented procedures that addresses objectives, roles and responsibilities in the response to a routine or non-routine security incident or event, such as an intruder detection.

	Audit and Accountability Procedure	Documented audit and accountability security procedure that addresses objectives, roles and responsibilities for the audit and accountability of the security program. Defines auditable events and frequency, record keeping, action, monitoring and reporting.
	Emergency Evacuation Procedure	Documented process to addresses the objectives, roles and responsibilities for a facility or operation-specific evacuation.
	Continuity Procedure	Continuity of operations process addresses the capability to continue and/or resume operations of BACS in the event of disruption of normal system operation. Activities include objectives, roles and responsibilities, and activating the crisis management team.
	Recovery Procedure	Documented process to addresses the capability to recover BACS operations after an event that disrupts normal system operation. Activities include objectives, roles and responsibilities, resources and information to aid timely return to normal operations.
	Information and Document Management Procedure	Documented procedure that addresses objectives, roles and responsibilities in the protection of information and documentation. Includes scope, storage, maintenance, retrieval, handling, issue, retention and destruction of both digital and hardcopy documentation.
	Visitor and Escort Procedure	Documented process to addresses the objectives, roles and responsibilities in escorting contractors or third-party visitors.
	Use of Contraband Detectors Procedure	Documented process to addresses the objectives, roles and responsibilities in the use of contraband detection, training, evaluation and assessment.
	Staff Security Awareness Education	Documented process to addresses the objectives, roles and responsibilities in providing security awareness and training to users, operators and maintainers of BACS.
	Key Control Procedure	Documented procedure for the control of the lock and key system, including key cutting, issue, storage, maintenance and accountability.
	Preventive Maintenance Procedure	Documented routine and preventive BACS maintenance, including local and remote maintenance tools and maintenance personnel.
Physical Security	Physical Security Program	The system of physical control barriers to allow only authorized persons, vehicles and materials to gain access to a protected zone. Includes physical delay and detection strategies. Physical strategies are designed to safeguard people, prevent unauthorized access to equipment, facilities and material; and to safeguard against a security incident.
	Security Zones	Articulation of areas or zones in a site and facility, commensurate with the security level where the BACS resides. Security zones provide a methodology for the application of physical and logical security mitigation strategies.
	Physical Barrier	A natural or man-made obstacle to the movement/direction of persons, vehicles or materials. Barriers include floor, walls, ceiling or roof, and portals.
	Portal Control Barrier	The control of persons, vehicles or materials through the physical barrier.

	Physical Openings (in Barrier)	Openings including windows, ducts or vents, utility or service tunnels, sewers and other drains. Where such openings exceed 96 square inches or 620 square centimetres, openings should be fortified with steel bars or grills.
	Container (utilities)	A physical enclosure to hold and protect BACS equipment.
	Seal	Seal to detect tamper or manipulation of a portal, such as a container door or enclosure lid.
	Access Control (Physical)	The system for the physical control of authorized persons, vehicles and materials through the implementation of security measures for a protected area.
	Portal Control Barrier	The control of authorized persons, vehicles or materials through the physical barrier.
	Mechanical Access Control (key control)	Lock and key system, includes door locks, cabinet locks and padlocks. In a master key system, a single key operates a series of mechanical locks, and each of those locks is also operated with another key specific to that lock. Validates one credentials in the form of something you have.
	Electronic Access Control	Validates one or more credentials, which can be in the form of something you know, are or have. Includes a credential reader, communication network, controller, central database, software and applications for request-to-exit devices for applicable doors
	Contraband Detection	Contraband consists of prohibited items, such as weapons, explosives, drugs, digital storage medium, cameras or tools. Includes metal detectors, X-ray machines, etc.
	Intrusion Detection	A system designed to detect and signal the presence, entry or attempted entry of a person or object in a protected zone.
	Intrusion Detection System	An electronic system of sensors, controls and annunciators (devices that announce an alarm via sound, light or other means) arranged to detect and signal the presence, entry or attempted entry of a person or object into a protected zone without authorization.
	Alarm Communication and Display	An electronic system that signals the presence, entry or attempted entry of a person or object into a protected zone, showing detection location.
	Security Detector	A sensor designed to detect and signal in response to the presence of intrusion, an attempted intrusion, breach or entry into a protected zone. Detectors include position, motion, sound, vibration, heat, temperature or capacitance sensors, and include line and fault monitoring.
	Tamper Detection	A sensor designed to detect and signal in response to an unauthorized interference or attempted interference to a protected enclosure.
	Uninterruptable Power Supply	Provides continuous power to an alternating current line within prescribed tolerances to protect against loss of primary power or intermittent brownouts.
	Video Surveillance (Physical)	The observation of a location, activity or person through persons, technology or other means.
	CCTV	A system in which a surveillance signal is transmitted to monitors and/or storage devices, and control equipment to observe a location, activity or person.

	CCTV Monitoring and Review	CCTV is primarily used to detect activities that require a security response, collect images of an incident for later review and/or evidence, and assist with post-incident assessment. Field of view or camera coverage extends from entry/exit points; full perimeter; internal access control portals; and integration with the access control system.
	Technical Surveillance Counter Measures	Physical and technical surveillance to provide an appropriate level of assurance, commensurate to the information risk, that sensitive information is free from unauthorized surveillance.
Cybersecurity	Access Control (Logical)	The system for the logical control of authorized persons to access BACS resources through the implementation of procedural and technical security measures.
	Account Management (Logical)	Manage BACS access to specifying account types, access rights and privileges, including authorizing, establishing, activating, modifying, disabling and removing accounts.
	Identification and Authentication	Process of verifying the identity of a user, process or device, as a prerequisite for granting BACS access. Process defines initial authentication credential, such as defining password length and composition, lost, compromised or damaged authentication credentials, revoking authentication credentials, changing authentication credentials on a defined frequency, and specifying measures to safeguard authentication credentials.
	Information Flow Enforcement	Regulate and enforce assigned authorizations for controlling the flow of information within BACS and between interconnected BACS. Specific examples of flow control enforcement can be found in boundary protection devices i.e., proxies, gateways, firewalls and routers that employ rule sets or establish configuration settings that restrict BACS services or provide a packet-filtering capability.
	Access Control Restrictions	Design and implementation controlled and monitored access to BACS from the organization's enterprise network.
	Remote Access Control	Remote access to BACS is controlled, monitored and managed through authenticated access to protect the confidentiality and integrity of external access sessions. Access is limited to a restricted number of managed access control points.
	Monitor and Audit Access Control	Monitor and notification of unauthorized use, connections or changes to the BACS, including scanning for unauthorized wireless access points on a defined frequency and taking appropriate action if an unauthorized connection is detected.
	Passwords	Develop and enforce BACS procedures concerning the generation and use of passwords that stipulate rules of complexity, based on the criticality level of the BACS to be accessed. Passwords shall be changed regularly and are revoked after a period of inactivity.
	Least Privilege	Assigns the most restrictive set of rights and privileges or access needed by BACS users for the performance of specified tasks; and configures BACS to enforce the most restrictive set of rights and privileges or access needed by users.

	Unsuccessful Login Attempts	Enforce a limit of consecutive invalid BACS login attempts during a defined time period. Due to potential for denial of service, automatic lockouts shall be temporary, automatically released after a predetermined time period.
	Session Lock and Remote Termination	Prevent BACS access by initiating a session lock after a defined time period of inactivity or receiving a request from a user; and terminate a remote session at the end of the session or after a defined time period of inactivity.
	Wireless Access Restrictions	Establish user restrictions and implementation guidance for wireless technologies, and authorize, monitor and manage wireless BACS access.
	Portable and Mobile Devices	Establish usage restrictions and implementation guidance for organization controlled mobile devices, including the use of writeable, removable media and personally owned removable media. Includes authorizing connection of mobile devices, monitoring for unauthorized connections of mobile devices and enforcing requirements for the connection of mobile devices to BACS.
	Intrusion Detection (Logical)	A system designed to software detect and signal the presence, entry or attempted entry of a logical intrusion in a protected zone.
	Information Integrity Monitoring	Monitor events on BACS to detect and signal logical attacks, unauthorized or attempted unauthorized activities or conditions. Monitoring capability may be achieved through a variety of tools and techniques, such as intrusion detection systems, malicious code protection software, log monitoring software, network monitoring software and network forensic analysis.
	Information Integrity Response	A process that notifies a predefined list of incident response personnel, in real-time, when indications of a compromise or potential compromise.
	Information and Communication Protection Plan	Documented plan to physical and logical separate the BACS network from other networks.
	Partition Networks and Functions	Partition BACS communication network services and management functionality. Isolate security functions from non-security functions.
	Information and Document Management	Sensitive digital and hardcopy BACS information that requires protection. BACS design, operations, procedures, risk management, business impact, criticality and threat assessments, etc., may contain sensitive information. This information must be protected and verified that the appropriate versions are retained.
	Program Backup	The BACS software program has certified and validated stored backup on a defined frequency.
	Information Destruction	Controlled disposal and/or destruction of information and documentation commensurate with the assigned security level of the information, both digital media and hardcopy.
	Security Authorization Plan	A documented process where connections made to the BACS network, Controllers or other devices, both physical and logical, are authorized and documented.
	Security Authorization Monitoring	Monitor and audit connections on an ongoing basis, verifying enforcement of documented security requirements.
	Audit and Accountability	Periodic audits and logging of the BACS to validate that the security strategies are operating as intended. Security audits review and examine records and activities to determine the adequacy of BACS security requirements

		and to ensure compliance with established security policy and procedures.
Incident Response	Incident Response Plan	Addresses the capability and processes to respond to either a routine or non-routine event, such as an intruder detection activation or other disruption. The plan defines the roles and responsibilities of employees, contractors and third-parties in the event of an incident, including incident detection, identification, containment, mitigation, reporting and recovery processes.
	Incident Response Training	Personnel are trained and exercised in their incident response roles and responsibilities with respect to the BACS, receiving refresher training on a defined frequency.
	Incident Post-investigation	Documented procedure to post-event investigation and analyse incidents, to ensure that lessons are learnt and BACS mitigation strategies improved.
Continuity Response	Continuity Response	An implemented continuity plan in case of BACS failure, disruption, compromise or loss of service, to enable the system to return to normal operations in a timely manner.
	Continuity Response Plan	Develop and document a continuity plan to maintain or re-establish BACS operations after a disruption or failure. Consider the implementation of a controlled, audited and manual override of automated mechanisms in the event of emergencies.
	Continuity Response Training and Testing	Train personnel in their continuity of operations roles and responsibilities with respect to BACS, providing refresher training. Undertake practical exercises in restoring BACS security.
	Recovery and Reconstitution	Provide the capability to recover and reconstitute the BACS to a known secure state after a disruption, compromise or failure. BACS recovery and reconstitution means all parameters are set to secure values, security-critical patches and configuration settings are re-established; application reinstalled and configured, information from the most recent, known secure backups is loaded and the BACS tested.
	Alternate Information Storage Site	BACS backups and transfer of backup information to an alternate storage site are performed on a defined frequency.
	Alternate Control Centre	Identify an alternate control center, with necessary telecommunications, and initiates any necessary agreements to permit the resumption of BACS operations for critical functions within a prescribed time period when the primary control center is unavailable.
	Continuity Post-investigation	Documented procedure to post-event investigation and analyse incidents, to ensure that lessons are learnt and BACS continuity strategies improved.
Maintenance	Maintenance Program	Maintenance activities encompass procedures for performing routine and preventive BACS maintenance, including the use of both local and remote maintenance tools and management of maintenance personnel.
	Maintenance Plan	Maintenance activities include routine, scheduled maintenance and repairs, and unplanned maintenance controlled whether performed on-site or remotely. Maintenance that require the physical access or removal of any BACS device or change of programming needs to be documented, listing the date, time, reason for

		removal/change, estimated date of reinstallation, and personnel.
	Maintenance Personnel	Third-party or contractor maintenance personnel shall meet all Personnel Security requirements as required by employees to gain and maintain BACS access. Only trusted maintainers to access the BACS, achieved by documented authorization and approval procedures. Non-approved maintenance personnel to be supervised by appropriate personnel.
	Asset Tracking	Manual or electronic logging of all BACS devices and equipment, with location.
	Configuration Management	A documented process to ensure that only approved changes to the BACS are made, which are planned, applied, documented and audited. Only tested and approved changes should be allowed, where vendor updates, patches and devices are thoroughly tested with baseline configuration, change control and monitoring.
	Legacy Upgrades	Documented plan to monitor and upgrade existing BACS legacy, including security mitigating measures commensurate with the organization's and BACS risk tolerance.
	Removal and Disposal	Controlled disposal of latent memory storage devices, information or other data. Implement procedures to address the addition, removal and disposal of all BACS equipment, where devices and information are documented, identified, and tracked so that their location and function are known.

8.5 CONCLUSION

The Building Automation and Control System (BACS) Management level provides the human interface and system functionality. The Management level is generally an information system software package, located and alongside many other business systems within the corporation's Information and Communication Technology (ICT) network. In contrast, the Field level provides connectivity from the many field devices to the Automation level Controllers. The field devices are spread throughout all parts of the facility, and provide the monitoring and control functions. However, both elements are vulnerable to attacks against the confidentiality, integrity and availability of data.

Both BACS architectural levels include hardware and software elements, and therefore have vulnerabilities associated with each of these elements. Given the quite different technologies, functionality, processing capability and communications connectivity, vulnerabilities of these elements are diverse. The Management level evaluated vulnerabilities include physical and network access to the workstation, cyberattack, destruction of device, wiretapping, device insertion and electromagnetic emanation attack. The Field level vulnerabilities include physical and network access with manipulation of devices, physically disconnect or destruction, security sensors (detectors), loss of function, monitoring and control of devices, spoofing device outputs and electromagnetic emanation attack.

Unlike the BACS Automation level, both the Management and Device levels are less prone to embedded vulnerabilities that can be exploited by interlopers. At the Management level, this is in part due to the ICT network and resulting corporate cybersecurity. At the Field level, devices are isolated and realized vulnerabilities result in limited impact. As with all ICT systems, generic mitigation strategies for managing the vulnerabilities that pose a risk exist, focused towards maintaining the confidentiality, integrity and availability of network data.

Section 9. Stage 2 Survey of Understanding

9.1 INTRODUCTION

Building Automation and Control Systems (BACS) are becoming embedded into todays' built environment and this impacts on many departments, groups or persons in an organization. To gain an understanding of security and facility professional's awareness and understanding, surveys were developed and sent to security and facility professionals. This section presents the analysis of the collected survey data and interpretation in response to the posed project questions and resulting sub-questions.

9.2 ANALYSIS & INTERPRETATION

In order to understand practitioner perspectives of BACS vulnerabilities, an online survey consisting of 18 questions was sent to 13,803 security and facility professionals from ASIS International, BOMA and SIA membership (Table 9.1). The survey received a response from a total of 331 participants, with a response rate of 2.4 percent.

The online survey used the term "building owners and operators". For ease and consistency of reading throughout the Report, the term "facility professional" is used; however, to align with the posed survey and developed sub-questions, the use of building owners and operators has been maintained. In the context of this section, these terms are considered to be interchangeable.

Table 9.1

Association Distribution and Response Rates

Body	Distributed	Response[1]	Rate (%)
ASIS	5379	240	3.06%
SIA	2469		
BOMA	5955	91	1.53%
Overall	13,803	331	2.40%

Note 1: Body allocation was based on job function, resulting in the combination of security functions of ASIS and SIA members.

Respondents categorized themselves according to their job function, revealing that 40 percent of respondents were security practitioners, 28 percent building owner or operators and 21 percent consultants, with 11 percent identifying with other job functions (Figure 9.1).

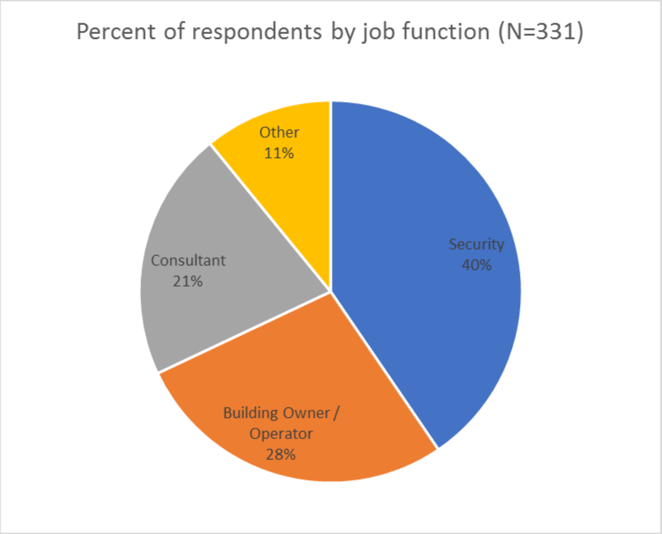


Figure 9.1. Percent of Respondents by Job Function

Extending from the project's primary Research Objectives, Stage 2 sub-questions were developed (see Section 2.3.4 Survey Data Analysis and Table 2.1) that aligned with the posed survey questions. The analysed survey data facilitated a response to these sub-questions, resulting in a later response to the Research Objectives.

9.2.1 Security & Building Professionals Awareness

The Stage 2 sub-question asked: *Are security and building owner/operator professionals aware of the threat and risks associated with BACS?*

The collected data indicated that two-thirds (75%) of respondents believed that they had an awareness of BACS architecture (Figure 9.2). BACS architecture comprises of the various hardware and logical levels of the system, being Management, Automation and Field devices.

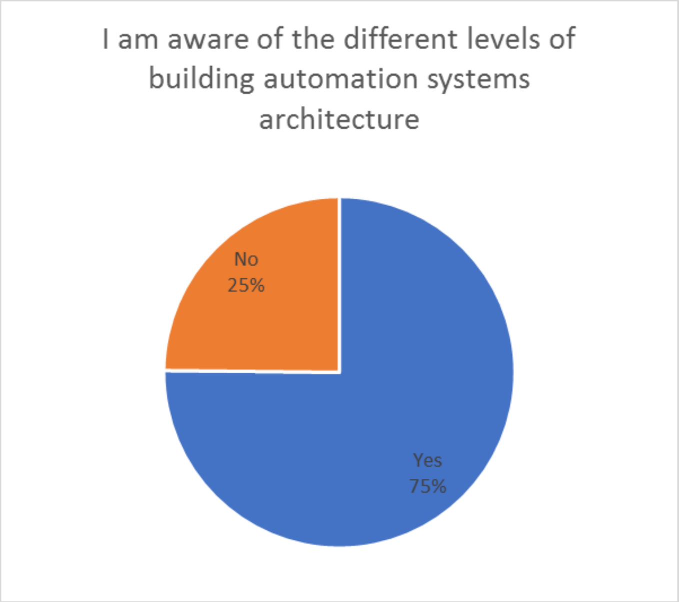


Figure 9.2. Awareness of BACS Architecture

Such awareness was further supported by the overall median understanding of the three BACS architecture levels, which was reported as being "somewhat high". Furthermore, 45 percent of the respondents stated that BACS vulnerabilities are included in their group risk register. The inclusion of BACS into a risk register was reported by 27 percent of building owner/operators and 41 percent of security professionals (Figure 9.3).

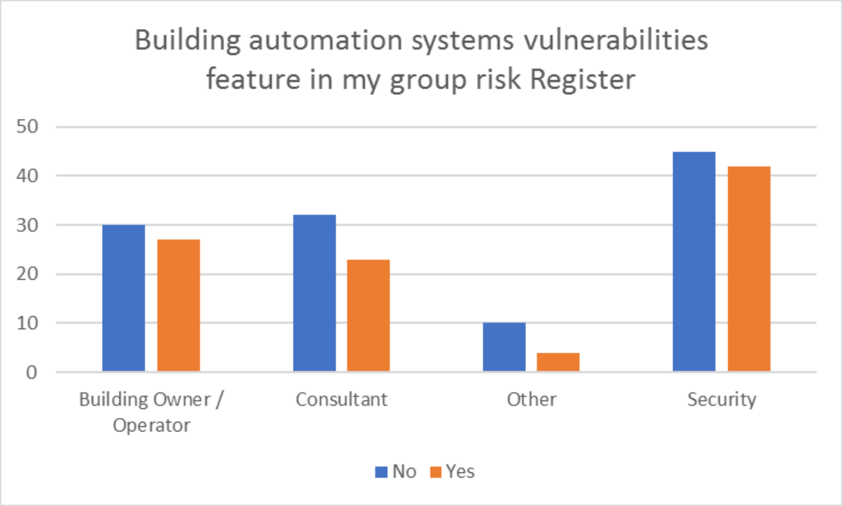


Figure 9.3. Risk Register and BACS

Nevertheless, such high level of confidence in awareness and an almost 50 percent inclusion of BACS vulnerabilities in risk registers was contradicted by the mean responses to the criticality of BACS vulnerabilities across the Automation, Management, and Field levels.

The contradiction is displayed in Figure 9.4. To simplify responses, the Likert measures of "Very High" to "Medium-High" significance were categorized as Significant, whereas "Medium" to "Low" significance were categorized as Not Significant for this analysis.

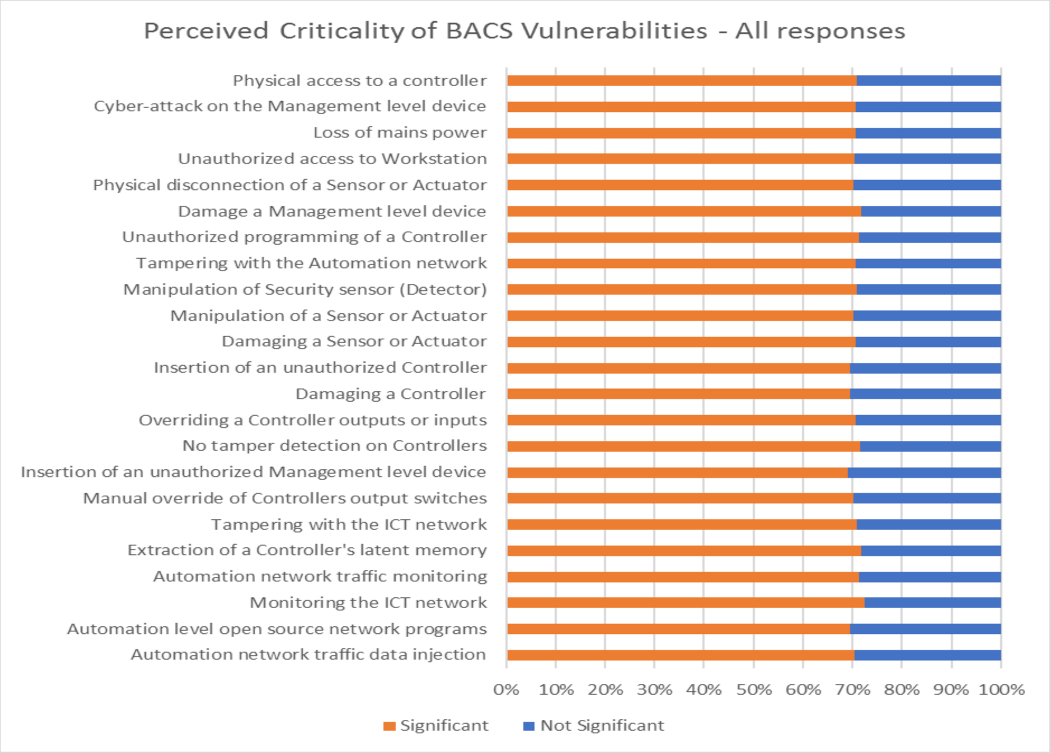


Figure 9.4. Perceived Criticality Significance of Automation, Management and Device Levels of BACS Vulnerabilities

Figure 9.4 indicates that BACS vulnerabilities were viewed as being of relatively equal criticality across all three levels of architecture. In addition, that there was little or no difference (M = 5.82 to 4.81) between the proposed vulnerabilities (Table 9.2). Despite 75 percent of respondents reporting they had an awareness of BACS architecture, the neutral (and arguably inappropriate) responses to the question of critical BACS vulnerabilities suggest that respondents did not understand the criticality of the BACS vulnerabilities.

Table 9.2

Overall Median and Mean Perceptions of Significance of BACS Vulnerabilities

BACS Vulnerabilities	**Median**	**Mean**	**SD**
Cyberattack on the Management level device	7	5.82	1.73
Unauthorized access to workstation	6	5.52	1.76
Unauthorized programming of a Controller	6	5.46	1.79
Tampering with the ICT network	6	5.43	1.66
Tampering with the Automation network	6	5.40	1.85
Insertion of an unauthorized Management level device	6	5.33	1.88
No tamper detection on Controllers	6	5.33	1.87
Overriding a Controller outputs or inputs	6	5.29	1.80
Manipulation of Security sensor (Detector)	6	5.28	1.82
Insertion of an unauthorized Controller	6	5.26	1.97
Physical access to a controller	6	5.23	1.89
Manual override of Controllers output switches	6	5.19	1.84
Automation level open source network programs	6	5.16	1.75
Manipulation of a Sensor or Actuator	5	5.09	1.71
Monitoring the ICT network	6	5.06	1.85
Loss of mains power	6	5.06	2.03
Extraction of a Controller's latent memory	6	5.05	1.84
Damaging a Controller	6	5.02	1.83
Automation network traffic monitoring	6	5.01	1.77
Damage a Management level device	6	4.99	1.79
Automation network traffic data injection	5.5	4.98	1.89
Physical disconnection of a Sensor or Actuator	5	4.81	1.88
Damaging a Sensor or Actuator	5	4.81	1.76

The lack of differentiation between the criticality of various BACS vulnerabilities also persisted within the job function groups, although some differences were found in the significance weighting between these groups (Table 9.3). Such variance suggested culturally defined differences in the perception of BACS between the various professional groups.

Table 9.3

Differences between Perceptions of BACS Vulnerability Significance by Job Function

Job Function	% of respondents indicating all vulnerabilities are critical	% of respondents indicating vulnerabilities are not critical
Building owner/operators	59%	41%
Consultants	41%	59%
Security	33%	67%

Greater accuracy in the perception of the BACS vulnerabilities was, however, found to be held by the more technical practitioners (Table 9.4). This group included integrators and cybersecurity professionals, making up an expert group (n=10) who demonstrated an awareness of the different levels of criticality of BACS vulnerabilities. This group's mean perceptions of the criticality of the different BACS vulnerabilities aligned with the findings from the project's Stage 1, which concluded that the greater risks lie in the Automation level with the BACS Controller.

Table 9.4

Expert Group Mean Perceptions of Significance of BACS Vulnerabilities

Building Automation System Vulnerabilities	Median	Mean	SD
Manual override of Controllers output switches	6	5.14	1.73
Physical access to a controller	5	4.29	1.83
Tampering with the Automation network	5	4.14	2.29
Automation network traffic monitoring	5	4.86	1.96
Automation network traffic data injection	5	4.71	1.48
Automation level open source network programs	5	4.43	1.99
Unauthorized access to Workstation	5	3.43	2.13
Insertion of an unauthorized Management level device	5	3.86	2.03
Extraction of a Controller's latent memory	4.5	3.83	2.11
No tamper detection on Controllers	4	3.86	1.96
Insertion of an unauthorized Controller	4	3.71	1.91
Unauthorized programming of a Controller	4	3.29	2.05
Loss of mains power	4	3.71	2.49
Damage a Management level device	4	3.29	1.67
Tampering with the ICT network	4	3.43	2.19
Monitoring the ICT network	4	4.14	1.88
Manipulation of a Sensor or Actuator	4	3.14	1.88
Physical disconnection of a Sensor or Actuator	4	3.86	1.55
Overriding a Controller outputs or inputs	3	3.14	2.10
Damaging a Controller	3	3.00	1.93
Damaging a Sensor or Actuator	3	3.71	1.83
Manipulation of Security sensor (Detector)	2	2.57	1.76

In response to the sub-question *Are security and building owner/operators professionals aware of the threats and risks associated with BACS?* the survey found a disconnect between respondents' expressed understanding of these issues, and their revealed understanding. Although 75 percent of security and builder operator professionals claimed to have an awareness of BACS architecture, and 48 percent feature BACS vulnerabilities in their group risk register, the majority of security and builder operator professionals displayed a limited understanding of the criticality of BACS vulnerabilities.

The exception to this limited understanding was found among Integrators and Cybersecurity professionals, who displayed a high level understanding of the criticality of BACS vulnerabilities. Their perceptions of critical BACS vulnerabilities correctly identified the greater risks as laying in the BACS Automation level Controller, a view which concurs with the Stage 1 findings.

9.2.2 Level of Professional Responsibilities

The Stage 2 sub-question asked: *What level of responsibility do security and builder owner/operator professionals have with BACS?*

When respondents were asked whether they are responsible for a BACS, the overall level of responsibility was found to be low, with only 15 percent of all respondents indicating that they have responsibility for a BACS. Consequently, 85 percent of all respondents were not responsible for BACS. Among those indicating that they are responsible for a BACS were 36 percent of all building owner/operators surveyed, 10 percent of all security professionals surveyed, and 1.5 percent of all consultants. These results indicated that there was little direct responsibility for BACS within the sample, and given that 75 percent of respondents claimed some awareness of BACS architecture, this suggested greater use than responsibility among the surveyed professionals.

The finding of a low level of BACS responsibility within each job function group was supported by the additional finding that 33 percent of all building owner/operators surveyed, and 7 percent of all security professionals surveyed, indicated that they:

a. Regularly discuss potential vulnerabilities within their BACS with other managers;
b. Regularly work with, manage, oversee, or make recommendations relating to a BACS; or
c. Regularly provide protective advice in regard to BACS vulnerabilities.

Together, these findings indicate that responsibility for BACS are largely outside security professionals' responsibilities, although the results do suggest some BACS responsibilities lying with building owner/operators.

Therefore, in response to the sub-question *What level of responsibility do security and builder owner/operator professionals have with BACS?*, the analysis indicted that building owner/operator professionals have a greater level of BACS responsibilities than security professionals, however, overall there is greater use of BACS than direct responsibility among the surveyed professionals.

9.2.3 Security Integration into BACS

The Stage 2 sub-question asked: *What is the degree of security systems integration into BACS?*

When the reported degree of security system integration into BACS was examined, the results indicated that 51 percent of respondents to the question had some security systems integration. Those reporting security system integration into BACS comprised of 52 percent security professionals, 24 percent consultants and 19 percent building owner/operators.

Although this finding suggested that there is currently a reasonable level (50%) of security systems integration into BACS, the data provided limited understating of the level of security integration. Of concern was the difference in the perceptions of the level of security system integration between the security professionals (52% reporting integration) and building owner/operators (19% reporting integration). These differences further support the suggestion of culturally defined differences arising from occupational perspectives of BACS.

It may also be asserted that the different groups and individuals in each group view integration quite differently. For example, is single data entry for staff that propagates through the enterprise systems into the ability to issue a security access card considered to be integration? This outcome highlights definitional and semantic issues which make the ability to define BACS problematic.

Therefore, in response to the sub-question *What is the degree of security systems integration into BACS?*, the study found that half of all reported BACS had integrated security systems. Although such security systems integration into BACS is likely to significantly increase in the future, the ability to define BACS is problematic and may lead to differing interpretations and perceptions of the level of security system integration between different job functions.

9.2.4 Security Systems Integration into BACS

The Stage 2 sub-question asked: *What type of security systems integrate with BACS?*

Respondents who reported security systems integration into their BACS were then asked about the types of security systems used. The systems reported as being integrated into BACSs were found to differ between the job function groups, further suggesting a culturally defined focus on different aspects of either BACS and/or security sub-systems. For example, security professionals primarily reported duress (62%), intruder alarm (60%), CCTV (51%) and electronic access control (51%) as being the most common integrated security systems. Whereas, building owner/operator professionals primarily selected other (60%), and reported non-security related systems such as HVAC, fire systems and lift control. Consultants focused on incident reporting (53%), radios (50%) and intercom systems (48%) (Table 9.5) and in general, provided a median response between the other professional groups.

Table 9.5

Security Systems Reported as Integrated with BACS by Function

	Building Owner/Operator	Consultant	Security	Total
Electronic access control	19%	31%	51%	**26%**
CCTV	14%	35%	51%	**19%**
Intruder alarm	11%	29%	60%	**13%**
Security lighting	19%	41%	39%	**15%**
Duress	8%	29%	63%	**9%**
Incident reporting	7%	53%	40%	**6%**
Intercom	24%	48%	29%	**8%**
Radios	17%	50%	33%	**2%**
Other[1]	60%	40%	0%	**2%**

Note: 1. *Other systems reported: HVAC, fire systems and lift control*

The sub-systems of duress (8% to 63%; 52), intruder alarm (11% to 60%; 49), CCTV (14% to 51%; 37) and electronic access control (19% to 51%; 32) had a broad perception of what was "integrated" into BACS between the professional groups. Such variation in the understanding of security system integration into BACS, based on job function type and responsibility, indicates that integration means different things to different BACS users. As such, the data provides a limited understating of the level of security integration into BACS.

Therefore, in response to the sub-question *What type of security systems integrate with BACS?*, the survey found that there are diverse views on what types of security sub-systems integrate into BACS, defined by the professional group being asked. Security professionals cited the most common BACS integrated security system as duress, intruder alarm, CCTV and electronic access control. However, building owner/operator professionals cited intercom, electronic access control, lighting, radios and CCTV as the most common BACS integrated security systems. The understanding of integration between security and builder owner/operator professionals lacks definition, likely leading to misunderstanding.

9.2.5 Most Critical BACS Vulnerabilities

The Stage 2 sub-question asked: *What do security and builder owner/operator professionals consider are the most critical BACS vulnerabilities?*

When respondents were asked to rate the criticality of 23 BACS vulnerabilities, the mean criticality rating of each vulnerability was relatively equal. As discussed earlier, although two-thirds of respondents indicated an awareness of BACS architecture (see Figure 9.2), this was contradicted by the overall mean responses to the criticality of different vulnerabilities across the BACS Automation, Management and Field device levels (see Figure 9.4).

To assess the mean critical significance of each vulnerability, the data was first reverse-scored so that higher means equated with higher significance ratings. The results indicated a perception of equivalence of criticality for all BACS vulnerabilities, which also persisted when each job function group was examined individually. For example, approximately 60 percent of building owner/operators in the simplified 2-scale analysis rated all vulnerabilities as significant (Figures 9.5 and 9.6), followed by 40 percent of consultants (Figures 9.7 and 9.8) and 30 percent of security professionals (Figures 9.9 and 9.10). Charts for this analysis were created to show both the 7-point Likert scale assessment as well as by the simplified 2-scale assessment (where the Likert measures of “Very High” to “Medium-High” significance were categorized as Significant, and the “Medium” to “Low” significance measures were categorized as Not Significant).

These results (Figures 9.5 to 9.10) display how each professional group provided a homogenous rating to all BACS vulnerabilities. This perception of equality of vulnerabilities demonstrates a lack of understanding of which BACS hardware or software is likely to be more or less vulnerable than other parts. Importantly, it indicates a lack of understanding of which parts of the BACS architecture are more critical to maintain operations, and may therefore require greater protection.

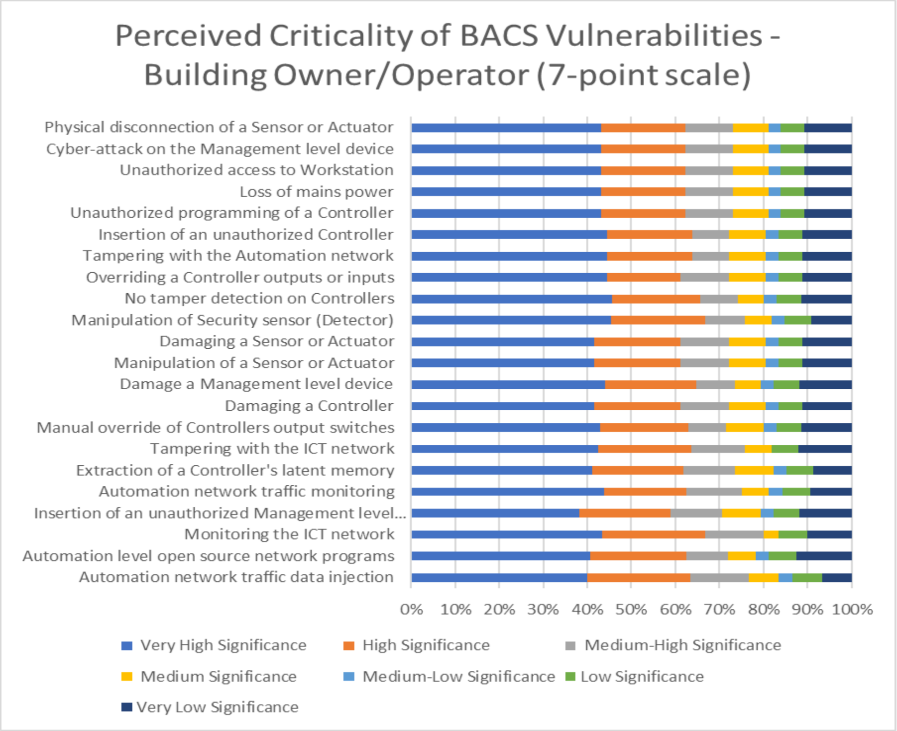


Figure 9.5. Perceived Criticality Significance of BACS Vulnerabilities: Building Owner/Operators (7-point Likert scale)

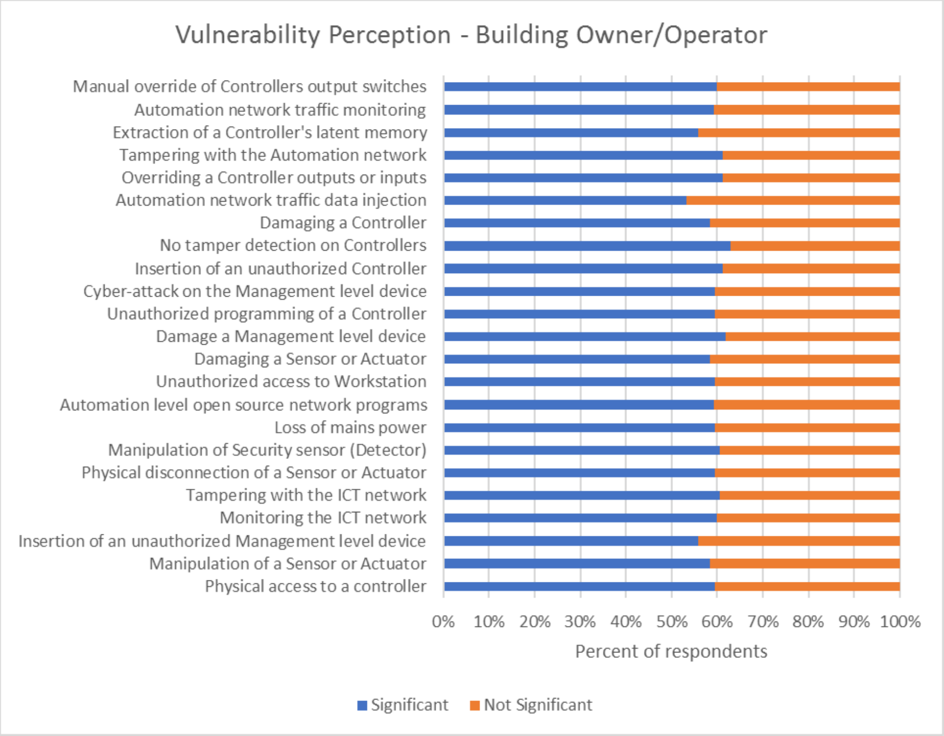


Figure 9.6. Perceived Criticality Significance of BACS Vulnerabilities: Building Owner/Operators (Simplified)

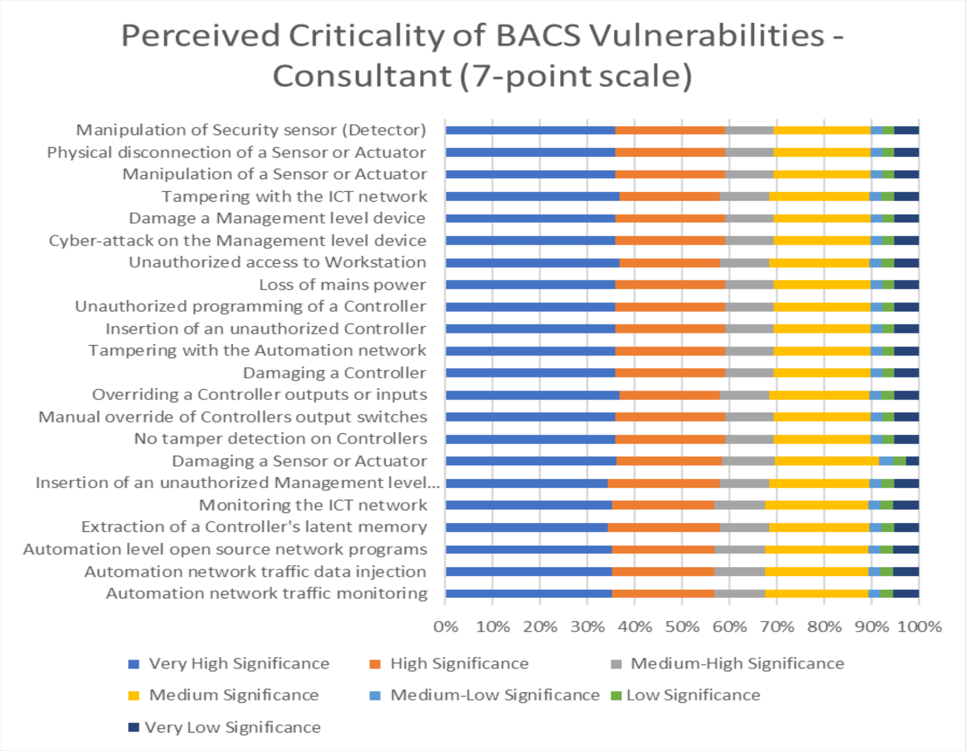


Figure 9.7. Perceived Criticality Significance of BACS Vulnerabilities: Consultants (7-point Likert scale)

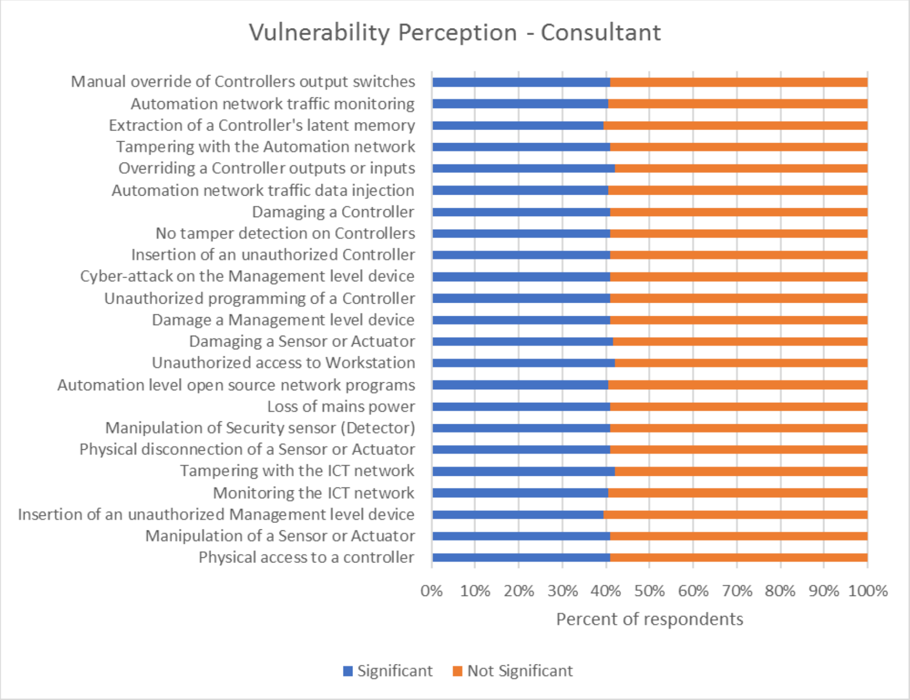


Figure 9.8. Perceived Criticality Significance of BACS Vulnerabilities: Consultants (Simplified)

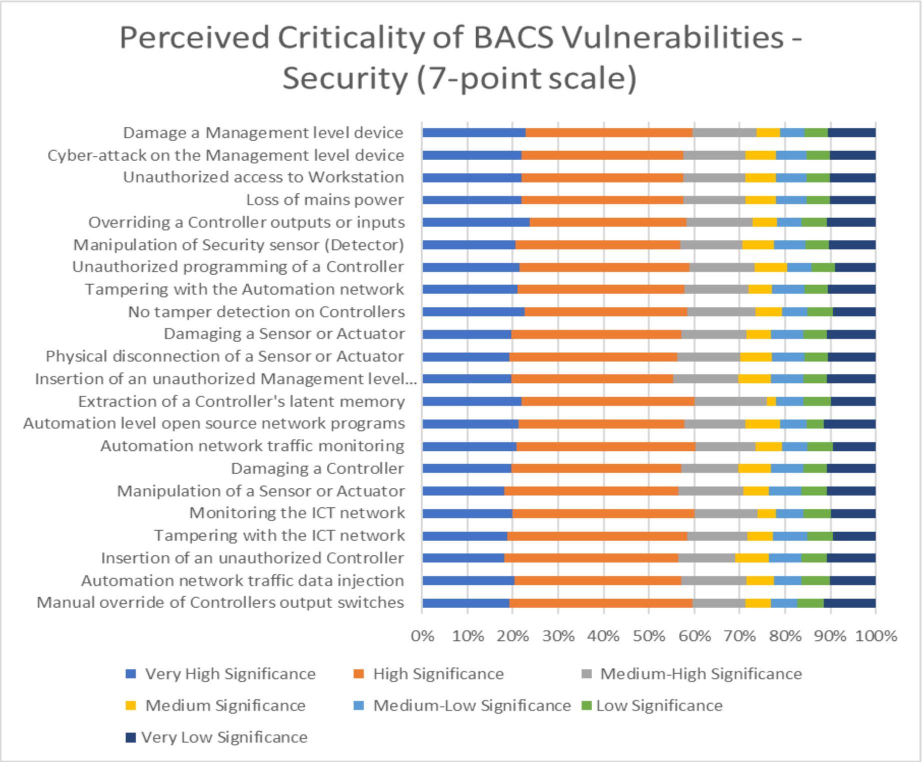


Figure 9.9. Perceived Criticality Significance of BACS Vulnerabilities: Security (7-point Likert scale)

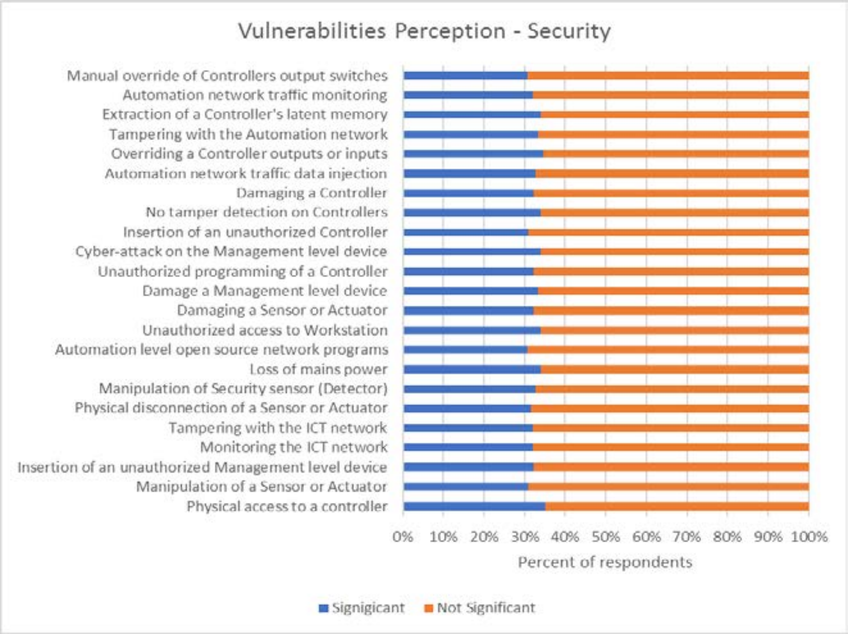


Figure 9.10. Perceived Criticality Significance of BACS Vulnerabilities: Security (Simplified)

Expert BACS Group

The expert group, consisting of cybersecurity professionals and integrators, provided criticality ratings of the 23 BACS vulnerabilities which showed a greater awareness of the variation in the criticality of BACS vulnerabilities (Figures 9.11 and 9.12). As Figure 9.12 indicates with its trend line, unlike the other job function group figures, there is a distinct difference between the most significant and least significant critical vulnerability.

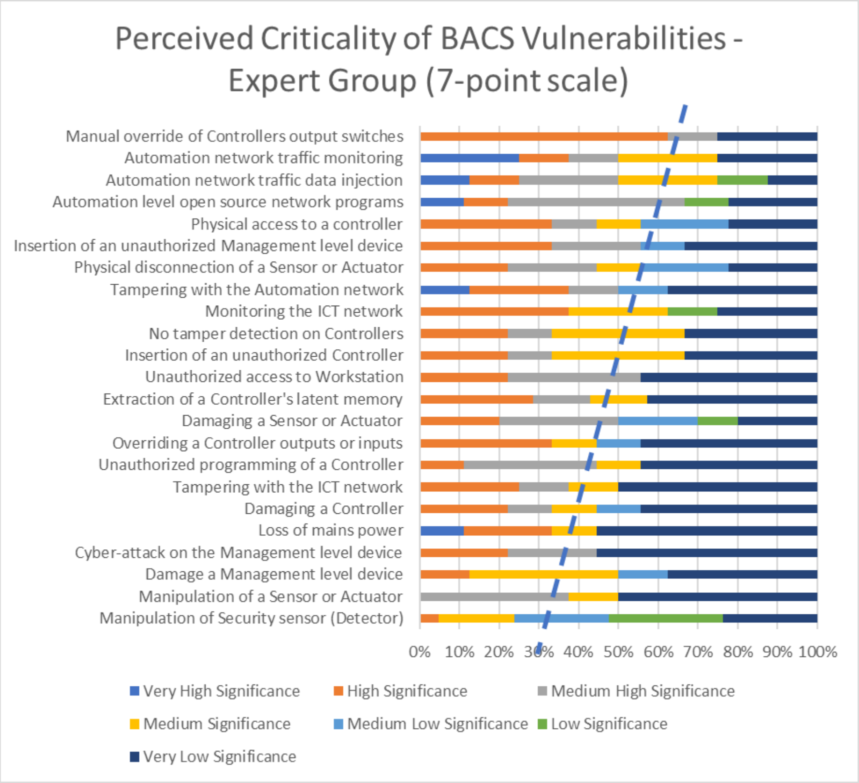


Figure 9.11. Perceived Criticality Significance of BACS Vulnerabilities: Expert Group (7-point Likert scale)

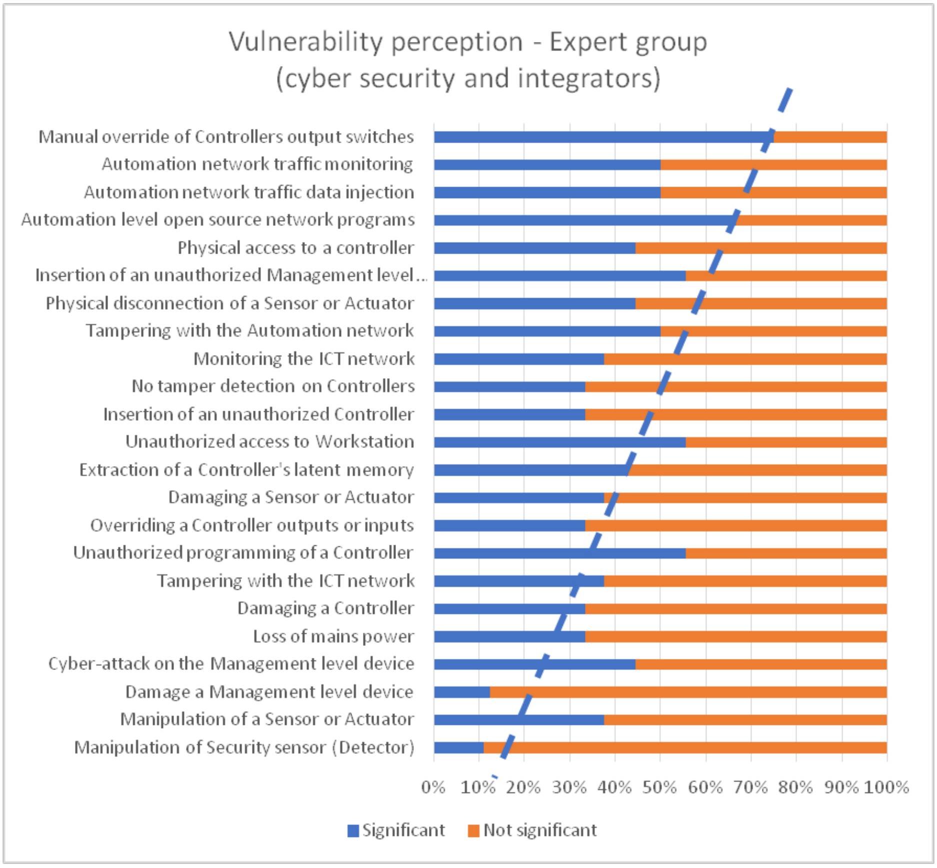


Figure 9.12. Perceived Criticality Significance of BACS Vulnerabilities: Expert Group (Simplified)

Examination of the mean and median criticality of each vulnerability (Table 9.6) revealed that the expert group, consisting of integrators and cybersecurity professionals, demonstrated the greatest level of awareness of BACS vulnerabilities. For example, rating manual override of Controllers output switches as most critical vulnerability. Security professionals and consultants, however, cited cyberattack on the Management level device as the most critical BACS vulnerability, while building owner/operators cited tampering with the Automation level network.

Table 9.6

Mean and Median Ratings of the Level of Criticality of BACS Vulnerabilities by Function

		All			**Security**			**Building Owner/Operator**			**Consultant**			**Expert Group**		
Level		***Mean***	***Median***	***SD***	***Mean***	***Median***	***SD***	***Mean***	***Median***	***SD***	***Mean***	***Median***	***SD***	***Mean***	***Median***	***SD***
Management	Cyberattack on the Management level device	**5.82**	**7**	*1.73*	**5.90**	**6.5**	*1.67*	5.97	7	*1.68*	**5.80**	**6.5**	*1.63*	3.00	1	*2.26*
Management	Unauthorized access to Workstation	5.52	6	*1.76*	5.55	6	*1.63*	5.54	6	*1.94*	5.50	6	*1.71*	3.44	5	*2.22*
Automation	Unauthorized programming of a Controller	5.46	6	*1.79*	5.25	6	*1.86*	6.00	7	*1.74*	5.31	6	*1.67*	3.22	4	*2.04*
Management	Tampering with the ICT network	5.43	6	*1.66*	5.34	5	*1.59*	5.76	6	*1.65*	5.32	6	*1.69*	3.13	2.5	*2.20*
Automation	Tampering with the Automation network	5.40	6	*1.85*	5.09	6	*1.98*	**6.14**	**7**	*1.53*	5.45	6	*1.63*	3.75	4	*2.38*
Management	Insertion of an unauthorized Management level device	5.33	6	*1.88*	5.11	6	*1.89*	5.65	7	*1.97*	5.54	6	*1.66*	3.78	5	*2.15*
Automation	No tamper detection on Controllers	5.33	6	*1.87*	5.13	6	*1.89*	5.60	6	*1.90*	5.48	6	*1.76*	3.56	4	*1.95*
Automation	Overriding a Controller outputs or inputs	5.29	6	*1.80*	5.02	6	*1.90*	5.94	6.5	*1.41*	5.24	6	*1.77*	3.22	3	*2.20*
Field	Manipulation of Security sensor (Detector)	5.28	6	*1.82*	5.17	6	*1.77*	5.67	7	*1.75*	5.33	6	*1.82*	2.22	1	*1.69*
Automation	Insertion of an unauthorized Controller	5.26	6	*1.97*	5.00	6	*2.06*	5.58	7	*2.03*	5.45	6	*1.66*	3.56	4	*1.95*
Automation	Physical access to a controller	5.23	6	*1.89*	5.07	6	*1.91*	5.32	6	*2.05*	5.41	6	*1.69*	3.89	4	*1.91*
Automation	Manual override of Controllers output switches	5.19	6	*1.84*	5.12	6	*1.75*	5.57	6	*1.90*	4.97	5	*1.85*	**4.63**	6	*2.12*
Automation	Automation level open source network programs	5.16	6	*1.75*	4.83	5	*1.87*	5.53	6	*1.48*	5.38	6	*1.62*	4.11	5	*2.08*
Field	Manipulation of a Sensor or Actuator	5.09	5	*1.71*	4.96	5	*1.71*	5.39	6	*1.80*	5.13	5	*1.59*	2.88	2.5	*1.90*
Management	Monitoring the ICT network	5.06	6	*1.85*	5.00	6	*1.78*	5.43	6	*1.99*	4.84	5	*1.81*	3.75	4	*2.05*
Automation	Loss of mains power	5.06	6	*2.03*	4.86	5	*1.97*	5.62	6	*1.95*	4.93	6	*2.09*	3.11	1	*2.47*
Automation	Extraction of a Controller's latent memory	5.05	6	*1.84*	5.02	6	*1.87*	5.21	6	*2.08*	4.87	5	*1.58*	3.43	4	*2.19*
Automation	Damaging a Controller	5.02	6	*1.83*	4.95	6	*1.86*	5.17	6	*1.96*	5.05	6	*1.68*	3.11	3	*2.08*
Field	Automation network traffic monitoring	5.01	6	*1.77*	5.02	5	*1.74*	5.22	6	*1.83*	4.84	5	*1.76*	4.38	4.5	*2.23*
Management	Damage a Management level device	4.99	6	*1.79*	4.86	5	*1.85*	5.29	6	*1.77*	4.92	5	*1.61*	3.00	3.5	*1.73*
Automation	Automation network traffic data injection	4.98	5.5	*1.89*	4.59	5	*2.00*	5.23	6	*1.84*	5.26	6	*1.76*	4.25	4.5	*1.85*
Field	Physical disconnection of a Sensor or Actuator	4.81	5	*1.88*	4.79	5	*1.92*	5.03	6	*1.94*	4.75	5	*1.76*	3.78	4	*1.81*
Field	Damaging a Sensor or Actuator	4.81	5	*1.76*	4.91	6	*1.78*	4.89	5.5	*1.95*	4.64	5	*1.49*	3.38	3	*1.93*

Significantly, the expert group (see Figures 9.11 and 9.12) also expressed a wider range of criticality ratings to BACS vulnerabilities (34.4% difference between least and most critical) when compared with consultants (17%), building owner/operators (18%) and security professionals (19%). These differences further supported the view that the expert group held the most accurate and nuanced understanding of BACS vulnerabilities (Table 9.7). For example, the majority of critical concerns where located at the BACS architectural level of Automation, where the top 10 contain six critical automation vulnerabilities.

However this expert group was small (n=10), yet nonetheless, held congruent views. For example, vulnerabilities such as insertion of a rogue Controller and unauthorized programming of the Controller were rated as a relatively low criticality, opposing Stage 1 findings.

Table 9.7

Expert Group Mean and Median Ratings of the Level of Criticality of BACS Vulnerabilities in Highest Order

Level	**Expert Group**	**Mean**	**Median**	**SD**
Automation	Manual override of Controllers output switches	**4.63**	6	*2.12*
Field	Automation network traffic monitoring	4.38	4.5	*2.23*
Automation	Automation network traffic data injection	4.25	4.5	*1.85*
Automation	Automation level open source network programs	4.11	5	*2.08*
Automation	Physical access to a controller	3.89	4	*1.91*
Management	Insertion of an unauthorized Management level device	3.78	5	*2.15*
Field	Physical disconnection of a Sensor or Actuator	3.78	4	*1.81*
Automation	Tampering with the Automation network	3.75	4	*2.38*
Management	Monitoring the ICT network	3.75	4	*2.05*
Automation	No tamper detection on Controllers	3.56	4	*1.95*
Automation	Insertion of an unauthorized Controller	3.56	4	*1.95*
Management	Unauthorized access to Workstation	3.44	5	*2.22*
Automation	Extraction of a Controller's latent memory	3.43	4	*2.19*
Field	Damaging a Sensor or Actuator	3.38	3	*1.93*
Automation	Unauthorized programming of a Controller	3.22	4	*2.04*
Automation	Overriding a Controller outputs or inputs	3.22	3	*2.2*
Management	Tampering with the ICT network	3.13	2.5	*2.2*
Automation	Loss of mains power	3.11	1	*2.47*
Automation	Damaging a Controller	3.11	3	*2.08*
Management	Cyberattack on the Management level device	3	1	*2.26*
Management	Damage a Management level device	3	3.5	*1.73*
Field	Manipulation of a Sensor or Actuator	2.88	2.5	*1.9*
Field	Manipulation of Security sensor (Detector)	2.22	1	*1.69*

To assess whether there were any statistically significant differences between the mean vulnerability perceptions of the security, building owner/operator and expert groups, a one-way between groups ANOVA was selected. The ANOVA allowed for comparison of the effect of role function (building owner/operator, security and expert group) on perceptions of the criticality of 23 BACS vulnerabilities. Before undertaking the ANOVA, an inspection of skewness, kurtosis and Shapiro-Wilk statistics indicated that the assumption of normality was supported for each group, and Levene’s statistic was non-significant, indicating homogeneity of variance was not violated.

These tests indicated that no statistical assumptions related to running an ANOVA had been violated.

The results of the ANOVA indicated statistically significant differences between groups for 14 of the 23 BACS vulnerabilities, indicating that perceptions of the level of criticality was influenced by role function for these vulnerabilities (Table 9.8). Hochberg's GT2 (using an α of .05) was selected as the post-hoc test, being more robust to the large differences between sample sizes of the groups. The results of the Hochberg's post-hoc analysis revealed that building owner/operators and security professionals generally perceived BACS vulnerabilities as more critical than the expert group (Table 9.8).

Table 9.8

Significant Results from One-way between Groups ANOVA on Role Function and Mean Vulnerability Perception

Vulnerability	***df***	***F***	**CI**	***p***	n^2	**Direction**	**Magnitude**	***p***	***d***
No tamper detection on Controllers	2, 94	4.02	[4.75, 5.56]	.021	.08	Building > Expert	2.04	.017	.58
Overriding a Controller outputs or inputs	2, 97	8.79	[4.81, 5.57]	< .001	.15	Building > Security	0.93	.048	.49
						Security > Expert	1.8	.02	.56
						Building > Expert	2.72	< .001	.82
Damaging a Controller	2, 98	4.14	[4.47, 5.26]	.019	.08	Security > Expert	1.84	.03	.53
						Expert > Building	2.06	017	.57
Tampering with the Automation network	2, 98	6.47	[4.96, 5.75]	.002	.12	Building > Security	1.05	.032	.52
						Building > Expert	2.39	.005	.65
Insertion of an unauthorized Controller	2, 97	3.54	[4.66, 5.5]	.033	.07	Building > Expert	2.03	.03	.53
Unauthorized programming of a Controller	2, 99	8.19	[4.95, 5.73]	.001	.14	Security > Expert	2.03	.009	.61
						Building > Expert	2.78	< .001	.81
Loss of mains power	2, 97	3.54	[4.57, 5.39]	.033	.1	Building > Expert	2.51	.004	.67
Unauthorized access to Workstation	2, 103	5.48	[5, 5.73]	.042	.09	Security > Expert	2.11	.005	.64
						Building > Expert	2.1	.008	.61
Cyberattack on the Management level device	2, 104	11.49	[5.31, 6.05]	< .001	.18	Security > Expert	2.9	< .001	.91
						Building > Expert	2.97	< .001	.89
Damage a Management level device	2, 96	5.02	[4.48, 5.24]	.008	.09	Security > Expert	1.86	.026	.55
						Building > Expert	2.29	.006	.65
Tampering with the ICT network	2, 91	7.76	[4.93, 5.67]	.001	.15	Security > Expert	2.22	.003	.72
						Building > Expert	2.63	< .001	.82
Insertion of an unauthorized Management level device	2, 96	3.27	[4.77, 5.57]	.042	.06	Building > Expert	1.87	.038	.52
Manipulation of a Sensor or Actuator	2, 96	6.51	[4.57, 5.32]	.002	.12	Security > Expert	2.09	.008	.63
						Building > Expert	2.51	.001	.74
Manipulation of Security sensor (Detector)	2, 96	13.39	[4.67, 5.47]	< .001	.22	Security > Expert	2.95	< .001	.94
						Building > Expert	3.44	< .001	1.05

The ANOVA results indicated that significant vulnerabilities with the largest magnitude of difference between the group's mean scores were those which the expert group rated as less critical than the other two groups, such as Manipulation of Security sensor (Detector) and Cyberattack on the Management level device (Table 9.8). Those vulnerabilities with no significant difference in the ANOVA were those which the expert group rated as more critical (and therefore closer to the consistent high ratings of the other two groups). As a result, seven of the expert group's 10 most critical vulnerabilities were found to be not significant, including:

- Manual override of Controllers output switches
- Automation network traffic monitoring
- Automation network traffic data injection
- Automation level open source network programs
- Physical access to a controller
- Physical disconnection of a Sensor or Actuator
- Monitoring the ICT network

This finding may be visualized by comparing the median vulnerability ratings for building owners (5.5 to 7), security professionals (5 to 6.5) and the expert group (1 to 6) (Figure 9.13).

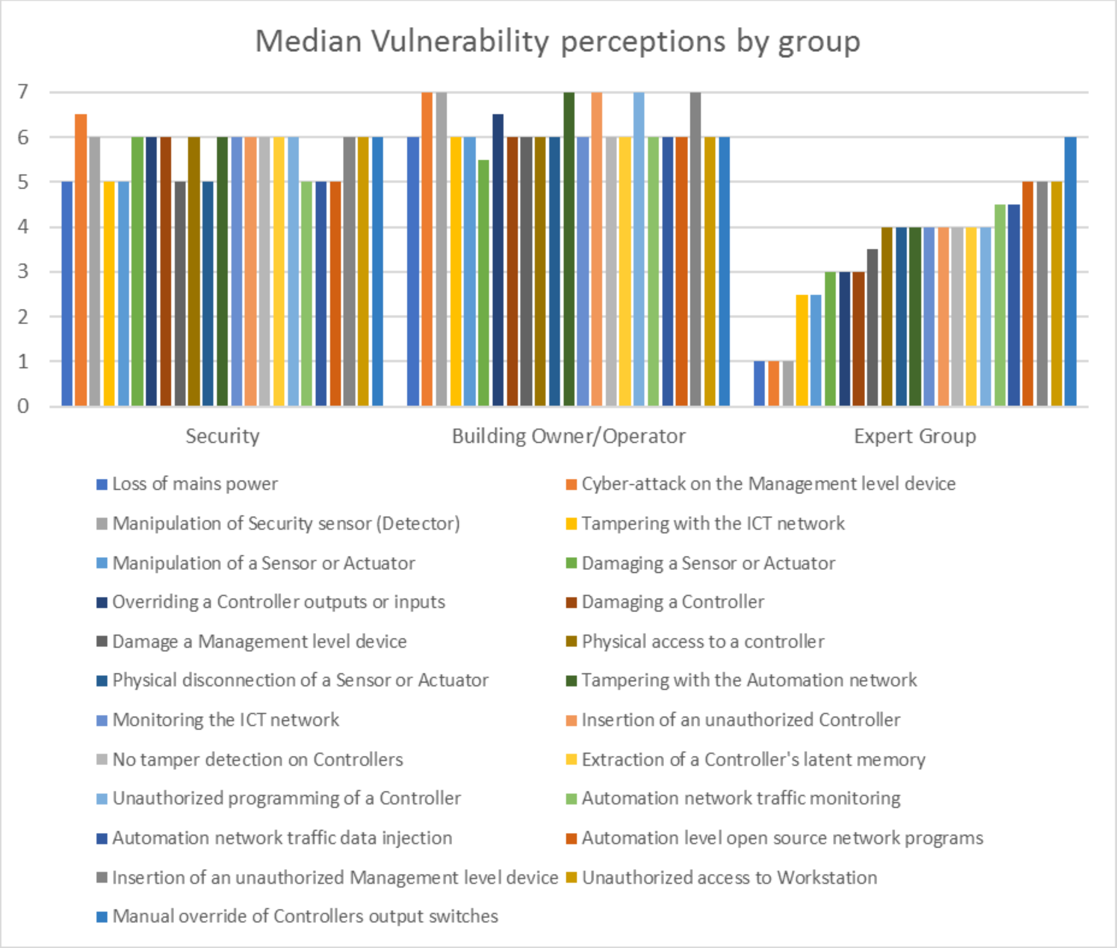


Figure 9.13. Median BACS vulnerability perceptions by group

Therefore, in response to the sub-question *What do security and builder owner/operator professionals consider are the most critical BACS vulnerabilities?*, the study found that most security and builder owner/operator professionals rated the criticality of each BACS vulnerability relatively equally and with limited distinction. This indicated that a blanket approach of considering all vulnerabilities to be equally critical was generally applied by security and builder owner/operator professionals. However, the expert group of integrators and cybersecurity professionals displayed the most diverse views and the most accurate understanding of BACS vulnerabilities by indicating that some vulnerabilities, particularly at the Automation level, were more critical than others.

9.2.6 Security Mitigation Strategies

The Stage 2 sub-question asked: *What security mitigation strategies do professionals generally apply to protect BACS?*

When asked which mitigation strategies they generally applied at each BACS architecture level, respondents who identified themselves as security professionals indicated the greatest level of practice and application of mitigation strategies (42%), followed by consultants (27%), building owner/operators (25%) and other roles (6%) (Table 9.9). As with the BACS critical vulnerabilities, the majority of respondents generally rated the mitigation strategies as being relatively equal and with limited variance. For example, the security professionals demonstrated a variance of 4 percent, building owner/operators of 5 percent, consultants of 3 percent and the expert group demonstrating the highest variance, at 12 percent.

To determine whether there was any statistically significant relationship between role function and the BACS architecture level of application of each mitigation strategy, a Pearson's chi-square test of contingencies (with $\alpha = .05$) was selected, given the categorical nature of the mitigation strategy data. The chi-square test was found to be statistically significant for the application of guidelines and standards $\chi2$ (4, N = 154) = 23.9, $p < .001$, V = .28), suggesting that the expert group were significantly more likely to apply guidelines and standards at the Field and Automation levels than the Management level. Likewise, this finding also suggested that security professionals and building owner operators were significantly more likely to apply this mitigation strategy at the Management level (Figure 9.14).

The chi-square test was also statistically significant for physical security $\chi2$ (4, N = 156) = 24.5, $p < .001$, V = .28), indicating that the expert group were significantly more likely to apply physical security mitigation strategies at the Automation level, whereas security professionals and building owner operators were significantly more likely to apply this mitigation strategy at the Field and Management levels (Figure 9.15).

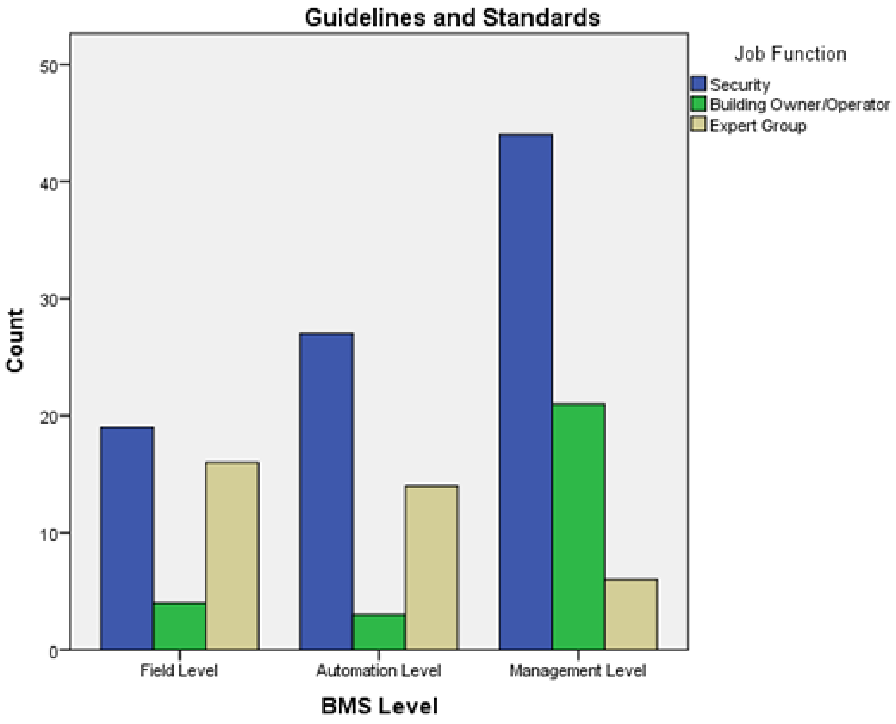


Figure 9.14. Level of Application of Guidelines and Standards by Role Function

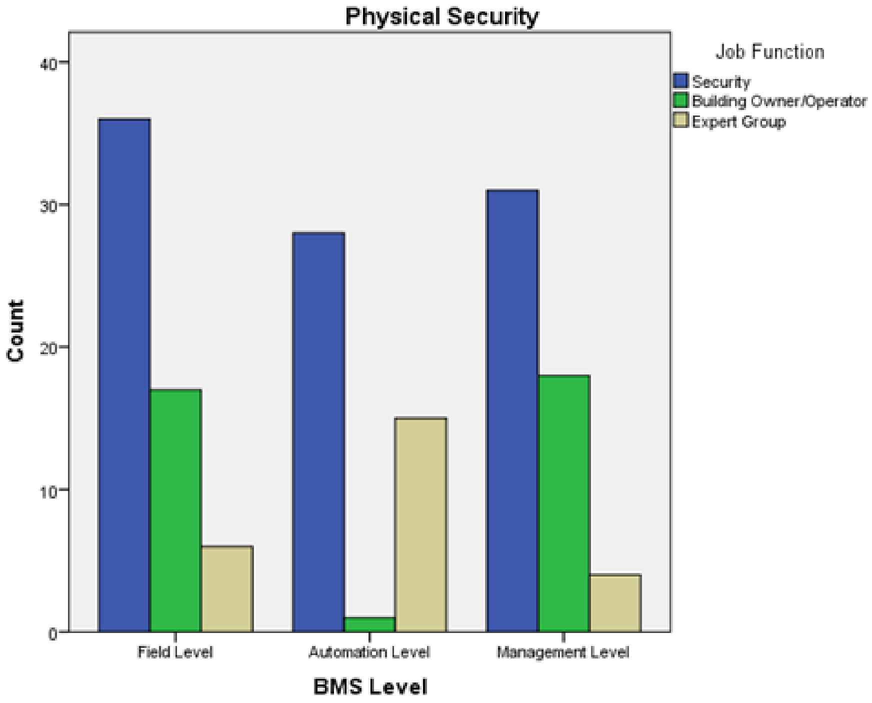


Figure 9.15. Level of Application of Physical Security by Role Function

The degree of application of each mitigation strategy was then calculated for each job function group to determine whether there were any discernible differences between the percent of respondents within each group that applied the mitigation strategies. The results (Table 9.9) indicated that security professionals, as would be expected, believe they apply the greatest level of security mitigation strategies; however, given the low level of their BACS responsibilities (10%) and neutral understanding of BACS critical vulnerabilities (see Figures 9.9 & 9.10), this finding may be unreliable. A similar assumption may be applied to building owner/operator and consultant.

Table 9.9

Average Degree of BACS Mitigation Strategy Application by Job Function

	Building Owner/Operator		Consultant		Expert Group		Security	
Mitigation Strategy	**% Applied**	**SD (levels of application)**	**% Applied**	**SD (levels of application)**	**% Applied**	**SD (levels of application)**	**% Applied**	**SD (levels of application)**
Policy	26% (n=33)	*6.18*	27% (n=35)	*9.20*	48% (n=8)	*1.89*	41% (n=48)	*15.12*
Guidelines/Standards	24% (n=31)	*2.94*	27% (n=34)	*5.72*	48% (n=8)	*1.25*	43% (n=54)	*10.42*
Procedures	25% (n=33)	*3.30*	27% (n=35)	*5.79*	52% (n=8)	*0.94*	42% (n=54)	*5.56*
Emergency response	26% (n=34)	*5.91*	26% (n=33)	*4.32*	44% (n=8)	*1.41*	42% (n=54)	*7.72*
Intruder alarm	24% (n=31)	*1.70*	28% (n=35)	*4.03*	41% (n=7)	*1.70*	42% (n=53)	*7.36*
Tamper detection	25% (n=31)	*2.16*	27% (n=34)	*3.77*	44% (n=8)	*2.16*	43% (n=54)	*7.36*
Physical security	24% (n=32)	*1.25*	28% (n=37)	*4.32*	41% (n=7)	*2.05*	42% (n=55)	*3.30*
ITC security	23% (n=26)	*5.73*	26% (n=30)	*1.70*	48% (n=8)	*0.94*	44% (n=50)	*6.60*
Security risk assessment	23% (n=31)	*8.01*	28% (n=37)	*10.21*	52% (n=8)	*1.25*	43% (n=57)	*11.43*
Threat assessment	24% (n=32)	*8.52*	27% (n=35)	*8.52*	52% (n=8)	*0.94*	43% (n=56)	*12.83*
Personnel security	27% (n=34)	*7.35*	25% (n=52)	*6.94*	41% (n=7)	*1.70*	42% (n=54)	*8.22*
Security awareness	26% (n=34)	*7.76*	27% (n=36)	*8.18*	52% (n=8)	*1.70*	41% (n=55)	*10.62*
Electronic access control	25% (n=34)	*3.09*	28% (n=37)	*0.94*	41% (n=7)	*1.25*	41% (n=55)	*4.55*
Maintenance	26% (n=34)	*4.03*	28% (n=36)	*4.92*	44% (n=8)	*0.82*	40% (n=52)	*5.31*
Continuity planning	24% (n=31)	*8.01*	28% (n=36)	*11.15*	52% (n=8)	*1.25*	42% (n=55)	*14.35*
Recovery planning	25% (n=32)	*8.99*	28% (n=36)	*10.80*	48% (n=8)	*1.89*	42% (n=54)	*15.28*
Auditing	22% (n=28)	*9.43*	28% (n=35)	*9.93*	44% (n=8)	*2.16*	44% (n=55)	*13.22*

Table 9.10 expands the previous table by indicating the mitigation strategy application at each BACS architecture level by job function. This analysis indicated that the building owner/operators tended to state that they apply a greater number of mitigation strategies at the BACS architectural level of Management. The other groups did not produce any clear division between BACS architectural levels. Although this data produced a greater variance between strategies, no clear conclusion of what security mitigation strategies are applied can be extracted from the data.

Table 9.10

Degree of Mitigation Strategy Application at each BACS Architecture Level by Job Function

	Building Owner/Operator			Consultant			Expert Group			Security		
Mitigation Strategy	*Automation level strategies (% applied)*	*Field level strategies (% applied)*	*Management level strategies (% applied)*	*Automation level strategies (% applied)*	*Field level strategies (% applied)*	*Management level strategies (% applied)*	*Automation level strategies (% applied)*	*Field level strategies (% applied)*	*Management level strategies (% applied)*	*Automation level strategies (% applied)*	*Field level strategies (% applied)*	*Management level strategies (% applied)*
Policy	45.45%	39.39%	81.82%	40.00%	37.14%	94.29%	33.33%	33.33%	77.78%	38.46%	25.00%	92.31%
Guidelines/Standards	45.16%	51.61%	67.74%	37.14%	94.29%	47.06%	33.33%	44.44%	66.67%	25.00%	92.31%	50.00%
Procedures	39.39%	48.48%	63.64%	94.29%	47.06%	52.94%	66.67%	44.44%	44.44%	92.31%	50.00%	35.19%
Emergency response	17.31%	40.38%	42.31%	47.06%	52.94%	85.29%	55.56%	22.22%	55.56%	50.00%	35.19%	81.48%
Intruder alarm	51.61%	38.71%	48.39%	52.94%	85.29%	40.00%	33.33%	66.67%	22.22%	35.19%	81.48%	46.30%
Tamper detection	58.06%	45.16%	41.94%	85.29%	40.00%	54.29%	22.22%	77.78%	33.33%	81.48%	46.30%	51.85%
Physical security	46.88%	53.13%	56.25%	40.00%	54.29%	80.00%	11.11%	66.67%	44.44%	46.30%	51.85%	70.37%
ITC security	46.15%	23.08%	76.92%	54.29%	80.00%	26.67%	55.56%	33.33%	55.56%	51.85%	70.37%	29.67%
Security risk assessment	25.81%	25.81%	80.65%	80.00%	26.67%	30.00%	55.56%	33.33%	66.67%	70.37%	29.67%	25.27%
Threat assessment	25.00%	31.25%	84.38%	26.67%	30.00%	43.33%	44.44%	44.44%	66.67%	29.67%	25.27%	45.05%
Personnel security	20.59%	47.06%	73.53%	30.00%	43.33%	62.86%	22.22%	33.33%	66.67%	25.27%	45.05%	73.58%
Security awareness	26.47%	52.94%	82.35%	43.33%	62.86%	65.71%	33.33%	44.44%	77.78%	45.05%	73.58%	54.72%
Electronic access control	50.00%	52.94%	70.59%	62.86%	65.71%	40.00%	22.22%	44.44%	55.56%	73.58%	54.72%	39.62%
Maintenance	41.18%	67.65%	44.12%	65.71%	40.00%	61.76%	44.44%	55.56%	33.33%	54.72%	39.62%	68.52%
Continuity planning	25.81%	25.81%	80.65%	40.00%	61.76%	61.76%	66.67%	33.33%	55.56%	39.62%	68.52%	53.70%
Recovery planning	21.88%	28.13%	84.38%	61.76%	61.76%	38.24%	33.33%	33.33%	77.78%	68.52%	53.70%	35.19%
Auditing	17.86%	17.86%	89.29%	61.76%	38.24%	56.76%	33.33%	22.22%	77.78%	53.70%	35.19%	50.91%

Therefore, in response to the sub-question *What security mitigation strategies do professionals generally apply to protect BACS?*, the study found that security, building owner/operator and consultant professionals apply most BACS mitigation strategies at some level and generally rated the mitigation strategies as being relatively equal and with limited variance. The results also indicated that security professionals believe they apply the greatest level of security mitigation strategies; however, given their low level of BACS responsibility and neutral understanding of BACS critical vulnerabilities, this finding may be relatively unreliable. Overall, no clear conclusion of what security mitigation strategies the professionals apply can be extracted from the data.

9.2.7 Ideal BACS Security Mitigation Strategies

The Stage 2 sub-question asked: *What are the ideal security measures used by security and building owner/operator professionals for protecting BACS?*

When the expert group's assessment of the mitigation strategies were isolated (Table 9.11) from the other groups, it was found that they produced a similar conclusion to project Stage 1. For example, the data indicated that the most selected mitigation strategies by the expert group were security risk assessment, threat assessment, procedures, security awareness and continuity planning. The mitigation strategy of security risk assessment and threat assessment may be assimilated under security risk management, which may also include criticality assessment. However, there was a relatively low variance between the highest (52%) to the lowest (41%) applied strategy, with a relatively consistent agreement between respondents.

Table 9.11

Average Mitigation Strategy Application by Expert Group

Mitigation Strategy	**Expert Group**	
	Average % Strategy Applied	**SD (between levels of application)**
Procedures	52%	0.94
Threat assessment	52%	0.94
Security risk assessment	52%	1.25
Continuity planning	52%	1.25
Security awareness	52%	1.70
ITC security	48%	0.94
Guidelines/Standards	48%	1.25
Policy	48%	1.89
Recovery planning	48%	1.89
Maintenance	44%	0.82
Emergency response	44%	1.41
Tamper detection	44%	2.16
Auditing	44%	2.16
Electronic access control	41%	1.25
Intruder alarm	41%	1.70
Personnel security	41%	1.70
Physical security	41%	2.05

In response to the sub-question *What are the ideal security measures used by security and building owner/operator professionals for protecting BACS?*, the study found that, according to the expert group, the five most significant BACS mitigation strategies are procedures, security risk management (threat, security risk and criticality assessments), continuity planning, security awareness and ITC security. The study was unable to determine the ideal security measures as used by security and building owner/operator professionals due to the homogenous rating of mitigation strategies by these two groups.

9.3 CONCLUSION

Project Stage 2 found that security and facility (building owners and operators) professionals need to take guidance from cybersecurity and technical integrators in the security of BACS. Integrators had a more robust understanding of the vulnerabilities, and therefore, security strategies necessary within a risk framework to protect the built environment and its facilities from BACS exploitation. As a group, security and facility professionals demonstrate limited understanding of the significance of BACS vulnerabilities and therefore, the appropriate mitigation strategies required to protect again malicious interference through the built environment connectivity architecture.

Section 10. Stage 3 Focus Groups

10.1 INTRODUCTION

This section presents the focus group interview analysis. Drawing from Stage 2 findings and enhanced through expert panel discourse, this stage provides a deeper understanding of Building Automation and Control Systems (BACS) concerns across the security and facility management domains. The Stage 2 survey assessed security and facility practitioner's awareness and understanding of BACS. Findings indicated that for many participants, they did not understand the security issues associated with BACS. These previous findings informed this final project stage, where focus groups where undertaken to further explore the findings of Stage 2, and assess the validity and useability of the draft BACS Guideline. This section presents the focus groups and their participants, the collected data, including key participant statements and analysis, and stage interpretations.

10.2 FOCUS GROUPS

Focus groups were undertaken to garner the understanding of both security and building professionals responses to the Stage 2 survey questionnaire. In addition, to gather their views on the draft BACS Guideline along with their perceived ability to apply the BACS Guideline in the pursuit of organizational and facility security. The focus groups used a Questionnaire (Appendix H) embedding semi-structured questions that were audio recorded and later, transcribed verbatim. These transcripts were later analysed and interpreted using content and thematic analysis techniques.

The focus groups were carried out during the ASIS International 63rd Annual Seminar and Exhibits 2017, held September 25th to 28th, 2017 (Table 10.1). Using a non-probability convenience sample, executive members from ASIS International, BOMA and SIA were requested to participate. Once volunteers were gained, they were assigned to one of the four focus groups with participants spread based on their member association and practice area. In addition, during a project presentation on the September 25th, 2017, further volunteers were solicited and gained to overcome non-attendance risks.

Table 10.1

Focus Groups

Focus Group	Day	Time
1	Tuesday, September 26th, 2017	10:00 - 12:00
2	Tuesday, September 26th, 2017	13:00 - 15:00
3	Wednesday, September 27th, 2017	10:00 - 12:00
4	Wednesday, September 27th, 2017	13:00 - 15:00

The focus group participants (N=14) came from a broad range of practice areas (Table 10.2), including corporate security, information technology, public safety, consulting, building engineer, commercial real estate, fire and life safety, and crisis management. The participants' years of experience ranged from the lowest, at 5 years, to the longest member with over 35 years. The highest held degree was a Master (one only), with two degrees and the majority of participants (security) with the ASIS International CPP certification.

Table 10.2

Focus Group Participants Overview

Title	Primary work area	Career	Quals/Certs	Previous work, roles or functions
Head of Security	Security/Engineer	15 years	CPP, CBCP	USMC, Signals intelligence 5 years. Security data centre 8 years. Commercial real estate 3 years.
General Manager	Commercial Buildings	26 years	CPM	General Manager of Building.
CSO (Retired)	Security Manager	35+ years	CPP, CSSA, CSP	CSO: Fortune 50 company.
Vice President/SFO Consultant	Consulting: Risk	26 years	BS, MSA, CPP	Director: Safety and Security of nuclear power plant. Corporate Security Director: Fortune 100 company.
Manager Security	Office buildings	11 years	CPP	Facilities security manager 8 years. Royal Air Force: Tactical support wing officer 11 years.
Comms & Technology Coordinator	Security	12 years	MS	Patrol Officer: Campus Safety.
Security & Compliance Manager	Physical, Cybersecurity NERC compliance	15 years	CPP, PSP	Army cavalry officer. Cybersecurity officer (US Army) Homeland Security. Cyber and Physical Security Auditor.
Integration Department Manager	BACS Security Management	30+ years	BS, Grad Cert, CPP, ALE	Security consulting. Programming. Project Management. Accounting and commercial work.
Applied Sci Council, PSWG	Manage Public Safety			Chair Applied Sci Council, PSWG, PHS Sat Vqips.
VP IS/CIO	Commercial real estate	15+ years	CISSP	Dept of Defense, Information Security. Higher Education. State Government. Commercial Real Estate.
Director Public Safety	Fire and Life Safety/Security	35 years	BA, CPP, PCI, PPS, AASe	Police Officer 16 years. International Police Advisor, Chief-East Baghdad. Personnel security Specialist (Iraq) DOS-CPA. Corporate Security.
Risk & Security Consultant	Building intelligence to mitigate risk and enhance security	25 years		Chief of Operations, risk, security and crisis management. Oversight personnel, facilities, systems, assets and brand.
Managing Principal	Site Security Executive Protection	20+ years		Site supervisor, Apple Campus. Consultant with Various Companies.
Industrial Security Officer	Security programs within industry	5 years	DD Certs, SPPC, PSC	Security operations. Personal security.

10.3 ANALYSIS & INTERPRETATION

Each focus group used the Stage 3 semi-structured Questionnaire (Appendix H), with questions put to the participants by the facilitators in a step through process. Each question was asked in order, which allowed all focus groups to be analysed with merged responses to uncover themes along with individual views. The focus groups followed the three discrete parts of the Questionnaire, with general participant information (see above Table 10.2), focus group questions to review the Stage 2 findings (Section 10.3.1 Focus Group Questions) and then critique the questions within the BACS Guideline (Section 10.3.2 BACS Guideline Review). However, additional themes developed from the participants that were also extracted and presented (Section10.3.3 Focus Group Themes). Analysis resulted in shared themes being extracted, shown in text boxes.

10.3.1 Focus Group Questions

This section covers the responses, analysis and interpretations of the reviews of the Stage 2 survey.

10.3.1.1 BACS Responsibilities

Focus group question 1 asked the participants: *During our online survey, we found only 8% of respondents had BACS responsibilities. Within this group, the majority of those responsible for BACS were facility professionals. Is this your personal experience in regard to BACS?*

Stage Two included a survey questionnaire which found that only eight percent of respondents included responsibilities for BACS in their occupational role. This finding resonated with focus group participants, who upheld such a low level of BACS responsibility across the security sector. For instance, EP stated that “the building automation systems are managed by our building staff engineers, our people operating are usually the facilities team ... but our access control systems is managed by security” (EP). This perspective was reinforced by DE, who explained that “from his (my) experience... sole responsibility for the BACS system is the building operations manager (DE). Such a lack of responsibility was expressed by AW as well, stating, that such a findings for the security professional “is absolutely true” when considering BACS, adding “in my experience the responsibility is with the facilities folks, the gap is on the security side. It’s not physical security focussed because as I say yes its IT” (AW).

For the security and facility management professional common themes of BACS responsibility emerged, suggesting Facility Managers manage and operate BACS. Whereas, Security Managers manage and operate the security systems, such as intrusion detection, access control and surveillance systems, and Information Technology manages and operates the technical elements of networked systems, including the broader BACS architecture.

At present, the Security Manager and their operations have a low level of BACS responsibility.

10.3.1.2 Poor Awareness of BACS Architecture

Focus group question 3 asked the participants: *Our survey results suggested that 75% of security and facility professionals felt they had an awareness of the different BACS architectural levels; however, on analysis the majority displayed limited understanding in their vulnerabilities? Why do you feel that these professionals believed that they understood BACS architecture, yet perhaps do not?*

BACS are characterised by a hierarchical architecture. Knowledge of this architecture is essential in understanding their vulnerabilities and associated security requirements. Consequently, the Stage 2 survey showed that 75% of security and facility professionals felt they had an awareness of the different BACS architectural levels. However, later questions revealed that participants did not have the detailed technical understanding they believed they held. Such a finding was put to the focus groups to uncover why this perceptual disconnect emerged. To explain these findings, SS stated “the security people think they understand their networks … I’ll be the first to tell you I don’t understand the network concept as far as the building automations controls, security wise I have somewhat of an idea, but I would think they are both pretty close to the same.” (SS). MM extended this explanation further, stating that:

> “You have people at our institution where you have HVAC and lighting, all being controlled through a central product so that is BACS. Somebody would say, yes, I understand I have a BACS, but then if you start asking questions about vulnerabilities some people will say who cares if you turn off some lights or someone jacks the heat up that is no big deal. That’s where you find you have people that say I know what BACS is but they don’t necessarily grasp the criticality of such vulnerabilities” (MM)

Such a view was supported by the other participants, for example DE stated “everyone says they know what BACS is but when we start probing it a little bit they don’t really. The security guys are like Yes it’s integrated because it’s all one system or somebody has told me they’re all tied together, what does that really mean” (DE). Furthermore, “people may not think anything on the network is automatically part of it, ideally the person managing the BACS system wouldn’t be confused here, but I think that maybe making sure it is extremely clear what a building automation control system is, is necessary” (EP).

The focus group participants collectively opposed the view that 75% of security and facility professionals have an appropriate awareness of the technical elements of BACS, especially the different BACS architectural levels.

Participants supported the view that a very different level of understanding exists between security and facility professions on these systems.

This stage supported that Security and Facility Managers professionals do not appear to understand the technical elements of connectivity and integration for today’s BACS. Furthermore, the assumption may be extended to resulting vulnerabilities.

10.3.1.3 Integrators: The BACS Expert

Focus group question 4 asked the participants: *Results identified that Security Integrators (including cyber) displayed a high level of understanding of BACS criticalities. Is this your experience as well and if so, why?*

The Stage 2 survey found that Security Integrators (including cyber professionals) displayed a high level of understanding of BACS criticalities. This findings was also well supported by focus group participants who highlighted that while security and facility professionals have limited skills and understanding of network security, integrators have sound levels of knowledge and skills in network connectivity, integration and network security. The view of the participants was that this was the occupational domain of information technology and in particular, the cybersecurity professionals. In addition, the relationship the Integrators had with their clients were often considered in a technical support and service role; rather, than as a strategic partner who could also provide security advice.

Lack of IT Skills

The focus group discussion developed the theme that there was a lack of information technology and cybersecurity skills within both traditional security and facility professionals. As MD stated

"Facilities management and security is having less impact; and it is probably because there are less IT skill sets and even less cybersecurity skill sets, because they are relying on the vendor services." (MD). MD further added "we pulled our security systems away from security when the grid came in four years ago. Prior .. facilities weren't even into security systems." (MD).

Integrator Reliance

The focus group discussion highlighted that due to the limited skills and understanding security and facility professionals have of network security, they have become over reliant on Integrators. Participant DC confirmed the issue of integrator or vender reliance, stating "Yes I have to agree ... we rely a lot on our vendors as the traditional security personnel don't have that IT background" (DC). SD added that their organisational approach was "We use xxxx to monitor the network and all access to the network, the request comes to us we put it to xxxx, give them a check sheet to see that we are comfortable with this, we have done our due diligence and we agree to give them an access point to this, they will give them the port and then it comes back to us and we will audit it as we go." (SD).

From an Integrators perspective, KS stated that "You, as an organisation recognise the importance of a contractor, we need remote access because that is how we can service our end users without having to roll a truck, I have customers who said no you can't have access, we are in 2017 ... [however, under the] Service contract the hourly rate is going to be three times the cost then... because we have to roll a truck every time you call" (KK). However, another participant stated that "We also have xxxx 24/7 monitoring for any unusual activity, so a switch has gone down, any transmissions we were not expecting, any intrusion attacks and so forth and so on." (DE). He went further, where "they will tell us when we have an intrusion, what the outcome is and tell us what they have done and what they would like us to do." (DE).

From an Integrators perspective, KS stated that "we have to do whatever the end user wants, we are not going to say this is best, because usually there is someone on the other side like... a CEO that is dictating this kind of policy because they have either had a breach, or read a white paper that said this is the best way to do it. Again as a contractor we are at the bottom, we do what the end user wants." (KS). Integrators, even given their skills, are a service and maintenance function; rather than being able to feel that they can provide best practice technical advice. Such an approach conflicts with many of the focus group participants views on Integrator reliance.

There was support in the view that Integrators, also referred to as Vendors, Installers or Maintainers, hold a high level of BACS technical understanding. However, notwithstanding their skills, Integrators provide a service and maintenance function; rather than providing best practice operational and security advice. Therefore, advice given by Integrators may be seen as "upselling" their products and services; rather than a strategic partner who provides BACS security advice.

The focus groups raised the view that both Security and Facility professionals lack the necessary information technology and cybersecurity skills, but these skills are held by integrators.

10.3.1.4 Differing Views of BACS & Security Integration

Focus group question 5 asked the participants: *The survey results indicated a significant divergence between security and facility professionals on what degree of security systems integrate into BACS. Security professional suggested a higher proportion of security systems integration, compared to facility professionals. Why do you think there is such divergence?*

The Stage 2 survey indicated a significant divergence between security and facility professionals regarding the degree of security system integration into BACS. Specifically, security professional suggested a higher proportion of security systems integration, compared to facility professionals. The Stage 2 survey found that 50% of participants suggested they had security integrated with BACS. However, the focus group response to this result was not supportive, arguing for a misunderstanding in what is meant by integration. For example both SS and EP stated "that seems high;" asking, "Are they integrated" (DC), and "I think there is kind of a misunderstanding, that seems awful high." (SS).

Each professional (Security, facility management, information technology) generally focused only on their areas of practice and responsibility. For the security and facility professionals, the technical elements of BACS fell outside their area of expertise and so did knowledge of the vulnerabilities and required security measures.

10.3.1.5 What does BACS Integration Mean?

Focus group question 6 asked the participants: *In your view, what does integration mean in the context of BACS and security systems from a security and/or facility professional view? Do these views differ?*

The issue of a common understanding arose, inasmuch as what does *integration* really mean? Participants responded with a view that integration was single data entry, where human resources (HR) inputs data and that data flows into the access control systems. There lacked a broader understanding that once a card was authorised, this could also control the BACS sub-systems, such as lighting, elevators and HVAC. For example, VL focused on access control stating that "HR... gives security the lead to go ahead and produce badges, we double check with HR for (who this has access), so you get an email ... access to buildings 3 and 4 and I send a confirmation back. If this is correct, this person gets this access". (VL). Such an approach was also taken by both KM and MP, where MP stated that they "all get that badge .. through the HR system" (MP).

The matter of what is integration arose, where EP stated:

> Unless there is a misunderstanding of what the definition is, not integration but .. if they are saying that their access control system is on the network. That is a completely different understanding of what we are discussing, as an access control system being integrated into a larger building system as a whole.

Participants suggested that this may be a language issue. For example, SS stated that this "may be the language issue here, you are talking a tamper attack opens up a panel, and having a tamper switch or a tamper attack meaning an intrusion event?" (SS). Another broader view was put forward by KK, who suggested that "When you say security professionals what do you mean? The survey indicated security professionals, I put down yes because I think as security professionals in the context of IT not in the context of facilities." (KK). Finally, MP also stated that "you are going across functions from security and facility management... and they might understand terms differently to what we do on the security side" (MP).

Integration was summarized by DE, who stated:

> "We have 11 towers in xxxx and if you ask me the same question, I would say that 7 of the 11 are BACS linked in respect that they are on the same network, the opportunity is there to integrate with the other systems .. whereas the others are standalone, [but] they talk to the CCTV and that is as far as they go, I wouldn't regard those as being on the BACS

> system. Once you've granted access to the same network .. there is an opportunity to integrated even though you are not necessarily using it because of compatibility issues, but I would regard that as being on the BACS yes" (DE).

Another theme that developed during the focus group and from the issue of integration, was having a clear understanding of "what is BACS?" For example, one participant raised the point of "How do we define BACS because you've got building automation systems, lighting systems, HVAC and all these things that are standalone aren't BACS … it's not until you move them to the integration stage on the same network when they become BACS" (DE). This definition issue was further expanded, when EP suggested that "even understanding of what a building automation system is has a number of different options and the standard so I would think that maybe, I don't know how, I don't think we can make it any smaller but I think that is probably where the discourse was, is the difference between just something on the network compared to something integrated and smart" (EP).

The focus group believed that integration is not properly understood at a holistic level. Integration is technically and functionally broad and undefined, with diverse views on meaning depending on the persons' practicing role. Consequently, a persons' focus (understanding) was generally aligned to their practicing roles, such as security, facility or information technology. For the security and facility professional, BACS lacks clear definition, in part, due to its broad range of technologies and functions.

There was a lack of common and clarity of language with BACS terms and practice.

There was a lack of common language with security terms and practice.

10.3.1.6 Security & Facilities Professionals Do Not Understand BACS Vulnerabilities

Focus group question 7 asked the participants: *When we surveyed 23 BACS vulnerabilities, we found a neutral response i.e., there was little difference between the criticality of the 23 vulnerabilities. Why do you believe that most security and facility professionals rated the criticality of BACS vulnerabilities relatively equally?*

The Stage 2 survey found that of the 23 identified generic BACS vulnerabilities, there was a neutral response in criticalities from security and facility professionals (n=321); however, an identified technical stream was able to clearly classify hierarchical criticalities (n=10). In other words, the majority of survey participants rated little difference between the criticality of the 23 BACS vulnerabilities. The Stage 3 focus group participants were asked why they believed that the security and facility professionals sample rated the criticality of BACS vulnerabilities relatively equal.

Responses to this question reinforced that view that the facility and security professionals are not responsible for the technical management of BACS and its network and that they do not hold the associated technical knowledge to facilitate such comprehension. As MR stated:

> "Anyone can control the network, generally speaking we have a third party we employ to manage our network, they monitor the network and look for intrusions, make sure they are the switching and the switches and ports are closed when they are supposed to be closed and we ask them to provide support when we want to add a new system into the program." (MR).

Furthermore, MR stated "One of the exceptions I found is where they [organization] have a large IT department and facilities department to support that, to be able to do that, they have dedicated people." (MR). However, generally network vulnerabilities and associated security requirements are managed by IT and cybersecurity professionals. Therefore, security and facility managers do not have a technical understanding of BACS architecture and therefore, its associated vulnerabilities and their risk significance.

The participants were also asked about separation between the automation control network and the boarder corporate network. The participants generally felt that these were separated. For example, MR stated that his are "Totally separate for us, no connection." (MR). Others stated that "very similarly, except ours are not fully integrated at that corporate level. Both of our systems sit on the corporate network" (MM).

> Security and facility professionals do not have a robust understanding of BACS vulnerabilities or their risk significance. The majority of security and facility professionals rely on third party professionals, or Information Technology specialist to provide the technical understanding and security practices for BACS protection. To manage BACS well, requires dedicated IT professionals within, or integrated with the facilities department
>
> Security and facility professionals BACS "third parties: may be in-house information technology or cyber professionals or contractors, such as Integrators.

10.3.2 BACS Guideline Review

This section covers the responses, analysis and interpretations of the BACS Guideline.

10.3.2.1 BACS Guideline General Readability

Focus group question 8 asked the participants: *In general, does the BACS Guideline provide enough (in plain English) information to give you an appropriate understanding and awareness of: BACS, BACS architecture, BACS vulnerabilities; and BACS mitigation strategies.*

Factors of the BACS Guideline were explored with the Stage 3 focus group participants. The participants were asked to comment on the Guideline's general readability, criticality or impact matrix (BACS Guideline Appendix A), BACS security questions (BACS Guideline Appendix B) and its links to security vulnerabilities. Further themes were also extracted during the focus groups.

10.3.2.2 Criticality Matrix (Appendix A)

To apply the BACS Guideline in context, a draft facilities Criticality or impact matrix was developed. In the first line of questioning participants were probed regarding the applicability and usability of this Criticality matrix. Participants responded positively towards the matrix. For example, DC stated that "No one has this .. I'm really happy to see that you have got the different levels there because I'll just show you this what" (DC). SS went further, stating that "You've done a great job here and all I ask that you normalise it with the terms" (SS). Such a view was further supported, with VL stating "Pretty clear and concise, yes, pretty simple language so it should be understood" (VL). Whereas (KM) stated "you sent this to me and I am already using it, I have just been doing this at work as a project and I am already adding elements I didn't think of". Nevertheless, VL provided further support:

> "I definitely want to spend some more time on it. I think also from my side going in and working with, not even just with government contracts but with general law firms and people in the states it would be a great matrix to go and speak with the managing partner or CEO .. I'm really excited to see even from the report or study into this I think that is really going to be helpful. Even from a sales perspective trying to work with industry, you

> can walk into the 60 year old CEO and say here is a cyber-question you need to answer" (VL)

Nevertheless, some the participants had a number of comments with the matrix, its categories and levels. For example, EP felt that "I think appendix A .. could be simplified and I don't know what the solution to simplifying is" (EP). These issues are further explored in the proceeding sections.

Articulating Type of Facilities

The participants were asked if they felt that it could assist them in articulating the types of built environments or facilities they manage and consequently if they would use the BACS Guideline? There was generally an affirmative response, with EP stating "I think the goal here is to be the guideline that everyone uses, because if Sure and Steen are using something different to what we are using compared to what is going on in Arizona let's say, then it doesn't compare but I think my thought here is as long as everyone is using the same one we don't really need to dive too much as to what is on this one, it covers categories then sets the standard." (EP). The other participant supported the use of a standardized guideline.

Specifically, such a view was further supported by DC, who understood the need to separate use or occupancy of multiple tenanted building and provide appropriate security measures across each area. DC made the comment that "I'm actually pretty good with that [matrix]. I do 1, 2 and 3 and combine all. Like xxxx .. he basically had a building in New Jersey that has a parking area on the entry levels, a mall on the next two levels, tenant 1 a common area, and then tenant 2 and then executive residences on top" (DC).

Another participant went further, stating that they had a government department as one of their tenants in a multi-tenanted facility. "Obviously they have their own infrastructure but we have our [BACS] system, we have learned .. that they can destroy the building, whether it's taking out the lights the air-conditioning, we learned this even includes just the burst pipes, I didn't even know that one, so in that is just one of my tenants of the 50 tenants I have in one building. Supreme Court Justice gets targeted so I think this is a nice guideline, but bottom line is you have to look at who your tenants are to determine really what level you can invest in" (LB).

Criticality Categories

The focus group participants were asked if they felt that the criticality categories were appropriate, valid and useable. For instance, does the matrix require a category of *reputation*? There were suggestions in relations to some of the categories, primarily *regulatory*, *life safety* and *occupancy*.

With regulatory, EP felt that "regulatory doesn't apply to me, but it applies to a power plant. I think they can all stay and those people that it doesn't apply to won't look at those" (EP). Furthermore, SS stated that regulatory "in itself is about five different areas and I know it has to do with more the market where this property is" (SS).

Another category discussed was life safety, where participant's comments commenced with the National Fire Protection Association (NFPA). For example, SS stated that "having a life safety perspective for this is going to be incredibly helpful, but you cannot involve the NFPA because they are not compliant [BACS] .. they need a life safety perspective' (SS). Therefore, the question was posed "if there was a need for life safety?" (DB). The response was positive, with "Yes, because we are out of organisation resilience, and the life safety system the fire alarm system should be designed to be the most resilient system in the building." (SS).

The category of occupancy was also raised. As MM suggested "ultimately, the impact of the loss of occupancy … if they can work out of the office next door, not nearly as critical, versus the residences hall" (MM). Further comment was the need to continue to operate, as KK suggested "We have an office in Houston and when the hurricane hit, we had a lot of people who physically couldn't make it to the office but they could still remote in if they had power and internet, to continue to work and do some of their work" (KK).

The category of financial had a limited discussion. For example, MM stated that "for one building to go offline, that is less than 10% financial impact. For them, something that completely comprises that building doesn't even reach the level of critical. Whereas for an institution like mine, if one residences hall goes off line "we are in deep shit"; that immediately escalates more rapidly." (MM). General discussion led to the view that there needed to be an explicit statement in the guide stating that the assessor needs to provide an financial framework, for example a cost value against each level based on their context to facilitate the assessment of risk and guide mitigation requirements against defined risk.

Finally, a validating response for the matrix was put forward by participant KK with:

> "The focus at least for us from what I've seen has been you have that separation because people see value in the financial data or the intellectual property of the company, that is why it is on the enterprise side and you put all those controls around it, there has not been value seen in those building networks" (KK).

Nevertheless, there was some opposing views. For example, MP suggested that the category "might be business impact initially, it might be regulatory... so the context is varied (MP). As followed, "Or it could be both" (KM). However, in general there was support amongst the participants for the matrix's identified categories.

Criticality Levels

The focus group participants were asked if they felt that the Guideline's criticality levels were appropriate, valid and useable. For instance, whether the matrix's use of a five point scale from *low* to *critical* were appropriate, and their descriptors understandable and useable.

In general, the focus group participants provided an affirmative response to the defined rating levels. For example, DC stated that "We use this almost exact in our risk compliance in everything we do. Every system we look at, just everything. It might have changed in the last year since I retired but you never know" (DC). In addition, SD raised the aspect that "The colours match the old homeland security colour scheme for criticality of an event ... I understand the visual reference, the colour coding makes sense to me" (DC).

One of the participants provided a practical example, when MM made the point that "the science department said we are going to designate this lab as a level 2, bio containment system... now we are doing level 2 research and no work was done to make sure that that space was actually compliant for the level of work .. so from my stand point, this guideline brings us a tool as we move forward and the next time we build a building what are we doing to make sure that we hit whatever an appropriate benchmark is for our BACS as it exists in this space'" (MM).

Nevertheless, there were opposing views. For example, DC felt that the use of one word descriptions might not be enough to relate to identify what is the difference between marginal and critical or high and extreme. He stated, "I have to get back to the kiss method" (DC). Also, as DE made the point that "every tenant brings baggage, so lawyers, they bring their own risk... oil and gas, so they bring their own different share... in protestors, everybody brings their baggage to some extent... they are always going to have to modify their own behaviours … Experienced step up the level of security on an individual system once you cross the balance, the integration point" (DE).

Furthermore, KK raised the point that:

> "The challenge is you've got a commercial facility, you've got folks doing classified work on a particular floor and you could have a dentist office, so what do you do from a BACS perspective, the approach we are taking is whatever the highest requirement is within the building across the board. I don't care who else is in the building, the most important thing is [treatments] gets applied to the building as a whole" (KK).

Integration with Risk

A theme that developed from the focus group was the integration of risk when assessing the criticality of the facility and subsequent, mitigation strategies.

Typical discussions that focused on or around risk related to the level of criticality rating. For example, KK suggested that there is "a big culture component to it .. what's important, here's the threat, you guys need to understand why it is important that we go through this process as painful as it can be" (KK). Whereas, MM went further:

> "I also think that the initial risk template helps drive that process, so we have got the guys on that floor that are all with intelligence and they acknowledge, they understand what our parameters are, they approve of them or they don't, and they recognise that the vulnerability is generated by the less secure tenants on other floors, and if something were to happen they would be like you guys did what you committed to do and no harm no foul and that's on us for whatever reason; or is it a floor full of lawyers that sue you, because their HVAC went haywire, that might be a different cost vulnerability" (MM).

The other participant's views focused on risk, but in a different context. As SD stated, "the financial question I thought would be, especially with a multi-tenant situation, if you've got a tenant that is a 1 and another tenant that is a 4 or 5, it's simple proportionate amount, if you have risk across that whole thing, the tenant in the lower level pays a proportionally lower amount then the higher level" (SD). MM clarified their view, with "I guess the question for me is, I don't have that situation, if you have a multi-tenant situation where the guys on floor 9 are a 4 then is this tool going to be driving people to say then the building needs to be at a 4" (MM). Consequently, general support was found across participants for the criticality matrix and supporting BACS Guideline to establish where the building as a whole sits according to the threats which pose a risk to the facility or building.

Nevertheless, there were some opposing views on where and how risk related to the Criticality Matrix. As EP raised "I was thinking I am used to a risk assessment being done where you are assessing the level at the question rather than having the questions pre-levelled" (EP). They went further, with "I'd be open to hearing this is the way we are used to doing risk assessments, but I'd be open to hearing why it was put backwards .. and maybe you guys are expecting to obtain this information, what you were hoping to get. Why you thought putting it by levels would be beneficial?" (EP). The levels were explained as a decision-making tool, to provide a means for articulating cost benefit analysis in terms of risk. As other participants identified, a risk assessment does not necessarily identify all treatments, as there needs to be a tool or guide for what to consider. It was articulated that the Guideline was not a "law", but a decision-aiding guidance tool. This explanation was accepted and supported across the focus group participants.

The Criticality Matrix provided a guide or tool to assist facility and security professionals in articulating their type of facilities. In general, there was support amongst the focus group participants for the Criticality Matrix's categories, with Government Operations, Business Operations, Board/Executive, Financial, Reputation, Life Safety (now Duty of Care) and Regulatory. Furthermore, in general, there was support amongst the focus group participants for the Criticality Matrix's levels, ranked from *low* to *critical*.

The focus groups supported that professionals are assessing risks to facilities, but not specifically to BACS in the absence of a standardized framework; however, risks to buildings was a major theme. Broadly, the participants did not understand predefined levels for building security. Nevertheless, they accepted the premise and note the value of the Guideline's criticality or impact matrix. In addition, occupancy was raised as a possible Criticality Matrix category. Financial was also raised with the suggestion that the Guideline needed to include an explicit statement that the Assessor/s provides a financial framework, for example a cost value against each level based on their context.

10.3.2.3 BACS Security Questions (Appendix B)

The BACS Guideline developed a list of security mitigation strategy questions (BACS Guideline's Appendix B), increasing hierarchically in security strength and threat focus with a rating from *low* to *critical*. These security questions aligned with the Criticality ratings in the Guideline's matrix. Therefore, participants were questioned regarding the applicability and usability of these security questions.

Participants' responses were positive and the security questions broadly supported. For example, MR stated that they "saw these at the session yesterday and thought they were pretty solid." (MR). Furthermore, when the participants asked if this was achievable, KM responded with "I've been living it for the last two years. We have gone from the Flintstones to the Jetsons in two years and reading this today [the Guideline] I felt very confident that we've done a lot of these steps. A couple on there that I had question marks next to that I'm going to follow up on just to close that gap, a couple of years ago it would have been very different." (KM).

A couple of the participants also suggested that the Guideline questions were useful for their analysis and review. For example, one participant stated that "I feel like the survey was good for me, again I took a copy of it to go back for some self-analysis, I'm using your matrix, I thought it was good, I'm glad I joined this focus group, I thought oh why would I do the systemology piece but it takes me out of my comfort zone a bit so I thought it was good' (KM). Furthermore, VL extended this view with "I'm looking at actions that I normally wouldn't and kind of expand my thought process because a lot of these coming from the security background, obviously and facilities, I have touched base on that and it lets me expand my knowledge on it as well and see how integrated those can be" (VL).

There was some concern regarding the weight or focus of various mitigation strategies. For example, KK made the comment that "If I'm in a higher crime area, I'm going to focus more on physical controls .. if somebody sits down and thinks through what types of threats they are facing against vulnerabilities, they will have a better idea of what they should be focussing on" (KK).

Comments from participants covered most security questions, but were primarily focused on the cybersecurity questions. Nevertheless, these also covered security risk management, policies and procedures, physical security, segregation of roles, network separation, cybersecurity, incident response, continuity planning and maintenance. In addition, the Guideline's methodology and structure was discussed, considering aspects such as briefing the executive, a score card approach and even a maturity model.

Security Risk Management

One participant supported the approach that a specific BACS threat assessment should be at a higher rating level by stating that "if you are starting to talk about threat assessments at level 4 and 5, I would say bring it in around that level, it would make sense" (MM). However, another opposed the view that a threat assessment should be a higher security strategy. AW stated "One of those things that can probably get a lower level .. was whether or not you undertake a threat assessment, I think as part of the risk management approach you still have to understand what the threats are so you can appropriately gauge what level you should be at in the first place" (AW). Consequently, the group agreed that this would sit at level 4.

There was comment made on the risk of an insider threat, which the Guideline does not explicitly address. TC asked if there is "anything with the BACS and the insider threat, do you compare it at all to insider threat, in some of your terms you don't want this to be, all this gaining access when it comes down to people inside or outside." (TC). However, this was explained to be captured generally at lower levels, and explicitly at higher levels, along with being braced by a BACS threat assessment for level 4.

Another aspect raised by a couple of the participants was how and when a threat assessment takes place. The Guideline currently requires a "threat context statement" at level 4 (extreme) and that there was possibly a language or definition issue. As KK stated "I'll play devil's advocate, I think it is kind of how you define a threat assessment, we participate and have close partnerships with folks but the individual that did the threat assessment for our recent risk management work, it was more based upon the vulnerabilities that had been identified, taking scenarios" (KK). Such a view was supported by MM, "the issue is a language issue, targeted assessment rather than" (MM). In response, it was noted that the Guideline's security questions level 4 posed a specific "threat context statement"; however, TC responded "I don't think anybody will understand that, I don't" (TC). Again, the issue of cross cultural terms and definitions was raised, supporting the necessity for a glossary.

Policies & Procedures

An aspect of policy and procedures was raised, where one participant suggested that "in our language, we use the terms differently... we lump policies and procedures together. When you say redundancies .. you have written endorsed security policy, do you have written endorses security procedure – a lot of the time policies and procedures becomes one meaning" (VL). Another stated that "you have asked that question a couple of times do you have a policy/ procedure for that." (KM). It was explained that the terms from a language perspective are significantly different, where policy is an overarching organisation intention and procedures are instructive ways to achieve tasks. Acknowledging that some organisations publish these as joint documents, the core meaning is very different.

Physical Security

There was supportive participant comments made on the physical security questions. For example, KK stated that "physical security right, there are things in here that made me think about putting tamper seals on the cabinet that has Controllers in" (KK). One of the facilitators responded, "Well Controllers need to be in their own box that are tampered" (DB), in which KK stated "Oh they're in their own box it's just the key is sitting in the lock."(KK). KK voiced their concern, when suggesting that “I still worrying about someone being about to pop into one of our switches in a closet, same physical security problems” (KK).

Separation of Networks

There was general comment by participants regarding separation of networks. For example, SD explained that “We have several clients where their server is a totally different network, there is the main BACS for the building but there is a BACS just for the server. There is a gap there, there is no kind of connectivity between the two at all: (SD). From a different but supportive view, MM added that “I think it’s a fair question, we don’t have that level of isolation. The xxxx won’t pay for separate” (MM).

Such an isolation view was favoured, where “Yes, isolation for us... and then recovery to be able to operate it manually until we find out what the cause [problem] is but isolation is first, and then we have a manual operation second, for the most part we pick it up when we fail to see something we can’t control or we spot something we can’t control” (DE).

Cybersecurity

There was general comment on the various cybersecurity questions at different levels: however, there was no single question or issues that resulted in significant discussion or disagreement. Nevertheless, one participant suggested the need for the “elimination of manufacturers’ back doors.” (DE). In response, it was noted that in Level 1, a questions does state “Has the factory or default password or other logical access enabler been deactivated” (p.10).

Another participant suggested “one thing that jumps out at me, Secure Id... on page 11 state secure id key, I wouldn’t limit it to ours. Really you are after multi factor personnel. Just not a particular vendor, you are after multi factor right” (KK). This view was further supported by TC, who suggested the use of “multi factor authentication” (TC) and KK with “citrix provides us the ability to do true role based access, active directory and adds a layer on top of that, gives us the multi factor” (KK). Therefore, acknowledging the participants views the Level 1 security question was adjusted to read multi-factor security ID key”.

One participant also highlighted a need for a “question on penetration (PEN) testing” (MR). Therefore, PEN testing was considered a valuable point for inclusion at one of the higher criticality levels, being inserted as a Level 4 security question. Then, in regard to Level 1 “session time out lock”, a participant extended this questions with “there’s the session disconnect, where I’ve logged in, I’ve authenticated based on activity when does it turn off or disconnect the session; or I think the other part of the session time out lock when does the screen lock based on lack of activity” (KK). However, there was limited support or additional comment on this security factor, which resulted in this comment not being added to the Level 1 (low) questions.

A Level 1 security questions on software patching was also raised by a couple of participants. For example, KS posed the question, “does it get patched when it needs to be patched? That is just the IVPN for remote access but there are so many” (KS). Another participant followed this lead, raising the issue with patching by stating that “patching, again that is a huge issue with respect to xxx” (KK).

One participant commented on the Level 1 BACS back-up. They stated that “I don’t know if there are backups or you talk about stuff like that in Level 1. To me there are some very basic things … We went into a building the other day that had our old XXXX system, the computer crashed and the building tech said don’t worry about it, as we have a good back up... but the backup was dead, no software backup along with no maintenance on the system for five years” (KK). KK expanded their comment, with “who was responsible for the backups, whose responsible for ensuring the scheduled maintenance plan, as a level 1 question, whether or not it has it is kind of like who is doing it and this goes back to what you mentioned early, who is responsible for what" (KK). Should this be included in level 1 (low) was posed to the group, with a result hat a questions of BACS back-up was inserted into Level 1.

The aspect of "network" monitoring was further raised by TC. TC commented that "*monitor on a real time basis* .. seeing alarms go off a lot of the time it's a false positive and nobody is really checking anything, I just see that as a huge vulnerability" (TC). However on review of the security questions, this requirement suggests the need to monitor the intruder alarm at Level 3 (high).

Finally, KK raised their concern that "I'm looking through the level 2 stuff and my gut reaction is I don't know how anybody is going to meet any of this still. Especially when it comes to authorisations added in, anomalies investigated to me that is a more mature model" (KK). Again, it was reinforced that the intent was a guideline that articulates the research informed requirements, and that organisations must make their own decision regarding their levels of security unless mandated through a regulatory environment. The guideline is a tool to aid informed decision-making, not a rule book. This point was accepted across this specific focus group.

Segregation of Roles

One of the participant's raised the issue of segregation of duties and roles across the broad BACS practice areas in facility and security. MP stated "Giving the fire tech access to the access control system at a certain level rather than segregating access by policy within the system" (MP). The response to this comment was that "in theory they can get to all the other sub systems due to the connectivity within the BACS, but as a base level" (DB). MP replied, "At a higher level look at possibly segregating users to what their function is within the system itself rather than having someone that works on air condition has access to the badging system" (MP).

Incident Response

One participant raised the issue of "how do we isolate that system so it doesn't reach the other systems and still continue to run the buildings, run it manually." (DE). Another commented whether "incident response training providing the BACS system a response, because that is something we do." (VL).

One participant suggested if there was a need to "have the ability to operate the [BACS] system manually, should an issue arise?" (DE). A counter-questions was asked if this would be necessary at a low or moderate level facility, where MM responded with "yes, I would put it in low level" (MM). Therefore, a security question that addressed the ability to take manual control of BACS functions was inserted into Level 1 (low) under the category Incident Response.

Maintenance

One participant supported the need to consider maintenance and in particular, an asset register that includes BACS. KK stated that "You can't start to talk about... BACS enclosures if you are don't know where they are at [located] .. I think there are a lot of things here that if you don't have an asset list" you would miss (KK). The participant went further to state:

> "part of it, again it goes back to the asset list, (for me) there was nobody within the company that we could go to that could give us a list of where all our remotely accessible IPs were ... nobody knowing what's actually hooked up to the internet and how the buildings are connected .. You have to have a starting point to apply this stuff, we can put all the policies in place that we want to, but it doesn't matter at the end of the day if it's

> not getting down to the building tech who may have hooked something up and they went to best buy and they bought a switch and they hooked their switch up so they could surf the web because they are bored in the middle of the night." (KK).

Briefing the Executive: A Score Card Approach

A theme that developed from the focus group was the need to be able communicate the Guideline findings, or more specifically, security gaps to senior or executive management. A number of the participants raised the ability to quickly and effectively brief and educate their executive with the issues found by the Guideline review. For example TC stated that "there is a huge lack of understanding at the top" (TC). Another supported this point, that the "focus with our CEO/CFO is on enterprise risk management of which cyber is one of maybe 10 things" (KK). Therefore, "where are the priorities of enterprise risk management, where does it fall" (TC). The focus was "what are you trying to protect or what problem are you trying to solve. Those two are very broad, but it should start the focus" (TC).

There was general consensus among the participants for a simple method of presentation. MR asked if "there was something you can take, really just shrinks this down so I can pitch this in the elevator, so I can show them a quick picture" (MR). One participant suggested that if "we fail at this level and then that is when you make it with the other chart and say we fail at this level and the impact is potentially a mess" (MM). After some discussion, VL suggested that you could "put the questions direction from the sections and add them to a PowerPoint presentation... and say these are the questions we need to focus on" (VL).

A Score Card Approach

The participants need to brief their executive extended into how to make a simple template approach, with some type of score-card. Consequently, participant MR suggested "the electric sector cyber capability training model, that has these donut charts at the end ... we actually did lots of pink, green. With BACS it went red across the board, we showed our executive that and said this is what happens when you don't do security vulnerability assessments, so I was able to really get that message across because when they could see the power point slide" they understood (MR). Such an approach was supported, when "argued that you can do that to some extent with... a little work .. if you can take this and say there are 35, 50 odd points of level 1 security, we passed 51 of 51, medium we were at this point and build it into a score even though it's not really a score" (MM).

Another participant suggested "a stop light - red/ yellow/ green. There is risk at an acceptable level, there's risk at a level to which we are not comfortable with but we are managing, or there's risk very high, right now we are working through it ... we are having the conversation and it's at least tracking it at a corporate level but the building system stuff was on nobody's radar" (KK).

Such a score card colour approach was supported. For example, VL suggested that "you have a colour at this point and if you are an orange company, then we need to add up to level - to level 4. If you are a 2 then we just focus on the first section. This makes a lot of sense structure wise. I also kind of like this layout" (VL).

In response to these comments, a score card template was drafted for the Guideline (Appendix 3).

Maturity Model

The participants not only suggested that they needed guidance to brief their executives, they also needed a method to gauge and track their BACS security and its vulnerabilities. Using a score card, where the assessor ranks the facility criticality and follows the relevant security questions for compliance. This lead to a robust discussion around the need and implementation of a maturity model.

As one participant suggested, "which is why we went down that path is that framework you assess where you are at, you develop your target and figure out where your are and you develop your action point and we recently went through it and it was the first time the company had gone through .. a security assessment to include the building systems" (KK). This view was supported, when TC stated that this approach "goes to a maturity thing that you're talking about" (TC). TC expanded on his point, stating:

> "Because all of this to me, if you are doing an intelligence plan or maturity plan it has to be collaborative because in every aspect of risk whatever you are talking about means something different, it's got change, change is pocket change, organisational change, change my clothes, it's kind of like that so everything that you are talking about that potentially impacts the rest of your organisation has to be done in a collaborative environment with a focussed process for it to work" (TC)

Nevertheless, there was some opposition, for example a question was raised, is there the "criticality or maturity of the organisation to be able to do it, arguing It may be critical but it may not be possible" (KK). And TC aligned policy with operational needs, stating "When I was reading the whole thing, it asks for policies, my stuff is more operation and management than technical, so the one thing I didn't see was who knows about it, you can have a policy that is not operationalised?" (TC).

The participants were supportive of the Guideline's Security questions (Appendix B) and their assigned criticality levels. Nevertheless, some questions were adjusted to be more concise, or relocated in their criticality level. However, what also emerged was the issue of language and/or definition issues with both BACS and security terminology. In addition, a majority of participants wanted guidance in how to communicate the outcomes of the BACS Guideline assessment to their senior executives.

To aid executive communication and provide a benchmark, it was proposed that a score card template, based on the ranked criticality rating of the facility and followed by the compliance to the relevant security questions, be developed for inclusion in the BACS Guideline.

The aspect of segregation of roles and functions was also raised, in particular due to the broad and diverse practitioners that may have to have access to parts of the broader BACS and its network.

10.3.2.4 BACS Vulnerabilities

The previous project stages developed a list of generic BACS vulnerabilities, presented in a tabulated format. This tabulated approach was summarized for the Guideline Questions. The participants were questioned regarding these vulnerabilities, their applicability and usability.

Most of the focus group participants felt that these were appropriate, but the format received queries. For example, MM stated that when it comes to "my physically security supervisor, I mentioned BACS his eyes glaze over... this security person doesn't necessarily understand BACS" (MM). Following this, one participant suggested that these vulnerabilities could be converted from tabulated to case study. "I might even suggest you include case studies on what a BACS is, to help the reader understand why they are even looking at this document, a similar model for some case studies on vulnerabilities just to highlight that would be helpful." (MR).

One participant commented on one vulnerability, namely wiretapping and general understanding of this term. Their concern was with general understanding, as "we all know that but I suspect a lot of the BOMA people would be like I don't know what that means, not necessarily inappropriately not know what that means" (MP).

The participants supported the Guideline's generic vulnerabilities; however, there was agreement that to improve general understanding of BACS, the Guideline's generic vulnerabilities should be rewritten as case studies.

10.3.2.5 BACS Guideline Instructions?

Focus group question 9 asked the participants: *Are the Guideline instructions clear and easy to follow?*

The participants were general supportive of the BACS Guideline. For example, one participant stated:

> "From a training stand point to .. I could bring in someone who works at a lower risk facility, put the guide in front of him and say you are going to learn this section. And then as I promote from within I go okay well now you are moving up to these questions and you could actually use it to bring people along … security licensing is minimal in the state, in house security training, on the job training is critical and bringing in a document like this where I can use it to train future supervisors, as a shift leader you can be responsible for section 1 and then you are going to consult with me on section 2 then 6 months to a year from now you can do 2 and 3 consult with him and I will do 4 and 5, use it to bring along and groom" (VL).

However, KM suggested that "You could streamline it a little." (KM).

10.3.2.6 Not all Facilities are Equal in Risk

Focus group question 10 asked the participants: *Acknowledging that all facilities are not equal in risk, do you support the level-based approach developed?* There was a nil response and risk was covered in the BACS Guideline Criticality Matrix and Security Questions sections.

10.3.2.7 Suitability of the BACS Case Studies

Focus group question 10 asked the participants: *Are the BACS case studies (pages 2 to 3) useful and do they support your understanding?* There was a nil response to this posed questions.

10.3.2.8 Suitability & Usability of the Criticality Categories

Focus group question 13 asked the participants: *Do the BACS mitigation questions (see Appendix B) make sense and could you apply these?*

This question extended the Focus Group question 8 (see section BACS Security Questions (Appendix B), although themes developed from this question. The participants were asked if the security questions sub-heading or categories were useful and made sense. These categories includes, management, security risk management, personnel security, physical security, etc. KM provided a positive response, responding "I think they apply" (KM). Furthermore, VL stated that "I like the fact that its physical security... okay now we are looking at cybersecurity" (VL). Extending to suggest that "It also signals to me that if I'm not cybersecurity specific I'm like okay I'm going to need to ask questions here" (VL).

The participants went further, with "If you are dealing with management, someone who is fairly new to the system and doesn't understand this setup, like just a company manager or CEO or someone like that, they can look at it and be like physical security, answers this question for me, they can delegate easier, where is my cyber guy - hey come and look at this section". KM: agreed with "exactly" and that "It's table talk, so it gives you that conversation piece to ask direct questions" (KM).

10.3.2.9 BACS Guideline Modifications

Focus group question 14 asked the participants: *Would you like to see any modifications (additions or removals) to the Guidelines?*

The focus group participants were asked if they have any suggestions for improvement to the Guideline. The participants suggested updating one of the figures.

Update BACS Architecture Figure

One of the participant questioned the validity of the BACS Guideline's architecture (see BACS Guideline Figure 2). The participant commented that "consult with the different architectures that have been employed today. This is good legacy stuff." (SS). They went further, with "you see management level there are no work stations that are used in a device to private cloud environment, there are just terminals they are just displays, they could very well be just tablets, in fact most of the time they are tablets" (SS).

Nevertheless, they did generally support the architectural figure, as "you've got a great architecture for what is going on today, most of the stuff that is going on today, what is getting deployed though in large buildings are device to a private network so to speak. It is not even a private cloud but you do have some gateways and data communication points that have some smarts and cyber hardening but its more about a fog" (SS)

10.3.3 Focus Group Themes

Focus group question 15 asked the participants: Do you have any *final comments?* Final comments allowed the focus group participants to vice any final questions, concern or suggestions.

The intent of the focus groups was to allow the participants to have an open forum, bounded by semi-structured questions. In other words, the Focus Group Questions (see Appendix XX) provided the participants with an understanding of the questions prior to attending and gave the facilitators structure in posing probing questions. In addition, this approach allowed both the facilitators and participants to extend beyond what was expected. The result is a number of additional BACS security themes that developed including some unexpected vulnerability concerns across the focus groups.

The additional themes included security zoning, background or pre-employment screening and a silo-approach that is contradicted through technology convergence.

10.3.2.1 Security Zone Issue

A theme that developed from the focus group participants was their understanding and application of the term *security zones,* extending from the BACS Guideline use of "zone" in its security questions.

The participants were asked if they use or understand a general national security hierarchy for building access for national security. It was commented that "in Australia we have an actual defined level of zones" (DB). Participant MP responded with "if you go online you see top secret, secret, confidential and classified, and there's all this stuff in the middle... you've got special access programs, you mentioned skiff, sensitive information, intelligence information" (MP). In reply, DB stated that these are “almost access levels, they are not zones” (DB). A zone could be considered “a whole three dimensional space so the floor has to be a certain physical nature, the roof has to be a certain physical nature, all the doors entry points” (DB).

Zones are defined by the American Institute of Architects Security Planning and Design Guide as layers of concentric defensive rings that go from public to semi-public to private zones, where security is applied to these primary lines of defence, as well as areas between. Zones are the division of space based on threat and criticality within a security context.

One participant raised the point that “We have an access area, high risk area or high security area, it becomes a zone a lot of times, we can list it as a specific room, this is a resource room” (VL). In contrast, KM stated that “We have general access, we have preferred access and then we have data centre access and then wire room access. So we try to keep it, we had 213 in the past access policies, we have got it down to 100 now. They were trying to give access policies to every single thing separately” (KM).

There appeared to be a lack of participant understanding of the term *security zone*. For example, KM stated “So what is the zone then” (KM). VL suggested that zones are “the rings of the Pentagon, at a certain level you get into 2, you get a certain level you get into 3, you have to have this level of access to get all the way inside” (VL). General discussion ensued, where one of the facilitators provided an example “in our research area, we have a zone 4 so it’s only one large area, but it’s a zone 4 so everything from that point, so you can’t take a laptop in there you can’t bring a laptop out without special authorisation, so it’s a security zone” (MC). VL responded, stating that “I like that idea a lot better” (VL) and this view was supported, with “We have never ranked it as a zone, that is interesting to me” (KM).

One participant raised the point that in the Guideline, “it mentions zones in 3 but in 4 entire risk, being security zoning for BACS at [automation and] management levels” (MP). In response, DB suggested that “it’s a whole three dimensional space so the floor, consistent with the zoning principle, has to be a certain physical nature, the roof has to be a certain physical nature, all the doors entry points” (DB).

The discussion on security zones led to the theme of compartmentalization. One participant stated that “when you compartmentalise everything you reduce risk of insider threat to gain access to all” (MP). In response, the facilitator suggested that “perhaps compartmentalisation could be a better term, because people would understand that perhaps, because it’s just a compartment” (DB).

The benefits of security zone were discussed. “From a security standpoint in the corporate world it would be much easier to consolidate the zone 5 stuff in the one building because then I can focus on that, if this is a zone 1 building I don’t have to expend resources as much. If I have multiple buildings on campus then this is a zone 1 building this is a zone 5” (VL). Whereas, “A call centre is a real zone 1 right?” (KL).

10.3.2.2 Background or Pre-employment Screening

Another theme that developed from the focus group participants was the consideration of background or pre-employment screening. For example, KM posed the question “if I recall was ‘do they do background checks on these vendors’ and that is part of our contractual agreement with that company but you’re kind of at the mercy of them doing the background checks” (KM). There was confirmation that in the Guideline that BACS maintainers are pre-employment screened at Level 2 (Moderate), but extended also repeated at Level 4 (Extreme).

Nevertheless, this does not remove the reliance of the third party undertaking screening and maintaining appropriate assessments. As MP suggested, “that’s how the target data is .. that guy has got connected to the HVAC guys and their systems and you can be targeted that way" (MP). Another participant added that "it is interesting because this brings up something that was discussed in another workshop I was in yesterday... they were talking about how for security companies bidding on contracts in this country [US] there has been a proposal to issue them essentially like a ficard credit score number .. if you don't have a score for your company wide as an 800 then you can't even bid on that contract" (VL).

10.3.2.3 Silo-approach, with Technology Convergence

Some of the participants' views were that BACS were both operated and maintained in a silo-approach; however, technology was converging, meaning this approach is outdated. For example, "We also found in a cybersecurity assessment last year that there was zero cybersecurity control, IT wasn't aware of the systems that were out there cybersecurity focus, BACS systems that were there so it's really popped a light for us on that one. It's a gaping vulnerability because it's been siloed off" (MR). Such a view was clarified, with "it's on a network, so I actually see that it is split between facility and IT" (SS).

Nevertheless, some participants still felt that BACS is a cluster of separate facility systems. For example, "they see the guys on the ground and they still refer to it by individual system but at the end of the day they are overseeing an integrated, focal point, very rarely does it fall to the operations team" (DE). DE went further, as "It's still the security people .. that operates the security systems, CCTV systems, we manage the ports, switches and so forth" (DE).

One participant, continued "I can speak for myself here and my company, I can say 40 years ago when automation just started to take off everybody was in their own silos, we kind of still are even in this advanced stage of technology today, however we see a lot more interface between the two, we currently don't do a lot of it yet but I've seen in the last 5-10 years more security folks from my world get a little more involved in the BAC system and vice versa" (SS).

Security practitioners have no or a limited understanding of the term "security zone". Yet this is a major security strategy for articulating different levels of security requirements. That is, security zones provide a methodology for physical and logical security mitigation, based on the security threat and risk assessments. Zones are a guide to develop a facility and its rooms physical security plan. Application of requirements based on the business impact level of any compromise, loss of integrity or unavailability of information and physical assets within zones gives assurance in information and asset sharing arrangements.

Pre-employment screening or background checking of BACS Maintainers is generally undertaken by a third party, being the Maintainer. There has to be assurance in compliance and maintenance of this process. Furthermore, BACS management remains in silos across the organization, between facility, information technology, cybersecurity and security professionals: however, BACS are converging due to increasing integration of technology. In other words, BACS is siloed in the organization that is contradicted through technology convergence.

Many security practitioners have no or a limited understanding of the term “security zone”.

Security zones provide a methodology for physical and logical security mitigation, based on the security threat and risk assessments.

Pre-employment screening or background checking of BACS Maintainers is generally undertaken by a third party, being the Maintainer, with limited assurance in compliance.

BACS management remains in silos across the organization, between facility, information technology, cybersecurity and security professionals.

10.4 CONCLUSION

This stage achieved two key outcomes; the first, to critique the Stage 2 findings and second, to allow a critical review on the ability of practitioners to understand and apply the BACS Guideline.

In general, the security and facility participants supported the findings of Stage 2, especially that security professionals have limited BACS responsibilities but are users. Furthermore, that security and facility professionals have a limited understanding of the BACS technical architecture and therefore, resulting vulnerabilities. In addition, that security and facility professionals have a different understanding of BACS, directed by their use, function and responsibilities. However, the majority of participants agreed that BACS Integrators hold a high level of technical understanding, but are only considered in a service and maintenance function rather than a mitigation advisory role. Another theme that emerged was a lack of common understanding and clarity of language with BACS and security terms and practice.

The participants felt that the BACS Guideline provided a robust tool to aid their understanding, raise questions for their consideration and supported organisational decision-making. The criticality rating scale (see BACS Guideline Appendix A), to assign a facility risk level, proved generally well received, as were the security questions (see BACS Guideline Appendix B).

Amongst the participants, risk to facilities, occupancy and communicating BACS risks to their executive become a focus of discussion. What become apparent was that BACS remains in silos across the organization, between facility, information technology, cybersecurity and security professionals. The focus group participants supported the development and publishing of a standardised BACS security guideline, and praised the draft guideline put to them in the group sessions; supporting the BACS Guideline as the model to move forward with. It was agreed that with minor refinements, the proposed BACS Guideline would become an essential organizational security decision-making tool that would assist organizations to manage the threats which pose a risk to their business objectives.

Section 11. Project Findings

11.1 INTRODUCTION

Building Automation and Control Systems (BACS) technologies have become embedded into the majority of the contemporary built environment. BACS technology and its connectivity extends across all types, sizes and functions of built facilities for the purposes of information and automation. Through connectivity, BACS functionality and its flow of information also extends across the organization, interconnecting many diverse departments. However, limited organizational awareness and understanding remains concerning BACS, their reach across the organization and importantly, the threats and vulnerabilities BACS potentially embeds into the organization.

This section provides a response to the project's defined Research Objectives. These include an overview of BACS, the various types and technologies, an evidence based understanding of security and facility professionals' BACS understanding, technological exploitation awareness, and demonstrated security practices. These responses are collated into a single usable document that interprets and summarizes the research findings through a hierarchical decision tool, as a functional aide memoir for security and facility professionals to ensure that the threats that pose a risk from BACS connectivity can be managed accordant with organizational expectations.

11.2 PROJECT OBJECTIVES

The purpose of the project was to meet the following Research Objectives:

1. Develop a meta-literature basis of current BACS, including their terminology, architecture and associated vulnerabilities,
2. Gain an evidence based understanding of the security and facility management professional's awareness and comprehension of BACS vulnerabilities, their criticality and associated security practices; and
3. Provide a summary guideline to support security and facility professionals' decision-making when undertaking BACS design, installation and security management activities.

This section addresses each Research Objectives in the following sub-sections.

11.3 PROJECT FINDINGS

Findings are divided sequentially into three discrete sections, each responding to one of the Research Objectives. In addition, a fourth section provides findings on security zones that developed as a theme during the project.

The first section, meta-literature review of BACS (Section 11.3.1) identified numerous BACS amalgamation and terminology, a large commercial market, and data set of generic vulnerabilities. Then, an understanding of security and facility professionals' awareness of BACS technologies, security vulnerabilities and their organisational criticality significance (Section 11.3.2) was gained, along with associated security mitigation measures. Findings for this stage highlighted participant's lack of robust technical knowledge of BACS, along with the associated criticality of technical and procedural vulnerabilities resulting in increased organizational security risks.

A BACS Guideline (Section 11.3.3) was developed and critiqued, to provide an aid to decision-making by security and facility professionals, towards better mitigation and communication of BACS threats and risks. Finally, the concept of security zones (Section 11.3.4) was identified as a concept that requires greater understanding, in particular, by security professionals.

11.3.1 Literature Basis of BACS

In response to Research Objective 1, *to develop a meta-literature basis of current BACS, including their terminologies, architecture and associated vulnerabilities,* a critical literature review was undertaken. The review included many BACS aspects including variations in BACS language or labels, and different types, combinations and equipment of these systems (see Section 3). In addition, the review included BACS technical and software architecture (see Section 4), the BACS manufacturing market (see Section 5), and the Integrators service and maintenance approach to this market. Finally, a synthesis of international standards was also provided (see Appendix B), further supporting such variability in BACS management.

What are BACS?

A Building Automation and Control System (BACS) is an automated building system that converges and integrates (connects) many different building technologies through information flow processes to a central monitoring and decision point.

BACS are also known by many additional terms, such as a Building Automation System (BAS), Facilities Management System (FMS), Energy Management System (EMS), Building Management System (BMS), Intelligent Building (IB) and today, Smart Buildings and Smart Cities; however, the core principles of BACS remain the same, regardless of name, to facilitate data communication and automated decision-making through connectivity. Therefore, "Building Automation and Control System" (BACS) was considered the most preferred term.

BACS Technology & Architecture

The technology and architecture of BACS is related to the scale of the built environment system. BACS varies from a low level, automated home heating system to a complex high rise Intelligent Building, which centrally monitors, automates and controls all building system functions including HVAC, lighting, elevators and life safety systems, along with maintenance, administrative and business functions. Today, security is also becoming embedded within the function and business of BACS resulting in connectivity across traditionally isolated systems.

Furthermore, with the advent of the Internet of Things (IoT), BACS will continue to expand into more diverse and complex areas of everyday life management. Connectivity through the IoT means, in simple terms means that any life activity or functionality concerning the built environment will be connected and integrated in the future.

Nevertheless, BACS are modular in nature, formed from the integration of a number of devices, equipment and communication platform networks. Consequently, the BACS technological architecture is thematically based on three levels, of Management, Automation and Field device. The Management level contains the human interface, connected via the enterprise software and communication network i.e., the Information Technology network.

The Management level of BACS equipment includes workstations, network switches and servers. The Automation level provides the various primary control devices, connected via networked Controllers and operating via open source communication protocols. They provide the interface between the BACS physical field devices and the Management level human interface. Examples of automation equipment includes Controllers and Routers. The Field device level provides the physical sensor input and output devices, such as sensor or activators connected to specific plant and equipment.

Common Communication Protocols

BACS use common and open communications protocols to achieve connectivity, which includes signalling authentication, error detection and correction, data transfer, and semantics and synchronisation of analogue and digital communications. Open communication protocols enable the integration of many different sub-systems and devices for the purposes of connecting, monitoring, deciding and controlling. Some common industry standards and protocols include BACnet, LonWorks, File Transfer Protocol (FTP), Transmission Control Protocol (TCP), Internet Protocol (IP), User Data protocol (UDP), Hypertext Transfer Protocol (HTTP), to name a few. Such open protocols facilitates nefarious actions in BACS connectivity and communications. For example, with one of the most common communications protocols that extends across the BACS Automation and Management levels, namely BACnet, there are many open source programs available on the Internet to read and write to BACnet controlled networks.

BACS Market

BACS are growing at approximately 15 to 34 percent per year, due to the demand for energy and operational efficiency, reduced maintenance, and the greater monitoring, control and operability. By 2022, the BACS industry will be worth an estimated $104 billion. Such growth highlights the current and expected impact that BACS will have in most future built environments, which if the security management of is not considered will expose organizations to harm.

Furthermore, the growth of the BACS market is also driven by the medium to long term requirement to save resources with improved efficiencies and environmental targets imposed by governments. With global rises in energy costs, pollution sanctions and green government incentives, BACS initiatives are at the forefront of the majority of future facility projects.

BACS Vulnerabilities

Vulnerabilities represent an aspect of the BACS architecture that can be exploited for nefarious gains. Due to their connectivity and common language protocols BACS are prone to technical and physical attacks at all architectural levels, although the Automation level could be considered the most vulnerable. Consequently, BACS vulnerabilities have been presented in the three architectural levels of Automation, Management and Field devices (see Appendix A). These vulnerabilities were extracted and tabulated from the reviewed literature.

A failure to understand such vulnerabilities means that organizations are exposed to security risks unknowingly. Therefore, the project sought to uncover security and facility professional's current awareness and understanding of BACS vulnerabilities, towards identifying any gaps in the knowledge and educational requirements.

11.3.2 Understanding BACS Awareness & Practice

In response to Research Objective 2, to *gain an evidence based understanding of the security and facility professional's awareness and comprehension of BACS vulnerabilities, their criticality and associated security practices*, surveys and focus groups were carried out. This section extends the Research Objective to a number of discrete themes, from BACS awareness, the role of Integrators, the professionals' function, roles and responsibility, security integration into BACS, the concept of integration, and finally, understanding BACS vulnerabilities and risk criticalities.

BACS Awareness

The project found a significant disconnect between expressed security and facility professionals' perceived understanding of BACS threats and risks, and their revealed actual understanding. Although 75 percent of security and facility professionals believed they had an awareness of BACS architecture, and half featured BACS risks in their group risk register, the majority of security and facility professionals displayed a limited understanding of BACS technical elements and its critical vulnerabilities.

For example, half (48 percent) of the respondents stated they had BACS and its vulnerabilities listed in their risk management "risk register". That is, they had identified and articulated that BACS poses some level of risk. Nevertheless, findings support the view that security and facility professionals do not understand the technical elements of connectivity and integration with contemporary BACS. In addition, these professionals lack the necessary information technology and cybersecurity skills to achieve a holistic state of security for such systems. Furthermore, they do not understand how the vulnerabilities relate to organizational risk criticality, although such knowledge and technical skills are held by Integrators and cybersecurity professionals.

BACS Experts

The research identified that an exception to the limited awareness and hence, understanding of BACS, was found among Integrators and cybersecurity professionals. Both of these professional groups displayed a high-level of technical understanding of the criticality of BACS vulnerabilities, especially at the different BACS architectural levels. The result being that this group could be considered BACS experts and necessary within the BACS security role.

The project found that there was support that Integrators, also referred to as Vendors, Installers or Maintainers, hold a high level of BACS technical understanding that could be drawn on by organizations to achieve a necessary level of BACS security. However, notwithstanding their skills, at present Integrators provide a service and maintenance function, rather than providing best practice operational and security advice. Therefore, advice given by Integrators may be seen as "upselling" their products and services, instead of being a strategic partner who provides BACS security advice.

BACS Responsibility

The project found that facility professionals have a greater level of BACS responsibilities than security professionals; however, overall there is greater use of BACS among different professionals within an organization than direct responsibility. Nevertheless, each professional (security, facility management, cybersecurity, information technology, etc.) generally focused only on their areas of practice and responsibility (silos). For the security and facility professionals, the technical elements of BACS fell outside their area of occupational undertaking and expertise, as did knowledge of the vulnerabilities and required security measures.

The project found that Facility Managers manage and operate BACS, with 36 percent of participating building owners and operators indicating they have such a responsibility. Whereas Security Managers manage and operate predominately the security systems, such as intrusion detection, access control and surveillance systems. Furthermore, Information Technology Managers manage and operate the technical elements of networked systems, including the broader BACS architecture and policies.

Security Integration into BACS

The project found that half (50 percent) of the participants reported BACS had integrated security systems. This figure is likely to significantly increase in the future given the expansive nature of BACS within the built environment. Furthermore, the ability to define BACS is problematic and may lead to differing interpretations and perceptions of the level and type of security system and other component integration between different practicing roles.

Findings indicates diverse views on what types of security systems integrate into BACS, which was directed by the professional being asked. Security professionals cited the most common BACS integrated security system as duress, intruder alarm, CCTV, and electronic access control. However, facility professionals cited intercom, electronic access control, lighting, radios, and

CCTV as the most common BACS integrated security systems. The understanding of *integration* between security and facility professionals' lacks definition, likely leading to a misunderstanding and therefore, siloed view of associated security risks.

What Does BACS Integration Mean?

The project found that the term *integration* is not well understood at a holistic level. Integration remains technically and functionally broad and undefined, with diverse views on meaning depending on a persons' occupational role. Consequently, practitioners focus and therefore, understanding, is generally aligned to their role and function, such as security, facility or information technology. For the security and facility professional, BACS lacks clarity of definition, in part, due to its broad range of technology and functionality.

Differences in security and facility professionals in their view of *integration* indicates a culturally defined difference between the occupational perspectives of BACS. There is a lack of common understanding and clarity of language with BACS terms and practices.

Understanding BACS Vulnerabilities

The project presented BACS case studies (see BACS Guideline) and tabulated vulnerabilities (see Appendix A) in response to the previous Research Objectives. However, the project found that security and facility professionals do not have a robust understanding of these vulnerabilities or their organizational risk significance.

The majority of security and facility professionals rely on third party professionals, or information technology specialist to provide the technical understanding and security practices for BACS protection. To manage BACS well, requires dedicated information technology professionals within, or integrated with the facilities department. BACS "third parties" may be in-house information technology, cybersecurity professionals or contractors, such as Integrators.

Understanding BACS Criticality Risks

The project found that security and facility professionals rated BACS criticality of vulnerabilities, at all architectural levels of Management, Automation and Field device, relatively equally and with limited distinction. Such a response indicated a blanket approach by the professionals when considering BACS vulnerabilities and security mitigations. These findings supported the assumption that security and facility professional lack robust understanding of BACS vulnerabilities.

In contrast, the expert group of Integrators and cybersecurity professionals displayed a divergent, and what is argued, more accurate understanding of BACS vulnerabilities and their organizational significance. This group rated higher criticality of attacks against the Automation equipment and its network.

The criticalities of vulnerabilities vary between the architectural levels of BACS components. Table 11.1 provides an overview of where the more significant BACS risks lie within the broader architecture. As indicated, the most significant critical and high risks (red and orange) lie within the Automation level, followed by moderate risks (yellow) at the Management level and finally, low (green) risks at the Field device level.

Table 11.1

BACS Generic Architectural Level Risks

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

Consequences of realized threats can be divided into three categories of loss, denial or manipulation (Figure 11.1). These consequences pose a risk to the confidentiality, integrity and availability for organizations, with possible cascading affects.

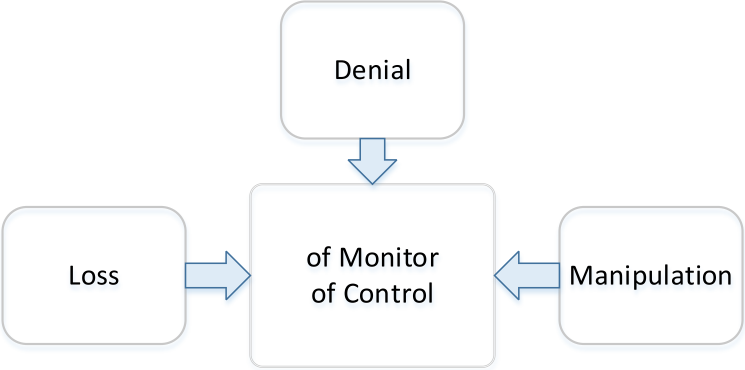


Figure 11.1 Consequences of Realized Threats to BACS

BACS risks are contextual, aligned with the facility's threat context and their functional criticality; nevertheless, as with all security vulnerabilities there are generic mitigation strategies that can be taken to protect these systems. BACS vulnerabilities are situational, better understood through understanding the facility's threats, criticalities and environmental context.

BACS Mitigation Strategies

The project found that there was a view that security and facility professionals apply the most BACS mitigation strategies. As with the BACS vulnerabilities, they generally rated the mitigation strategies as being relatively equal and with limited variance. Also, the security professionals believe they apply the greatest level of security mitigation strategies; however, given their low level of BACS responsibility and neutral understanding of BACS critical vulnerabilities, this finding lacked support. Therefore, the result suggests that security and some facility professionals do apply BACS security mitigation strategies, but do so with an ad-hoc approach and with limited total system understanding. Overall, no definitive conclusion of what security mitigation strategies the professionals apply could be provided.

Nevertheless, the expert group of Integrators and cybersecurity professionals indicated that their five most significant BACS mitigation strategies are procedures, security risk management, continuity planning, security awareness and information technology (cyber) security.

Across the literature, BACS vulnerabilities are broad and at times abstract, presented without context (situation). Such presentation results in these being difficult for practitioners to understand and mitigate against. Therefore, a contextual question must be asked: Does the security, facility or cybersecurity professional need to mitigate against all, some or none of the vulnerabilities? Given the very nature of BACS, there was no explicit response to such a question. To overcome this complex issue, the BACS Guideline (Appendix I) was developed as a summary, yet functional guidance document. The guideline includes presented case studies for ease of reading and understanding to contextualise the reader, followed by the identified hierarchically generic tabulated vulnerability treatment strategies.

11.3.3 BACS Guideline

In response to Research Objective 3, to *provide guidelines to support security and facility professionals' decision-making when undertaking BACS design, installation and management activities*, the BACS Guideline was developed and critiqued.

The BACS Guideline (see Appendix I) was developed to provide guidance to help ensure that a facility's BACS is, where necessary, protected from foreseeable threats and risks that may impact the organization. The intent of the Guideline is to provide a tool to aid decision-making, whereby security or facility professionals can address relevant security related questions to gain a level of assurance in protecting their organization, or make informed decisions to accept risk without treatment.

The project found that there was robust support for the BACS Guideline, including its risk based approach based on a criticality matrix (BACS Guideline's Appendix A) and subsequent security questions (BACS Guideline's Appendix B). During the project, some security questions were adjusted to be more concise or relocated in their criticality level. However, what emerged was the issue of language and definition issues with both BACS and security terminology. In addition, the majority of participants wanted guidance in how to communicate the outcomes of the BACS Guideline assessment to their senior executives.

The project found that there was a need to support professionals in assessing facility risks, specifically to BACS, in the absence of a standardized framework. The resulting BACS Guideline is seen to be an important publication to support security, facility and cybersecurity professionals in assessing, mitigating and communicating BACS risks.

11.3.4 Security Zones

The project found an additional and important security related issue, being the professionals understanding and application of "security zones". The BACS Guideline has to be capable of application across a broad range of different built environments, with exposure to different threats and with varying organizational criticalities. Therefore, the Guideline used security zones in its security questions (BACS Guideline Appendix B). However, the majority of participants had a limited understanding and practice of designing and applying security zones as a defense in depth method.

Security zones are defined by the American Institute of Architects in *Security Planning and Design* (The American Institute of Architects, 2004) as layers of concentric defensive rings, from public to semi-public to private zones. Security is applied to and between these primary layers as lines of defense. In addition, the Australian Government *Physical Security Management Guidelines: Security Zones and Risk Mitigation Control Measures* (Attorney-General's Department, 2011) provide guidance on achieving a consistent approach to determining physical security controls in facilities, using security zones based on risk. Security zones are the division of space based on threat and criticality within a security context.

Security zones have important implications for BACS, as shared tenancy facilities may include low and high-level security requirements based on client risk, achieved through the application of physical security. However, such security, as with other facility services, is integrated on the same

BACS for the entire facility, permeating all security areas. As one participant in the focus group stated, “we establish the highest security level tenant and that sets the level of security for the BACS”. Notwithstanding such an issue, the project found that many participants had no, or a limited understanding of the term “security zone”. Nevertheless, security zones provide a methodology for physical and logical security mitigation, based on organizational criticality, the security threat and risk assessment. Therefore, security professionals need to be better educated, and have a greater awareness and application of security zoning.

11.4 CONCLUSION OF FINDINGS

The project found that BACS security body of knowledge is spread across a vast array documents; however, to date there is no single source document that facility and security professionals can use to understand the significance of this security concern. Much of the knowledge is published across multidisciplinary domains, meaning the core knowledge is not available in a concise and useable format for such professionals. Consequently, the importance in the need to better understand, raise the awareness of, and protect BACS can, in part, be highlighted through the significant interest this project raised at each progressive stage through to its completion. The partnership of three international professional associations with ASIS International, BOMA and SIA, shows the interest that this project generated and its importance.

The project found that there are many, and diverse threats and risks to BACS, through a board range of BACS vulnerabilities. These vulnerabilities are further complicated by the need of professionals to understand reasonable threats, what is critical in their organization and the subsequent risks, all within the environmental context (or situation) of their facility and its operations.

Through an evidence based approach, the project found a lack of awareness and understanding by security and facility professionals in BACS security. However, a positive is their acknowledgement of BACS risks in their risk documentation. Furthermore, that as professionals there is a robust group that can provide deeper technical advice, being Integrators and cybersecurity professionals. With Integrators, there needs to better embedded input into relevant departments, or have true partnerships to be able to strategically apply their expertise for organizational security.

The more significant and useful project outcome, being the BACS Guideline, provides a first generation starting point for all the professions to address the many and changing threats and risks to BACS and its organization. The BACS Guideline will not only provide a tool to inform the many relevant professions, but also start to align language between the many BACS stakeholders.

Finally, the professionals lacked knowledge and practice of security zones. Security zones can provide a systematic methodology to design, apply and maintain protective security strategies across the built environment and its facilities.

References

ABC News (2017, Aug 5). *Donald Trump: Washington formally tells UN of Paris agreement withdrawal*. Retrieved January 4, 2017 from http://www.abc.net.au/news/2017-08-05/trump:-us-formally-tells-un-of-withdrawal-from-paris-agreement/8777420

Advantech. (n.d.). *Building automation system BAS-2000 series*. Advantech.

Anand, M., Ives, Z., & Lee, I. (2005). *Quantifying eavesdropping vulnerability in sensor networks*. Paper presented at the DMSN'05, Trondheim, Norway.

Assante, M. J., & Lee, R. L. (2015). *The Industrial Control System Cyber Kill Chain*. Singapore: SANS Institute.

Attorney-General's Department. (2011). Physical security management guidelines: Security zones and risk mitigation control measures. Canberra: Australian Government.

Auddy, A., & Sahu, M. S. (2008). Tempest: Magnitude of threat and mitigation techniques. In *Proceedings of the 10th International Conference on Electromagnetic Interference and Compatibility* (pp. 603-611). Bangalore: Society of EMC Engineers.

Australian Building Codes Board. (2016). *National Construction Code Volumn One: Building Code of Australia Class 2 to 9 Buildings (Vol. One)*. Canberra: Australian Building Codes Board.

Autor, D., H (2015). Why are there still so many jobs? The history and future of workplace automation. *The Journal of Economic Perspectives*, *29*(3), 3-30.

Barisani, A., & Bianco, D. (2009). *Sniffing keystrokes with laser and voltmeters*. Paper presented at the Paper presented at the Black Hat USA 2009.

Boed, V. (1999). *Networking and integration of facilities automation systems*. Boca Raton, FL: CRC Press.

Brooks, D. (2012). Security threats and risks of Intelligent Building Systems: Protecting facilities from current and emerging vulnerabilities. In C. Laing, A. Badii, & P. Vickers (Eds.), *Security Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection* (pp. 1-16). Hershey, PA: IGI Global.

Brooks, D. J. (2010). What is security: Definition through knowledge categorization. *Security Journal*, *23*(3), 225-239.

BSRIA Institution. (2015). *Threats/Opportunities for Building Automation Systems*. Bracknell: BSRIA Institution.

BSRIA Institution. (2016). *Global building energy management systems market*. Retrieved from https://www.designingbuildings.co.uk/wiki/Global_building_energy_management_systems_market

CBS.MarketWatch. (2000). *Cisco pushes past Microsoft in market value*. Retrieved from http://www.marketwatch.com/story/cisco-pushes-past-microsoft-in-market-value

Chan, W. L., & So, A. T. P. (1999). *Intelligent building systems*. Berlin: Springer.

CIBSE. (2000). *Building control systems: CIBSE Guide H*. Oxford: Butterworth-Heinemann.

Cisco. (2017). *Cisco Smart+Connected Real Estate* [Press release]. Retrieved from http://www.cisco.com/c/dam/en/us/products/collateral/physical-security/network-building-mediator/brochure_c02-424448.pdf

Control Solutions Inc. (2015). *The ultimate guide to building automation*. Retrieved from http://controlyourbuilding.com/blog/entry/the-ultimate-guide-to-building-automation#automation

Coole, M. P., Brooks, D. J. & Minnaar, A. (2017). Educating the Physical Security Professional: Developing a science-based curriculum. *The Security Journal*, pp. 1-24

DDC Online. (n/a). *Introduction to direct digital control systems*. Retrieved from www.ddc-online.org/getting-started.html

Dey, P. (2016). *Honeywell launches new building management system*. Retrieved from http://www.constructionweekonline.com/article-39702-honeywell-launches-new-building-management-system

Diffie, W., & Landau, S. (2009). Communications surveillance: Privacy and security at risk. *Communications of the ACM*, *52*(11), 42–47.

Elwell, C. (2013). *Economic recovery: Sustaining US economic growth in a post-crisis economy*. Retrieved from https://fas.org/sgp/crs/misc/R41332.pdf

EY Ltd. (2015). *How PPPs can help governments close the "gap" amid financial limitations*. Victorian Department of Treasury and Finance (Australia) Retrieved from http://www.ey.com/Publication/vwLUAssets/EY-public-private-partnerships-and-the-global/$FILE/EY-public-private-partnerships-and-the-global.pdf.

Fritsch, J. (2013). *World study: Building automation and control systems (BACS)*. UAE: BSRIA.

Frost & Sullivan. (2008). *Bright green buildings: Convergence of green and intelligent buildings*. Retrieved from https://www.caba.org/CABA/DocumentLibrary/Public/Bright_Green_Buildings.aspx

Garcia, M. L. (2007). *Design and evaluation of physical protection systems*. Burlington, MA: Butterworth-Heinemann.

Grand, J. (2004). Practical secure hardware design for embedded systems. Paper presented at the In *Proceedings of the 2004 Embedded Systems Conference*, San Francisco.

Granzer, W., Praus, F., & Kastner, W. (2009). Security in building automation systems. *IEEE Transactions on Industrial Electronics*, *57*(11), 3622-3630.

Gutmann, P. (2001). Data remanence in semiconductor devices. *Tenth USENIX Security Symposium*. Retrieved from www.usenix.org/publications.library/proceedings/sec01/gutman.html

High Performance HVAC. (2017). *Building automation systems*. Retrieved from http://highperformancehvac.com/building-automation-systems-hvac-control/

Hosain, S. (2016). *Reality check: 50B IoT devices connected by 2020 – beyond the hype and into reality*. Retrieved from http://www.rcrwireless.com/20160628/opinion/reality-check-50b-iot-devices-connected-2020-beyond-hype-reality-tag10

IETF. (2000). *I.E.T.F: Rfc 2804: Ietf policy on wiretapping*. Retrieved from http://tools.ietf.org/html/rfc2804

International Organization for Standardization. (2004). *ISO 16484-2: Building automation and control systems (BACS) part 2 hardware*. Geneva: International Organization for Standardization.

International Organization for Standardization. (2007a). *ISO/IEC 14908-1: Open data communication in building automation, controls and building management - control network protocol part 1 protocol stack*. Geneva: International Organization for Standardization.

Kaparthy, Z. (2016). *BACS market cooling in US dollars as a result of Brexit & US presidential elections*. BSRIA.

Karg, S. (2015). *BACnet stack: An open source BACnet protocol stack for embedded systems*. Retrieved from http://bacnet.sourceforge.net/

Karnouskos, S. (2011). *Stuxnet worm impact on industrial cyber-physical system security*. Paper presented at the IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society.

Kelley, M. (2013, November 20). The Stuxnet attack on Iran's nuclear plant was 'far more dangerous' than previously thought. *Business Insider Australia*. Retrieved from https://www.businessinsider.com.au/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11?r=US&IR=T

King, R. O. N. (2016). Cyber security for intelligent buildings. *Engineering and Technology Reference*, 1-6. doi:10.1049/etr.2015.0115

Kujuro, A. (1990). *Trend of system technology in intelligent buildings in Japan*. Singapore: Asia-Pacific Exhibitions and Conventions Pte Ltd.

Langston, C., & Lauge-Kristensen, R. (2002). *Strategic management of built facilities*. Boston: Butterworth-Heinemann.

Lawson, H. (2014). *Global BEMS market set to approach $7 billion by 2020*. Retrieved from https://blogs.bsria.co.uk/2014/12/08/global-bems-market-set-to-approach-7-billion-by-2020/

Lonix Building Connectivity. (n.d.). *System overview*. Retrieved from www.lonix.com/training/Lecture_Systems_Overview.pdf

LonMark International. (2017). *LonWorks control-networking technology as an ISO/IEC series of standards*. Retrieved from http://www.lonmark.org/technical_resources/standards

LonWorks Americas. (n.d.). *Lonworks technology 101: A lonworks platform overview.* Retrieved from http://www.stitcs.com/en/LonWorks/LonWorks\%20Technology\%20101.pdf

Lowry, G. (2002). Modelling user acceptance of building management systems. *Automation in Construction*, *11*(6), 695-705.

Marketsandmarkets. (2016). *Smart building market: Global forecast to 2021* [Press release]. Retrieved from http://www.marketsandmarkets.com/PressReleases/smart-building.asp

Marketsandmarkets. (2017). *Building automation system market by communication technology (wired, and wireless), offering (facilities management systems, security & access control systems, and fire protection systems), application, and region - global forecast to 2022*

(SE2966). Retrieved from http://www.marketsandmarkets.com/Market-Reports/building-automation-control-systems-market-408.html

Martin, R., & Talon, C. (2015). *Next-generation building energy management systems*. Retrieved from Boulder, Boulder, CO: Navigant Consulting Co.

McGowan, J. J. (1995). *Direct digital control: A guide to distributed building automation*. Lilburn, GA: Fairmont Press.

Morgan, J. (2014). *A simple explanation of 'the internet of things'*. Retrieved from https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#1f8c6a41d091

Nardone, M. S. (1999). *Direct digital control systems: Application commissioning.* Norwell, MA: Springer Press.

Network World. (2003). *The 10 most powerful companies in networking*. Retrieved from http://www.networkworld.com/article/2329300/wireless/the-10-most-powerful-companies-in-networking.html?page=2

OSAC. (2017). *Devastating cyberattack program returns to Saudi Arabia*. Diplomatic Security Services, United States Department of State,

Panke, R. A. (2001). *Energy management systems and direct digital control*. Lilburn, GA: Fairmont Press.

Parasuraman, R., & Riley, V. (1997). Humans and automation: Use, misuse, disuse, abuse. Human Factors: *The Journal of the Human Factors and Ergonomics Society*, *39*(2), 230-253.

Persistence Market Research. (2016). *Global market study on building automation systems: Security and surveillance system segment projected to increase 2.6x between 2016 and 2026*. Retrieved from http://www.persistencemarketresearch.com/market-research/building-automation-systems-market.asp

Pieri, A. (2016). *Honeywell launches business unit to tackle IoT*. Retrieved from http://www.constructionweekonline.com/article-38783-honeywell-launches-business-unit-to-tackle-iot/

Sall, I. (2017). *Does IoT mean the death of the BMS?* Retrieved from http://www.facilitiesshow.com/does-iot-signal-death-bms

Schneider Electric. (2015). *Guide to open protocols in building automation*. Andover, MA: Schneider Electric.

Schneider Electric TAC. (2004). *Product catalogue*. Schneider Electric.

Shang, W., Ding, Q., Marianantoni, A., Burke, J., & Zhang, L. (2014). Securing building management systems using named data networking. *IEEE Network*, *28*(3), 50-56.

Sharples, S., Callaghan, V., & Clarke, G. (1999). A multi-agent architecture for intelligent building sensing and control. *Sensor Review*, *19*(2), 135-140.

Shaw, W. (2006). *Cybersecurity for SCADA systems*. Tulas, OK: PennWell Corporation.

Sherbini, K., & Krawczyk, R. (2004). *Overview of intelligent architecture*. Paper presented at the 1st ASCAAD International Conference on E-Design in Architecture, Dhahran.

Siemens. (2017). *Communication: Desigo – standardized communication protocols for more economy*. Retrieved from http://www.buildingtechnologies.siemens.com/bt/global/en/buildingautomation-hvac/building-automation/building-automation-and-control-system-europe-desigo/system/communication/Pages/communication.aspx

Simpson, J. A., & Weiner, E. S. C. (Eds.). (1989). *The Oxford English Dictionary* (2nd ed.). Oxford: Oxford University Press.

Sinopoli, J. (2012). *Security issues with integrated smart buildings*. Retrieved from http://www.automatedbuildings.com/news/dec12/articles/sinopoli/121119103101sinopoli.html

Smart Accelerate. (n.d). *Intelligent building assessment methodology*. Retrieved from http://www.ibuilding.gr/definitions.html

Smart Grid Interoperability Panel. (2010). *Guidelines for smart grid cyber security: Vol. 1, Smart grid cyber security strategy, architecture and high-level requirements*. Retrieved from https://www.smartgrid.gov/document/nistr_7628_guidelines_smart_grid_cyber_security_vol_1_smart_grid_cyber_security_strategy_ar

So, A. T. P., & Wong, K. C. (2002). On the quantitative assessment of intelligent buildings. *Facilities*, *20*(7/8), 288-295.

Takagi, H. (1991). Application of polling models to computer networks. *Computer Networks and ISDN Systems*, *22*(3), 193-211.

Talon, C., & Gartner, J. (2016). *Assessment of strategy and execution for 15 intelligent building software solutions providers*. Retrieved from http://www.navigantresearch.com/research/navigant-research-leaderboard-report-building-energy-management-systems

Technavio. (2016). *Global integrated building management systems market 2017-2021*. Retrieved from Toronto: https://www.technavio.com/report/global-automation-global-integrated-building-management-systems-market-2017-2021?utm_source=T5&utm_campaign=Media&utm_medium=BW

The American Institute of Architects. (2004). *Security planning and design: A guide for architects and building design professionals*. Hoboken, NJ: John Wiley & Sons Ltd.

TMR Analysis. (2017). *Commercial building automation market 2016-2024*. Retrieved from New York: http://www.transparencymarketresearch.com/commercial-building-automation.html

Trading Economics. (2017). *European Union GDP annual growth rate*. Retrieved from http://www.tradingeconomics.com/european-union/gdp-annual-growth-rate

TROX GmbH. (n.d.). *Fire protection with LON technology*. Neukirchen-Vluyn: TROX GmbH.

US Department of Energy. (2017). *Database of state incentives for renewables & efficiency*. Retrieved from http://www.dsireusa.org

Van Eck, W., & Laborato, N. (1985). Electromagnetic radiation from video display units: An eavesdropping risk? *Computers and Security*, *4*, 269–286.

Wyman, R. (2017). Consider the consequences: A powerful approach for reducing ICS cyber risk. *Cyber Security: A Peer Reviewed Journal*, *1*(1), 1-17.

Young, J. (2014). *BIoT: Building internet of things*. Retrieved from http://www.automatedbuildings.com/news/mar14/articles/realcomm/140219043909realcomm.html

Appendix A. Vulnerabilities Matrix

Report Section	Evaluation Category	Vulnerability	Vulnerability Explained	Loss of View or Control	Denial of View or Control	Manipulation of View or Control	Threat level
	Automation level		The Automation level devices and network are located throughout the facility, generally in plant rooms and electrical enclosures				high
6.2.1	Device Access (Physical)	Device cover, such as a Controller	Devices have a cover that are designed to protect their internal circuitry, not to protect against external entry			✓	high
		No anti-tamper detection to Device cover	The cover does not contain any form of anti-tamper detection, allowing unauthorized access to the internal circuitry and exploitation			✓	high
		No anti-tamper detection to Device mount	The Device does not contain anti-tamper detection to protect against unauthorized removal			✓	medium
		Manual control of service switches	Most Devices provide maintainers with switches to locally adjust output states, such as on, off or auto	✓	✓	✓	medium
		Covert control of outputs	Output relays may be overridden or held in a state through the use of magnets	✓	✓		low
		Covert control of inputs	Inputs may be overridden or held in a state through removal, bypass or short circuiting the input, which do not use anti-tamper detection			✓	medium
		Damaging the Device, such as a Controller	Destroying or damaging the Device will result in a loss of control and monitoring, leading to denial of service and loss of information		✓		medium
6.2.2	Network Access (Physical)	Network tamper, allowing communication access	Automation level network contains no anti-tamper detection capability, allowing unauthorized network access		✓	✓	high
		Network traffic monitoring and analysis	Access to the network allows traffic monitoring and analysis, leading to an observer building a "picture" of the facility			✓	medium
		Open source and free network programs and code	Automation network operating programs are open source, with free open source programs that can capture, alter and inject commands	✓	✓	✓	high
		Network traffic data injection	Network access allows the use of open source programs to inject false commands back into the traffic			✓	medium
		Device insertions	Physically inserting an rogue device anywhere on the network, allows unauthorized monitor and control			✓	medium
6.2.3	Wiretapping	Wiretap automation network	Covert access to the automation network, to facilitate unauthorized monitoring and control			✓	high
6.2.4	Electromagnetic Emanation	Network information extraction	Covert access to the automation network, to facilitate unauthorized monitoring and control			✓	low
6.2.5	Remote Connect Workstation	Unauthorized access	Gaining automation level network connectivity facilitates the connection of an unauthorized workstation		✓	✓	high
		Traffic monitoring and analysis	An unauthorized workstation allows traffic monitoring and control			✓	medium
6.2.6	Foreign Device Replacement	Insertion of an rogue (unauthorized) device	Physical insertion of a rogue device anywhere on the network, allows unauthorized monitor and control			✓	medium
6.2.7	Internal & External Memory	Extraction of latent memory	A removed device retain program and activity data, that may be extracted			✓	low
6.2.8	Device Programmer	Unauthorized programming at Controller, using a secondary device	Access to a automation level device, like Controller, allows connectivity of a dedicated programming tool	✓		✓	medium
6.2.9	Embedded Functionality	Unknown or unauthorized dormant device capability	Devices , like Controllers, are mass produced with common site-upgradeable hardware that are only activated when required, such as wireless connectivity			✓	medium
6.2.10	Power Supply	Loss of mains power	Devices, such as Controller, require mains power, so loss results in loss of the automation system and its functionality	✓	✓		medium
		No uninterruptable power supply capability	Automation level devices, such as Controllers, are not battery powered due to the plant and equipment they monitor and control. Loss of mains power results in loss of the automation system and its functionality	✓	✓		medium
	Management level		Management level devices are the corporate information and communication (ICT) network and its hardware, such as Workstations, routers and switchers				low
7.3.1	Device Access (Physical)	Device access, such as a Workstation	Unauthorized access to an unprotected Management level Workstation allows access to the automation system and possible corporate applications			✓	medium
		Cyber-attack of devices, such as a Workstation	Attacks using malicious code through insertion of an infected storage device	✓	✓	✓	medium
		Destruction of devices, such as a Workstation	Destroying or damaging the Device will result in a loss of control and monitoring oversight		✓		low
7.3.2	Network Access (Physical)	Monitor and analyze network connections	Access to the ICT network allows traffic monitoring and analysis			✓	low
		Wiretapping of the network	Wiretapping of the ICT network to monitor and analyze the network and its systems			✓	low
		Insertion of illegal or unauthorized device	Physical insertion of a rogue device anywhere on the ICT network, allows unauthorized monitor and control			✓	low
7.3.3	Device Access (Digital)	Cyber-attack of devices, such as a Workstation	Attacks using malicious code through cyber delivery, such as email	✓	✓	✓	medium
7.3.4	Electromagnetic Emanation	Monitor and analyze network connections	Covert access to the ICT network, to facilitate unauthorized monitoring and control			✓	very low
	Field level		Field level devices are control actuators and monitoring sensors, spread throughout the facility				low
7.4.1	Device Access (Physical)	Manipulation of Sensor & Actuator input/outputs	Manipulation of a Sensor or Actuator to alter outputs or input, resulting in the physical environment (for example, room temperature) not matching what the automation system measures	✓	✓	✓	low
		Physical disconnection	Disconnecting the Device will result in a loss of control and monitoring, leading to denial of service and loss of information	✓	✓		low
		Destruction of device	Destroying or damaging the Device will result in a loss of opertaor control and monitoring, leading to denial of service and loss of information		✓		low
		Security sensors (detectors) tamper detection	Connected Security Sensors do not have anti-tamper functionality, allowing access to manipulate or disconnect without detection at the Automation or Management level	✓	✓		high
7.4.2	Connectivity Access (Physical)	Loss of function	Disconnection, manipulation or destruction of devices, such as sensor or actuator, results in loss of monitor or control function		✓		low
		Monitoring of the connection	The connection cable between the field device and automation level allows monitoring of field device input or output			✓	low
		Control (remote) of devices via connection	Access to the connection cable between the field device and automation level allows control of the field device input or output		✓	✓	low
		Spoofing device outputs	The field device output or input may be bypassed to spoof the automation level control and monitoring	✓	✓		low
		Security sensors (detectors) tamper detection	The Security Sensor connection cable does not have anti-tamper line circuitry, allowing manipulation or disconnection without detection at the Automation or Management level	✓	✓		high
7.4.3	Electromagnetic Emanation	Monitor and analyze network connections	Covert access to the sensor or actuator connection will allow unauthorized monitoring of the device's state			✓	very low

Appendix B. International Standards

B.1 INTRODUCTION

A review of relevant international and national standards relating to Building Automation and Control Systems (BACS) is presented.

B.2 BUILDING AUTOMATION STANDARDS

International standards, pertinent to BACS, are listed in Table B.1.

Table B.1

International Relevant Standards

Code	Title
ISO 16484 Parts 1 to 6	Building automation and control systems (BACS)
ISO/IEC DIS 14908 Parts 1 to 6	Open Data Communication in Building Automation, Controls and Building Management - Control Network Protocol
EN 50090	Home and Building Electronic Systems (HBES) (To be replaced by EN 50491)
EN 50491	General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS)
BS EN 16947-12	Building Management System. Part 1. Module M10-12
BS EN 63044-1	General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS). Part 1. General requirements
ASHRAE 135-2016: Standard 135-2016	BACnet-A Data Communication Protocol for Building Automation and Control Networks
BS EN 62361-2:2013	Power systems management and associated information exchange. Interoperability in the long term. End to end quality codes for supervisory control and data acquisition (SCADA)
DD CEN/TS 15231:2006	Open data communication in building automation, controls and building management. Mapping between Lonworks and BACnet
ISO 10303.225-2004	Industrial automation systems and integration - Product data representation and exchange Application protocol: Building elements using explicit shape representation
TIA/EIA 862:2016 (also ANSI/TIA-862-B)	Structured Cabling Infrastructure Standard For Intelligent Building System

B.3 SYNTHESIS OF BUILDING AUTOMATION STANDARDS

A synthesis of the most pertinent international standards for BACS is provided.

International Organization for Standardization

The International Organization for Standardization (ISO) is considered the world's largest developer and publisher of International Standards, with its Central Secretariat located in Geneva, Switzerland. ISO has a membership of 162 national standards bodies (International Organization for Standardization, n.d.), with each country having one member.

ISO is a non-governmental organization that forms a link between the public and private sectors. Many of its member institutes are part of the governmental structure in their countries, or are mandated by their government. Other members are in the private sector, having been set up by national partnerships of industry associations. Therefore, ISO enables a consensus to be reached on solutions that meet both the requirements of business and the broader needs of society (International Organization for Standardization, n.d.).

ISO 16484: Building Automation and Control Systems (BACS)

ISO 16484 suite of standards specifies the phases required for Building Automation and Control Systems (BACS) projects and requirements for the hardware to perform the tasks within a BACS. It also specifies the requirements for the overall functionality and engineering services to achieve building automation and control systems. Besides, defines data communication services and protocols for computer equipment used for monitoring and control of heating, ventilation, air-conditioning and refrigeration (HVAC) and other building systems, and the method for verifying that an implementation of the BACnet protocol provides each capability claimed in its Protocol Implementation Conformance Statement (PICS) in conformance with the BACnet standard. This standard contains several Communication Profile Families (CPF), which specify one or more communication profiles. The international norm ISO 16484 is regarding Building automation and control systems (BACS).

The standard consists of five documents, excluding a Part 4 that is under preparation:

> ISO 16484 Part 1 Building Automation and Control Systems (BACS). Project specification and implementation
>
> ISO 16484 Part 2 Building Automation and Control Systems (BACS). Hardware
>
> ISO 16484 Part 3 Building Automation and Control Systems (BACS). Functions
>
> ISO 16484 Part 4 Building Automation and Control Systems (BACS). Applications (under preparation)
>
> ISO 16484 Part 5 Building Automation and Control Systems (BACS). Data communication protocol
>
> ISO 16484 Part 6 Building Automation and Control Systems (BACS). Data communication conformance testing

ISO 16484-1:2010 specifies guiding principles for project design and implementation and for the integration of other systems into the Building Automation and Control Systems (BACS). It specifies the phases required for the BACS project, including design (determination of project requirements and production of design documents including technical specifications), engineering (detailed function and hardware design), installation (installing and commissioning of the BACS), and completion (handover, acceptance and project finalization). This Part 1 also specifies the requirements for as-built documentation and training. ISO 16484-1:2010 is not applicable to operation and maintenance, nor is it applicable to retro or continuous commissioning, including a commissioning authority.

ISO 16484-2:2004 specifies the requirements for the hardware to perform the tasks within a building automation and control system (BACS). It provides the terms, definitions and abbreviations for the understanding of ISO 16484-2 and ISO 16484-3. ISO 16484-2:2004 relates only to physical items/devices, i.e. devices for management functions, operator stations and other human system interface devices; controllers, automation stations and application specific controllers; field devices and their interfaces; cabling and interconnection of devices; engineering and commissioning tools.

ISO 16484-3:2005 specifies the requirements for the overall functionality and engineering services to achieve building automation and control systems. It defines terms, which shall be used for specifications and it gives guidelines for the functional documentation of project/application specific systems. It provides a sample template for documentation of plant/application specific functions, called BACS points list.

ISO 16484-5:2007 defines data communication services and protocols for computer equipment used for monitoring and control of heating, ventilation, air-conditioning and refrigeration (HVAC&R) and other building systems. It defines, in addition, an abstract, object-oriented representation of information communicated between such equipment, thereby facilitating the application and use of digital control technology in buildings.

ISO 16484-6:2009 defines a standard method for verifying that an implementation of the BACnet protocol provides each capability claimed in its Protocol Implementation Conformance Statement (PICS) in conformance with the BACnet standard.

Keywords: building, home, automation, hardware, project, protocol

---

ISO/IEC DIS 14908-1 to 6: Open Data Communication in Building Automation, Controls and Building Management - Control Network Protocol

ISO/IEC 14908 standard consists of six parts:

ISO/IEC 14908-1: Information technology -- Control network protocol -- Part 1: Protocol stack

ISO/IEC 14908-2: Information technology -- Control network protocol -- Part 2: Twisted pair communication

ISO/IEC 14908-3: Information technology -- Control network protocol -- Part 3: Power line channel specification

ISO/IEC 14908-4: Information technology -- Control network protocol -- Part 4: IP communication

BS EN 14908-5 Open Data Communication in Building Automation, Controls and Building Management Implementation Guideline - Control Network Protocol Part 5: Implementation

BS EN 14908-6 Open Data Communication in Building Automation, Controls and Building Management - Control Network Protocol Part 6: Application elements

ISO/IEC 14908 adopts the LonTalk protocol, optimized for control. Originally developed by Echelon Corporation for networking devices over media such as twisted pair, power-lines, fiber optics and Radio Frequency (RF). It is popular for the automation of various functions in industrial control, home automation, transportation, and buildings systems. The protocol has been adopted as a family of standards by CEN (EN 14908), as well as by ISO/IEC (ISO/IEC 14908). This standard specifies a multi-purpose control network protocol stack optimized for smart grid, smart building, and smart city applications.

Keywords: ICT, buildings, automation, field buses, devices, sensors

---

EN 50090: Home and Building Electronic Systems (HBES)

European Standard EN 50090 concentrates on control applications for Home and Building HBES Open Communication System and covers any combination of electronic devices linked via a digital transmission network. Home and Building Electronic System, as provided by the HBES Open Communication System, is a specialized form of automated, decentralized and distributed process control, dedicated to the needs of home and building applications.

EN 50090 consists of 14 parts:

EN 50090-2-1:1994: System overview-Architecture

EN 50090-2-2:1996: System overview-General technical requirements

EN 50090-2-3:2005: System overview–General functional safety requirements for products intended to be integrated in HBES

EN 50090-3-1:1994: Aspects of application-Introduction to the application structure

EN 50090-3-2:1995: Aspects of application-User process

EN 50090-3-2:2004: Aspects of application-User process for HBES Class 1

EN 50090-4-1:2004: Media independent layers-Application layer for HBES Class 1

EN 50090-4-2:2004: Media independent layers–Transport layer, network layer and general parts of datalink layer for HBES Class 1

EN 50090-4-3:2015: Home and Building Electronic Systems. (HBES)-Media independent layers-Communication over IP

EN 50090-5-1:2005: Media and media dependent layers-Power line for HBES Class 1

EN 50090-5-2:2004: Media and media dependent layers-Network based on HBES Class1, Twisted Pair

EN 50090-7-1:2004: System management-Management procedures

EN 50090-8:2000: Conformity assessment of products

EN 50090-9-1:2004: Installation requirements–Generic cabling for HBES Class 1 Twisted Pair

The EN 50090 series concentrates on HBES Open Communication System Class 1 and includes a specification for a communication network for Home and Building. For example, control of lighting, heating, food preparation, washing, energy management, water control, fire alarms, blinds control, different forms of security control, etc.

Keywords: home, building, automation, field buses, Building Electronic Systems, HBES

EN 50491: General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS)

EN 50491 standard consists of 11 documents that provide requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS) regarding general requirements, eEnvironmental conditions, electrical safety, general functional safety for products intended to be integrated in Building Electronic Systems (HBES) and Building

Automation and Control Systems (BACS), EMC requirements, HBES installations-and Smart Metering. It contains requirements for HBES devices including environmental performance, safety, functional safety, EMC, and design, planning and installation.

The EN 50491 series is in the process of replacing the existing EN 50090 series of standards covering the areas system overview, aspects of application, media independent layers, media and media dependent layers, interfaces, system management, conformity assessment of products and installation requirements.

EN 50491-1 General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS) - Part 1: General requirements - This European Standard applies to all Home and Building Electronic Systems (HBES) and Building Automation Control Systems (BACS) and specifies the general requirements for these systems and products covering the following functionalities: - HBES class 1: simple control and command; - HBES class 2: simple voice and stable video transmission including class 1; - HBES class 3: video transfers including class 2. This European Standard provides an overview of this series of European Standards. To enable integration of a wide spectrum of applications, EN 50491 series covers: - electrical safety, - functional safety, - environmental conditions, - EMC requirements, - installation and cabling rules and topologies, - Smart Metering – Application specification (under development), - Smartgrid — Application specification — Interface and framework (under development). EN 50491 series is a product family standard.

DIN EN 50491-2 General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS) - Part 2: Environmental conditions

EN 50491-3:2009 provides the electrical safety requirements for all devices connected to HBES/BACS. This European Standard is applicable to – operator stations and other human system interface devices, – devices for management functions, – control devices, automation stations and application specific controllers, – field devices, – cabling and interconnection of devices. This European Standard covers the following requirements and compliance criteria: – protection from hazards in the device; – protection from over-voltages on the network; – protection from touch current; – protection from hazards caused by different type of circuits; – protection of the communication wiring from overheating caused by excessive current.

EN 50491-4-1:2012 sets the requirements for functional safety for HBES/BACS products and systems, a multi-application bus system where the functions are decentralized, distributed and linked through a common communication process. The requirements may also apply to the distributed functions of any equipment connected in a home or building control system if no specific functional safety standard exists for this equipment or system. The functional safety requirements of this European Standard apply together with the relevant product standard for the device if any. This European Standard is part of the EN 50491 series of standards. This European Standard does not provide functional safety requirements for safety-related systems.

EN 50491-5-1:2010 sets the minimum level of EMC performance for HBES/BACS products intended to be connected to an HBES/BACS system. A set of devices connected to perform a standalone application is not considered to be an HBES/BACS system and therefore are outside the scope of this European Standard. This European Standard provides the general performance requirements and test setups for EMC for all products connected to HBES/BACS. This connection can be wired (e.g. communication cable, power line) or wireless (e.g. radiofrequency, infrared). This European Standard is applicable (but not limited) to – operator stations and other human system interface devices, – devices for management functions, – control devices, automation stations and application specific controllers, – field devices and their interfaces, – cabling and interconnection of devices, – dedicated devices for engineering and commissioning tools for HBES/BACS CLC/TR 50491-6-3:2011 establishes the general rules for assessing HBES installations, according to its complexity and energy performance.

Keywords: building, home, automation, systems, BACS, HBES

BS EN 16947-1. Building Management System. Part 1. Module M10-12

Buildings, Energy conservation, Efficiency, Performance, Energy consumption, Automatic control systems, Control systems, Thermal environment systems, Thermal design of buildings, Air-conditioning systems, Space-heating systems, Ventilation, Lighting systems, Heat engineering, Mathematical calculations

---

BS EN 63044-1. General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS). Part 1. General requirements

Domestic, Electronic equipment and components, Domestic electrical installations, Building services, Automatic control systems, Domestic facilities, Electrical household appliances, Open systems interconnection, Physical layer (OSI), Data link layer (OSI), Radiofrequencies, Radiocommunication, Data transmission

---

IEC 63044-3:2017 Home and Building Electronic Systems (Hbes) And Building Automation And Control Systems (Bacs) - Part 3: Electrical Safety Requirements

IEC 63044-3:2017 provides the electrical safety requirements related to the HBES/BACS network in addition to the product safety standards for HBES/BACS devices. It also applies to devices used within an HBES/BACS network for which no specific HBES/BACS product safety standard exists. In addition, it defines safety requirements for the interface of equipment intended to be connected to an HBES/BACS network. It does not apply to interfaces to other networks.

IEC 63044-5-1:2017 Home and Building Electronic Systems (Hbes) And Building Automation And Control Systems (Bacs) - Part 5-1: Emc Requirements, Conditions And Test Set-Up

IEC 63044-5-1:2017 is a product family standard that sets the minimum level of EMC performance for the HBES/BACS network in addition to the product EMC standards for HBES/BACS devices. It also applies to devices used within an HBES/BACS network for which no specific HBES/BACS product EMC standard exists. In addition, it defines EMC requirements for the interface of equipment intended to be connected to an HBES/BACS network. It does not apply to interfaces to other networks.

IEC 63044-5-2:2017 Home and Building Electronic Systems (Hbes) and Building Automation And Control Systems (Bacs) - Part 5-2: Emc Requirements For Hbes/Bacs Used In Residential, Commercial And Light-Industrial Environments

IEC 63044-5-2:2017 is a product family standard that sets the minimum level of EMC performance for the HBES/BACS network in addition to the product EMC standards for

HBES/BACS devices. It also applies to devices used within an HBES/BACS network for which no specific HBES/BACS product EMC standard exists. In addition, it defines EMC requirements for the interface of equipment intended to be connected to an HBES/BACS network. It does not apply to interfaces to other networks.

IEC 63044-5-3:2017 Home and Building Electronic Systems (Hbes) and Building Automation And Control Systems (Bacs) - Part 5-3: Emc Requirements For Hbes/Bacs Used In Industrial Environments

IEC 63044-5-3:2017 is a product family standard that sets the minimum level of EMC performance for the HBES/BACS network in addition to the product EMC standards for HBES/BACS devices. It also applies to devices used within an HBES/BACS network for which no specific HBES/BACS product EMC standard exists. In addition, it defines EMC requirements for the interface of equipment intended to be connected to an HBES/BACS network. It does not apply to interfaces to other networks.

ASHRAE 135-2016: Standard 135-2016 BACnet-A Data Communication Protocol for Building Automation and Control Networks

Standard 135 defines data communication services and protocols for computer equipment used for monitoring and control of HVAC and other building systems, and to define, for application interoperability, an abstract, object-oriented representation of information communicated between such equipment, thereby facilitating the application and use of digital control technology in buildings.

The 2016 publication of the standard was motivated by the large number of additions and enhancements added to the 2012 version, including support for IPv6 networks. Both the extended data model and the new RESTful Web services, added by Addendum am to Standard 135-2012, are major steps in advancing BACnet for the future information technology landscape. This edition of the standard also includes the recently adopted changes for the lighting and the elevator industry.

BACnet, the ASHRAE building automation and control networking protocol, has been designed specifically to meet the communication needs of building automation and control systems for applications such as heating, ventilating, and air-conditioning control; fire and other life safety and security systems; energy management; lighting control; physical access control; and elevator monitoring systems.

The BACnet protocol provides mechanisms by which computerized equipment of arbitrary function may exchange information, regardless of the particular building service it performs. As a result, the BACnet protocol may be used by mobile and cloud-hosted devices, head-end computers, general-purpose direct digital controllers, and application-specific or unitary controllers with equal effect.

This protocol provides a comprehensive set of messages for conveying encoded building automation data between devices including, but not limited to hardware binary input and output values, hardware analog input and output values, software data values, schedule information, alarm and event information, trend and event logs, files, control logic, application specific data for a large range of building services, and network configuration including security.

Keywords: BACnet, building automation, building control network, building automation network

BS EN 62361-2:2013: Power Systems Management and Associated Information Exchange. Interoperability in the Long Term. End To End Quality Codes for Supervisory Control and Data Acquisition (SCADA)

Electric power systems, Information exchange, Data security, Data transmission, Telecommunication, Communication networks, Computer networks, Data management, Data integrity, Communication technology

DD CEN/TS 15231:2006: Open Data Communication in Building Automation, Controls and Building Management. Mapping Between Lonworks and BACnet

Data processing, Data transmission, Communication procedures, Computer networks, Communication networks, Data transmission methods, Computer applications, Buildings, Controllers, Control equipment, Information exchange, Open systems interconnection, Lighting systems, Thermal environment systems, Energy conservation, Security systems in buildings, Building services, Application layer (OSI)

ISO 10303.225-2004: Industrial Automation Systems and Integration - Product Data Representation and Exchange Application Protocol: Building Elements Using Explicit Shape Representation

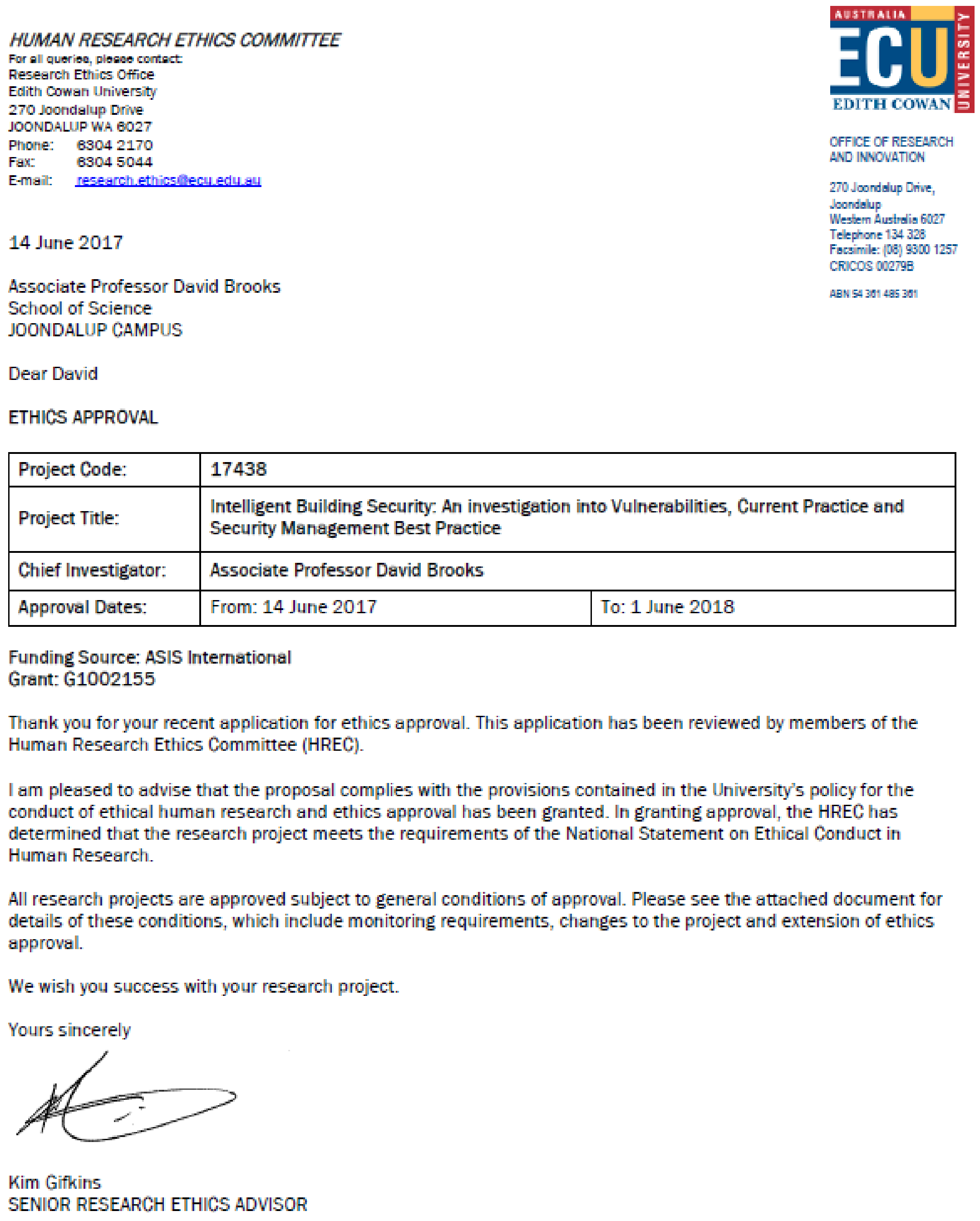
ISO 10303-225 specifies a representation of product information, along with the necessary mechanisms and definitions to enable product data to be exchanged between different computer systems and environments associated with the complete product lifecycle, including product design, manufacture, use, maintenance, and final disposition of the product.

Certain documents referenced in the publication may have been amended since the original date of publication. Users are advised to ensure that they are using the latest versions of such documents as appropriate, unless advised otherwise in this Reconfirmation Notice.

TIA/EIA 862:2016 (also ANSI/TIA-862-B): Structured Cabling Infrastructure Standard for Intelligent Building System

ANSI/TIA-862-B “Structured Cabling Infrastructure Standard for Intelligent Building Systems” was developed by the TIA TR-42.1 Commercial Building Cabling Subcommittee and published in February, 2016. Expanding on the content of ANSI/TIA-862-A, TIA-862-B specifies minimum requirements for intelligent building (previously called building automation system or BAS) cabling to support applications that use Internet Protocol (IP) communication, as well as accommodate other protocols that are typically used between devices. Specific content addresses recommended cabling topology, architecture, design and installation practices, test procedures, and components.

Appendix C. Edith Cowan University Ethics Approval



HUMAN RESEARCH ETHICS COMMITTEE
For all queries, please contact:
Research Ethics Office
Edith Cowan University
270 Joondalup Drive
JOONDALUP WA 6027
Phone: 6304 2170
Fax: 6304 5044
E-mail: research.ethics@ecu.edu.au

OFFICE OF RESEARCH
AND INNOVATION

270 Joondalup Drive,
Joondalup
Western Australia 6027
Telephone 134 328
Facsimile: (08) 9300 1257
CRICOS 00279B

ABN 54 361 485 361

14 June 2017

Associate Professor David Brooks
School of Science
JOONDALUP CAMPUS

Dear David

ETHICS APPROVAL

Project Code:	17438	
Project Title:	Intelligent Building Security: An investigation into Vulnerabilities, Current Practice and Security Management Best Practice	
Chief Investigator:	Associate Professor David Brooks	
Approval Dates:	From: 14 June 2017	To: 1 June 2018

Funding Source: ASIS International
Grant: G1002155

Thank you for your recent application for ethics approval. This application has been reviewed by members of the Human Research Ethics Committee (HREC).

I am pleased to advise that the proposal complies with the provisions contained in the University's policy for the conduct of ethical human research and ethics approval has been granted. In granting approval, the HREC has determined that the research project meets the requirements of the National Statement on Ethical Conduct in Human Research.

All research projects are approved subject to general conditions of approval. Please see the attached document for details of these conditions, which include monitoring requirements, changes to the project and extension of ethics approval.

We wish you success with your research project.

Yours sincerely

Kim Gifkins
SENIOR RESEARCH ETHICS ADVISOR

Conditions of approval

1. Monitoring of Approved Research Projects

Monitoring is the process of verifying that the conduct of research conforms to the approved ethics application. Compliance with monitoring requirements is a condition of approval.

The *National Statement on Ethical Conduct in Human Research* indicates that institutions are responsible for ensuring that research is reliably monitored. Monitoring of approved projects is to establish that a research project is being, or has been, conducted in the manner approved by the Ethics Committee. Researchers also have a significant responsibility in monitoring, as they are in the best position to observe any adverse events or unexpected outcomes. They should report such events or outcomes promptly to the Ethics Committee and take prompt steps to deal with any unexpected risks.

All projects approved by an ECU Ethics Committee are approved subject to the following conditions of approval:

- If the research project is discontinued before the expected date of completion, researchers should inform the Ethics Committee as soon as possible, giving reasons.

- An annual report (for projects that are longer than one year) and a final report at the completion of the research will be provided to the Ethics Committee. You will also be notified when a report is due. The ethics report form can be found on the ethics website http://intranet.ecu.edu.au/research/research-ethics/human-ethics-applications/managing-your-ethics-approval

- Researchers must also immediately report anything that might warrant review of the ethical approval of the protocol, including:
  Any serious or unexpected adverse effects on participants
  Any unforeseen events that might affect continued ethical acceptability of the project.

The Ethics Committee retains the right to require a more detailed and/or more frequent report if the research is deemed to be of high risk, and to recommend and/or adopt any additional appropriate mechanism for monitoring including random inspections of research sites, data and signed consent forms, and/or interview, with their prior consent, of research participants.

2. Changes and amendments

Compliance with the approved research protocol is a condition of approval, and any changes to the research design must be reported to the Ethics Committee. Amendments to the research design that may affect participants and/or that may have ethical implications must be reviewed and approved by the Ethics Committee before commencement.

Any changes to documents and other material used in recruiting potential research participants, including advertisements, letters of invitation, information sheets and consent forms, should be approved by the Ethics Committee.

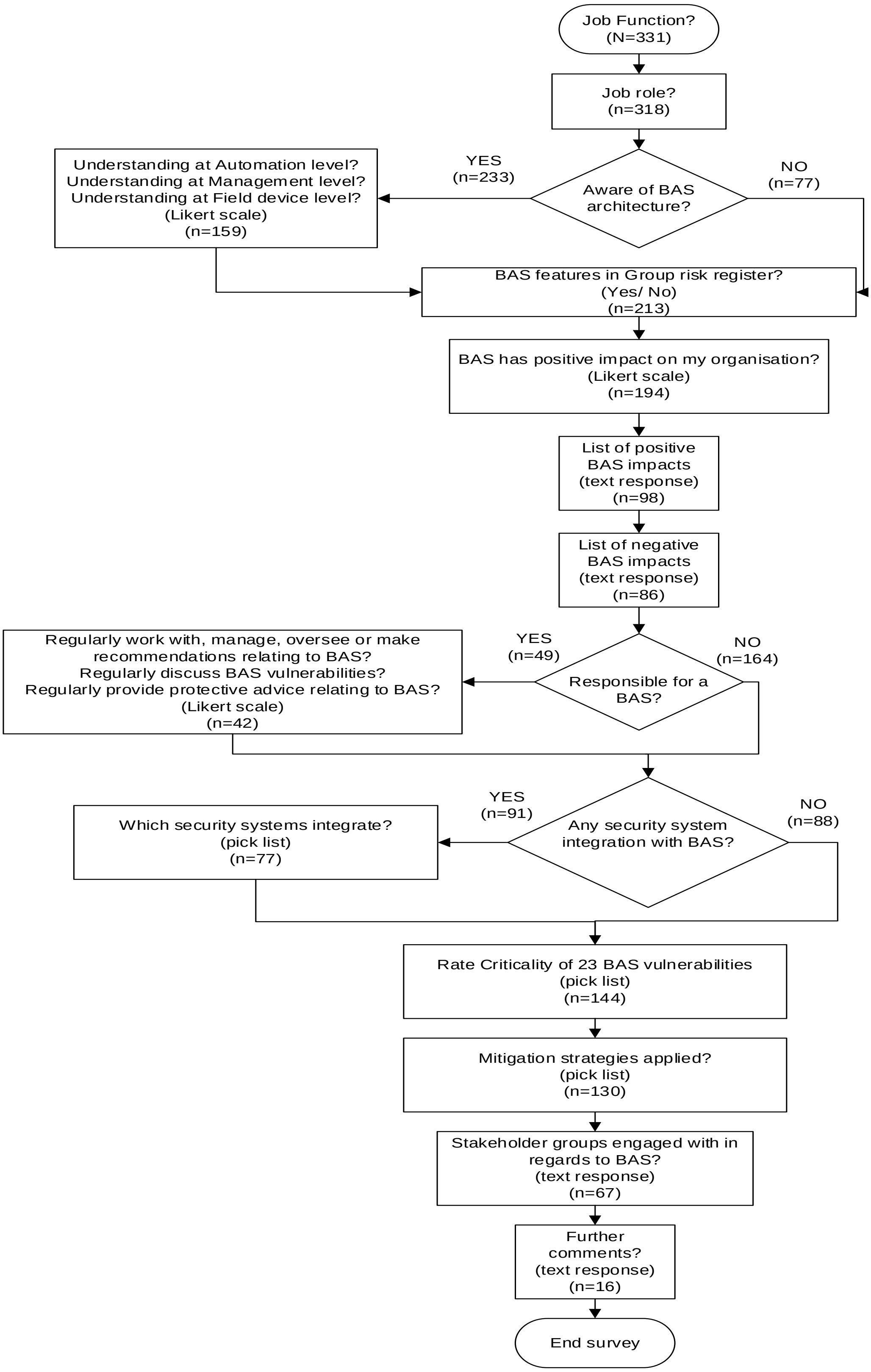
In order to request approval for a change, please send an email to the Ethics Office outlining why the change is needed, describing the change (e.g. the new participants or new research procedures), and attach a copy of any amended documents.

3. Extension of ethics approval

All research projects are approved for a specified period of time – from the date of approval until the date of completion provided in the ethics application. If an extension of the approval period is required, a request must be submitted to the Ethics Committee. Please ensure that requests for extension of approval are submitted before the original approval expires.

In order to request an extension of ethics approval, please send an email to the Ethics Office providing a brief reason why the extension is needed and giving the new expected date of completion.

Appendix D. Stage 2 Online Survey Logic



Job Function?
(N=331)
Job role?
(n=318)
Aware of BAS architecture?
YES
(n=233)
NO
(n=77)
Understanding at Automation level?
Understanding at Management level?
Understanding at Field device level?
(Likert scale)
(n=159)
BAS features in Group risk register?
(Yes/ No)
(n=213)
BAS has positive impact on my organisation?
(Likert scale)
(n=194)
List of positive BAS impacts
(text response)
(n=98)
List of negative BAS impacts
(text response)
(n=86)
Responsible for a BAS?
YES
(n=49)
NO
(n=164)
Regularly work with, manage, oversee or make recommendations relating to BAS?
Regularly discuss BAS vulnerabilities?
Regularly provide protective advice relating to BAS?
(Likert scale)
(n=42)
Any security system integration with BAS?
YES
(n=91)
NO
(n=88)
Which security systems integrate?
(pick list)
(n=77)
Rate Criticality of 23 BAS vulnerabilities
(pick list)
(n=144)
Mitigation strategies applied?
(pick list)
(n=130)
Stakeholder groups engaged with in regards to BAS?
(text response)
(n=67)
Further comments?
(text response)
(n=16)
End survey

Appendix E. Stage 2 BACS Online Survey

Q1 Which of the following best describes your job function?

○ Security (1)

○ Building Owner / Operator (2)

○ Consultant (3)

○ Other (4)

Display Question 2.1:

If Which of the following best describes your job function? Security Is Selected (Q1 = 1)

Q2.1 Which of the following best describes your job role?

○ Physical

○ Installer

○ Integrator

○ Guard force

○ Emergency responder

○ Crisis planning

○ Cyber security

○ ICT

○ Risk analyst

○ Distributor

○ Educator

○ Investigator

○ Other ____

Display Question2.2:

If Which of the following best describes your job function? Building Owner Operator Is Selected

(Q1 = 2)

Q2.2 Which of the following best describes your job role?

○ Building/Property management/administration

○ Strata management/administration

○ Asset management/administration

○ Facility management/administration

○ Real Estate management/administration

○ Plant maintenance

○ Support services

○ Financial management/administration

○ Architect

○ Engineer

○ ICT

○ Educator

○ Other ____

Display Question 2.3:

If Which of the following best describes your job function? Consultant Is Selected (Q1 = 3)

Q2.3 Which of the following best describes your job role?

○ Security design

○ Technology design

○ Building design

○ Risk services

○ Architect

○ Emergency planner

○ Cyber security

○ ITC

○ Financial services

○ Engineer

○ Architect

○ Educator

○ Other ____

Display Question 2.4:

If Which of the following best describes your job function? Other Is Selected (Q1 = 4)

Q2.4 Which of the following best describes your job role?

○ ICT

○ Cyber security

○ Business continuity

○ Educator

○ Retail

○ Engineer

○ Architect

○ Risk analyst

○ Crisis planning

○ Human resources

○ Financial services

○ Distributor

○ Other ____

Q3 I am aware of the different levels of building automation systems architecture.

○ Yes (1)

○ No (2)

Display Question 3.1:

If I am aware of the different levels of building automation systems architecture. Yes Is Selected (Q3 = 1)

Q3.1 My understanding of building automation system vulnerabilities at the...

	Very High	Somewhat High	Neither High nor Low	Somewhat Low	Very Low
automation level is	○	○	○	○	○
management level is	○	○	○	○	○
field device level is	○	○	○	○	○

Q4 Building automation systems vulnerabilities feature in my group risk register.

○ Yes

○ No

Q5 The building automation system has a positive impact on my organization.

○ Strongly disagree

○ Somewhat disagree

○ Neither agree nor disagree

○ Somewhat agree

○ Strongly agree

○ Don't Know

Q6.1 Please list positive business impacts that a building automation system has in your organization.

[Text Response]

Q6.2 Please list negative business impacts that a building automation system has in your organization.

[Text Response]

Q7 I am responsible for the building automation system.

○ Yes (1)

○ No (2)

Display Question 7.1.1:

If I am responsible for the building automation system. Yes Is Selected (Q7 = 1)

Q7.1.1 I regularly work with, manage, oversee or make recommendations relating to a building automation system.

○ Strongly agree (1)

○ Somewhat agree (2)

○ Neither agree nor disagree (3)

○ Somewhat disagree (4)

○ Strongly disagree (5)

Display Question 7.1.2:

If I am responsible for the building automation system. Yes Is Selected (Q7 = 1)

Q7.1.2 I regularly discuss potential vulnerabilities within my building automation system with other managers.

○ Strongly agree (1)

○ Somewhat agree (2)

○ Neither agree nor disagree (3)

○ Somewhat disagree (4)

○ Somewhat disagree (5)

Display Question 7.1.3:

If I am responsible for the building automation system. Yes Is Selected (Q7 = 1)

Q7.1.3 I regularly provide protective advice in regards to building automation system vulnerabilities.

○ Strongly agree (1)

○ Somewhat agree (2)

○ Neither agree nor disagree (3)

○ Somewhat disagree (4)

○ Somewhat disagree (5)

Q8 Do any of your security systems integrate with a building automation system?

○ Yes (1)

○ Don't know (2)

○ No (3)

Display Question 9:

If Do any of your security systems integrate with a building automation system? Yes Is Selected (Q8 = 1)

Q9 Which following security systems integrate into the building automation system?

□ Intruder alarm

□ CCTV

□ Electronic Access control

□ Duress

□ Intercom

□ Radios

□ Security lighting

□ Incident reporting

□ Other ____

Q10 Building automation systems have threats that pose a risk to the Confidentiality, Integrity and Availability of their data and other business elements.

Please rate the significance of the following building automation system vulnerabilities.

	Very sig (1)	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	No sig (7)	Don't know (8)
Physical access to a controller (1)	○	○	○	○	○	○	○	○
No tamper detection on Controllers (2)	○	○	○	○	○	○	○	○
Manual override of Controllers output switches (3)	○	○	○	○	○	○	○	○
Overriding a Controller outputs or inputs (4)	○	○	○	○	○	○	○	○
Damaging a Controller (5)	○	○	○	○	○	○	○	○
Tampering with the Automation network (6)	○	○	○	○	○	○	○	○
Automation network traffic monitoring (7)	○	○	○	○	○	○	○	○
Automation network traffic data injection (8)	○	○	○	○	○	○	○	○
Insertion of an unauthorized Controller (9)	○	○	○	○	○	○	○	○
Automation level open source network programs (10)	○	○	○	○	○	○	○	○
Extraction of a Controller's latent memory (11)	○	○	○	○	○	○	○	○
Unauthorized programming of a Controller (12)	○	○	○	○	○	○	○	○
Loss of mains power (13)	○	○	○	○	○	○	○	○
Unauthorized access to Workstation (14)	○	○	○	○	○	○	○	○

Cyber-attack on the Management level device (15)	○	○	○	○	○	○	○	○
Damage a Management level device (16)	○	○	○	○	○	○	○	○
Tampering with the ICT network (17)	○	○	○	○	○	○	○	○
Monitoring the ICT network (18)	○	○	○	○	○	○	○	○
Insertion of an unauthorized Management level device (19)	○	○	○	○	○	○	○	○
Manipulation of a Sensor or Actuator (20)	○	○	○	○	○	○	○	○
Physical disconnection of a Sensor or Actuator (21)	○	○	○	○	○	○	○	○
Damaging a Sensor or Actuator (22)	○	○	○	○	○	○	○	○
Manipulation of Security sensor (Detector) (23)	○	○	○	○	○	○	○	○

Q11 What mitigation / control strategies do you apply or recommend when protecting building automation systems?

	Management level	Automation level	Field level	Don't know
Policy	□	□	□	□
Guidelines/Standards	□	□	□	□
Procedures	□	□	□	□
Emergency response	□	□	□	□
Intruder alarm	□	□	□	□
Tamper detection	□	□	□	□
Physical security	□	□	□	□
ITC security	□	□	□	□
Security risk assessment	□	□	□	□
Threat assessment	□	□	□	□
Personnel security	□	□	□	□
Security awareness	□	□	□	□
Electronic access control	□	□	□	□
Maintenance	□	□	□	□
Continuity planning	□	□	□	□
Recovery planning	□	□	□	□
Auditing	□	□	□	□
Other	□	□	□	□

Q12 Please list the stakeholder groups you engage with regarding building automation systems?

[Text Response]

Q13 Do you have any further comments?

[Text Response]

End of Survey

Appendix F. Stage 2 Raw Data Analysis

Table F.1
Distribution and response rates

Body	Distributed	Response*	Rate (%)
ASIS	5379	240	3.06%
SIA	2469		
BOMA	5955	91	1.53%
Overall	13,803	331	2.40%

**Note*: The response and rate have been calculated using the participants' job function. Therefore, the stated figures are not an accurate reflection on membership responses; rather, are indicative.

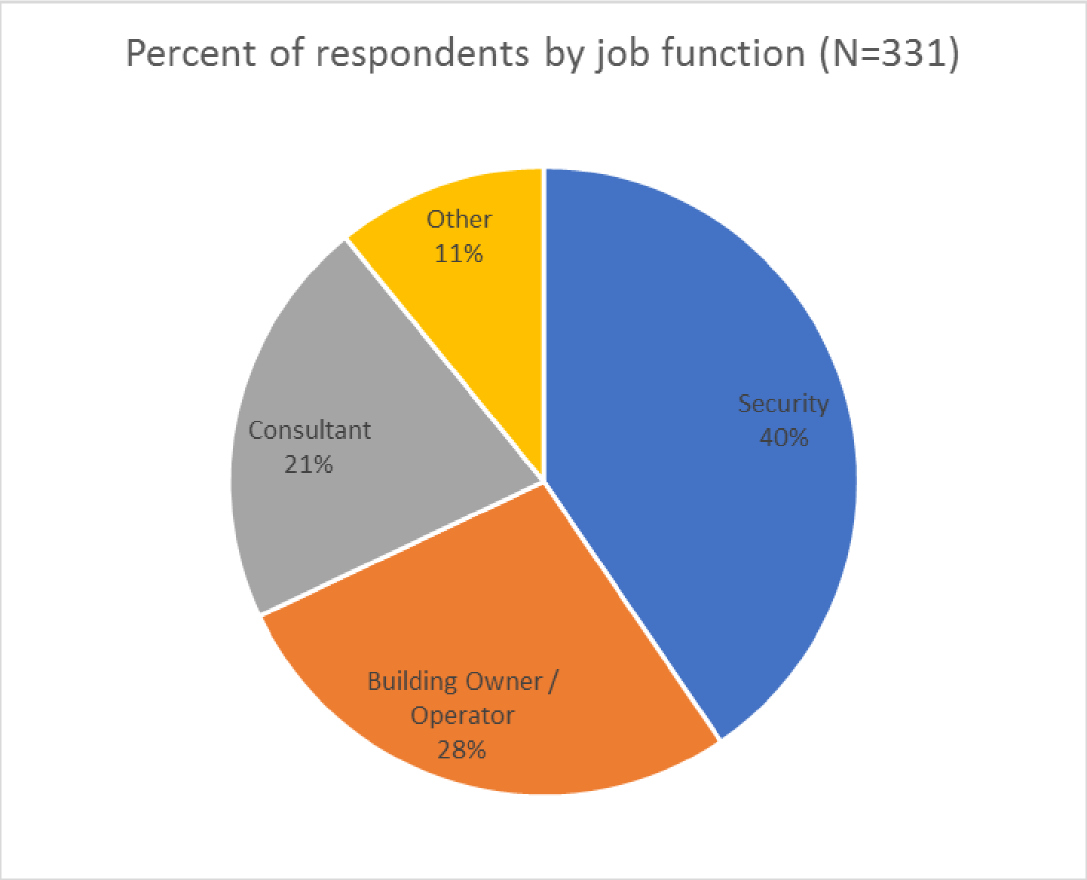


Figure F.1. Percent of respondents by job function

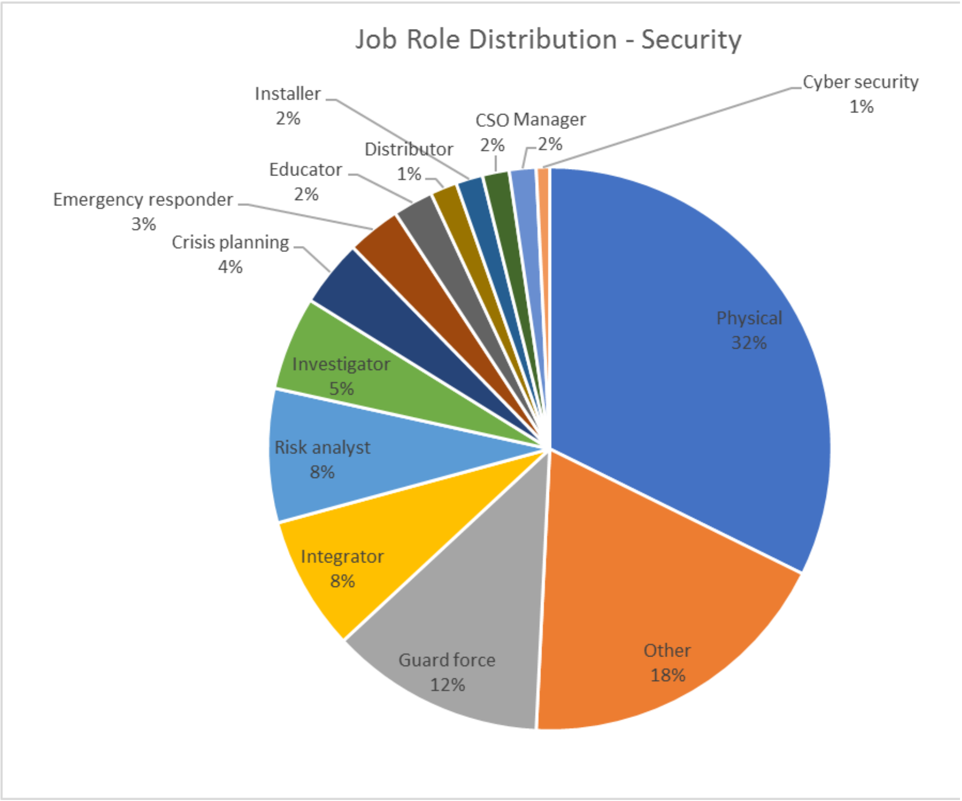


Figure F.2. Job role distribution: Security (n=130)

Table F.2
Other reported Security roles

Other reported roles (Security)
Administrator
Chief of Police
Command Security Manager
Director - Manager
Director of Security
Emergency & Security Manager across domestic and international operations
Head of Corporate Security
Hospital public safety (security) manager
Information Gathering (Secret Agent)
Manufacturer Sales
Regional Asset Protection Manager
Sales (Security Services and Technology)
SECURITY EXECUTIVE
security management
security of 3 domains: people, physical and information

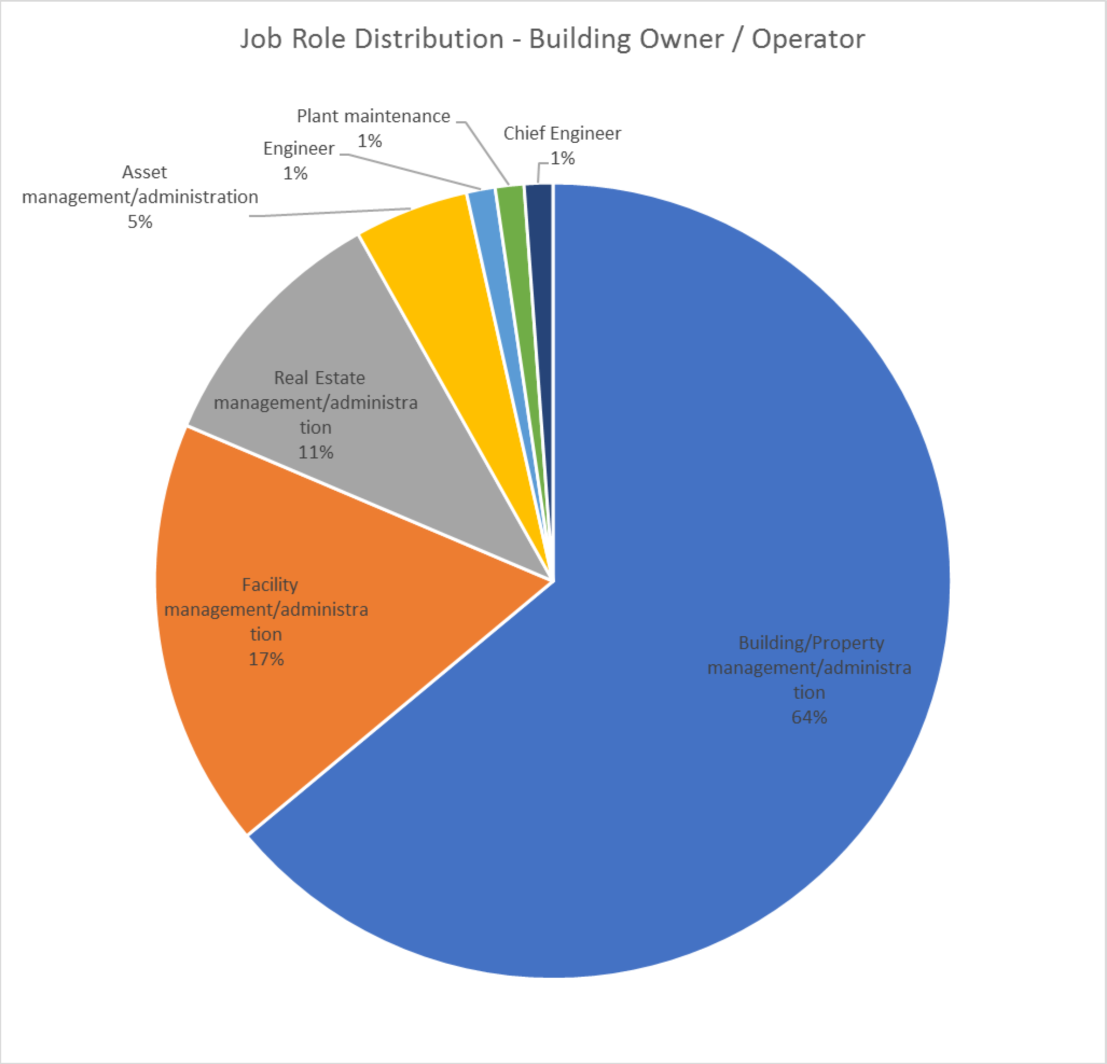


Figure F.3. Job role distribution: Building Owner/Operators (n=86)*

**Note*: No other reported roles as text responses

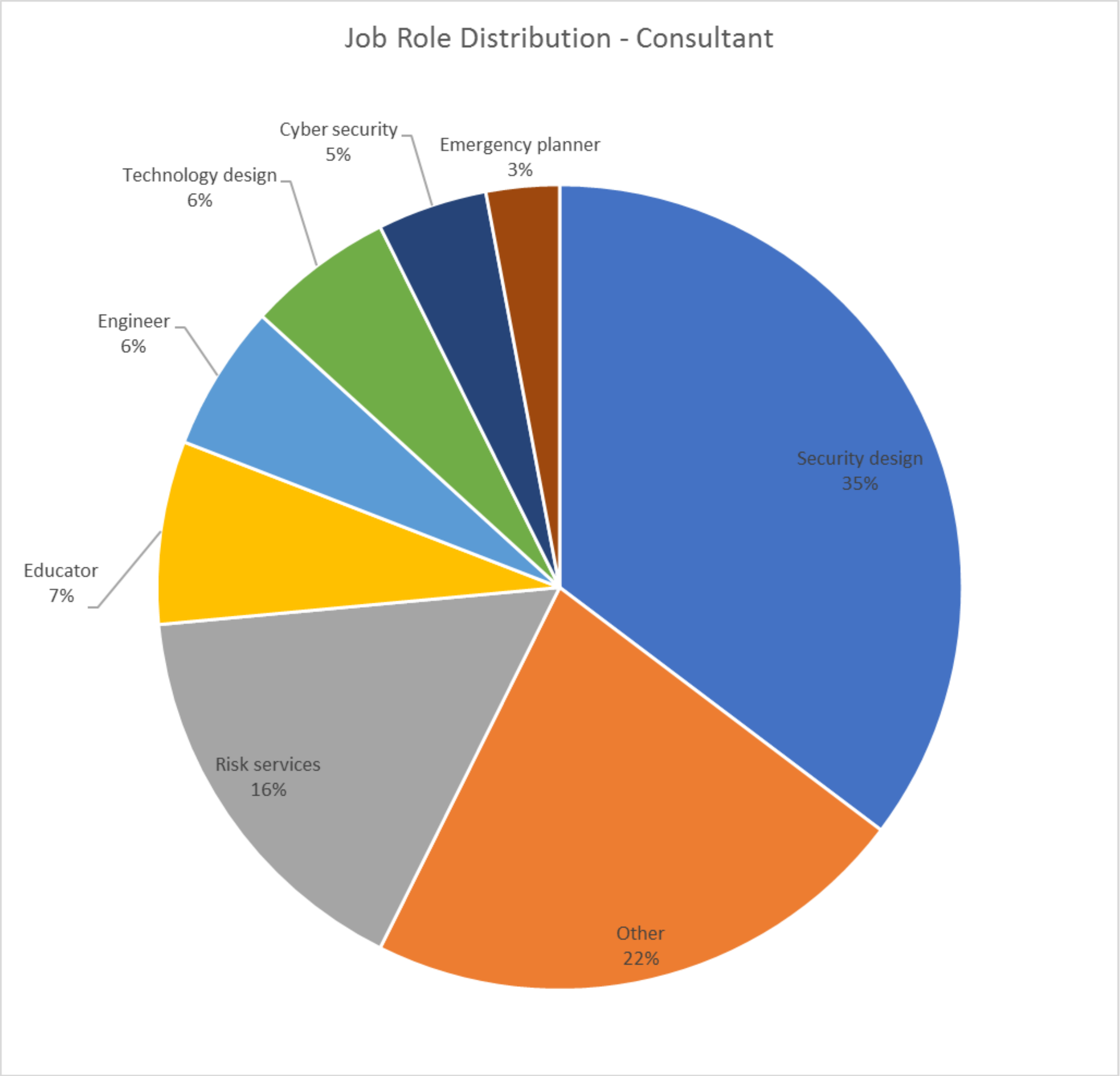


Figure F.4. Job role distribution: Consultants (n=68)

Table F.3
Other reported Consultant roles

Other Reported Roles (Consultant):
Advisor
Business Continuity / Disaster Recovery
critical infrastructure federal standards compliance
Due Diligence and Compliance Investigations
forensic scientist
International Consultant
my role covers a number of the above elements
Solutions Engineer

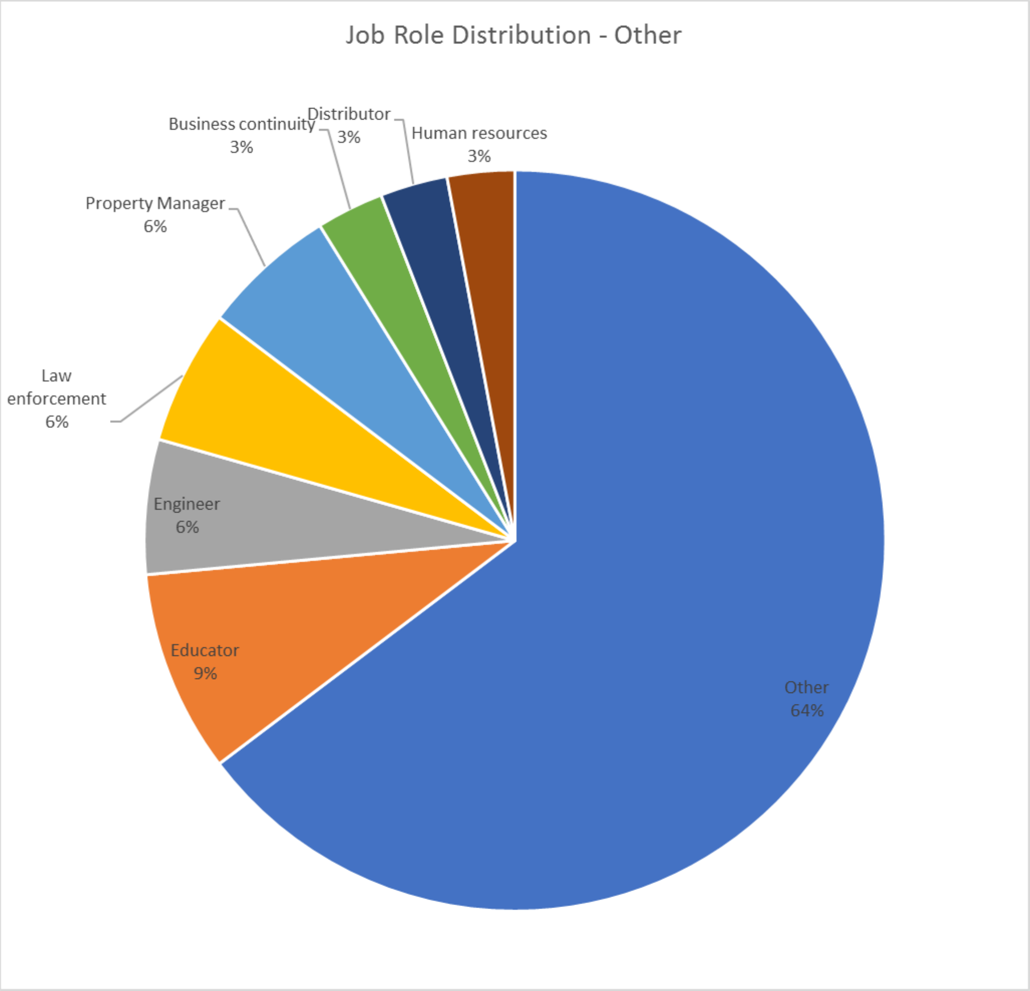


Figure F.5. Job role distribution: Other role functions (n=34)

Table F.4
Other reported role functions

Other reported role functions
Administration
Corp Bus Dev for Security Product Manufacturer
DEveloper of Risk Management and Incident reporting applications
Federal LEO
Integrator
Law enforcement
Manufacturer
Physical Security
Program Manager
QSHE
Service Provider
Systems Integrator
Technical Services Director

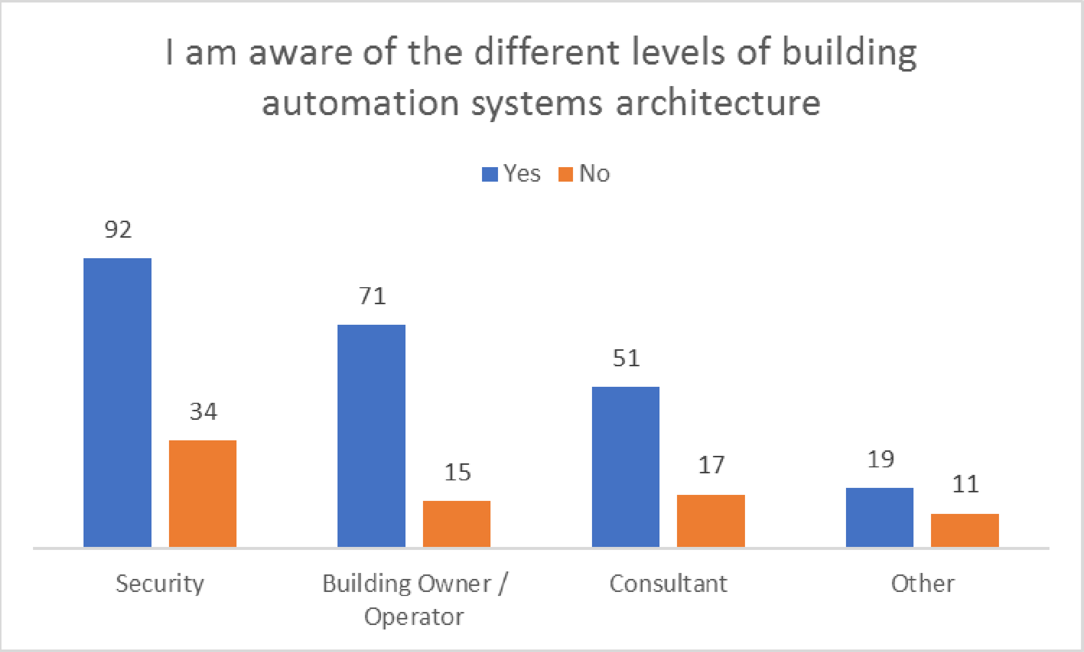


Figure F.6. Awareness of BACS architecture (n=310)

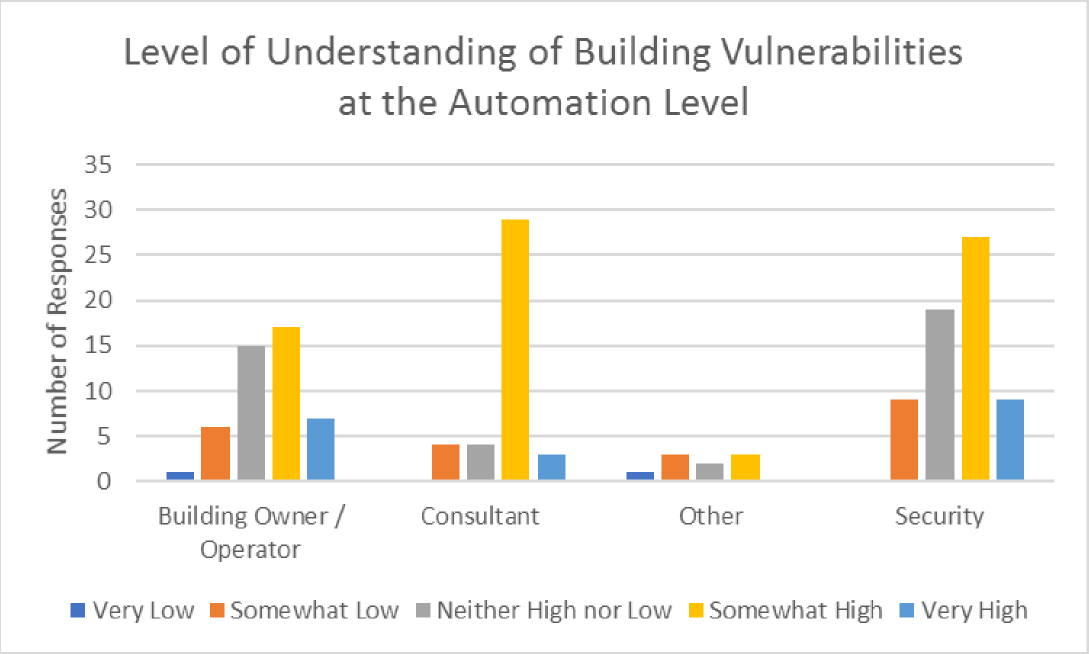


Figure F.7. Level of BACS understanding: Automation level (n=159)

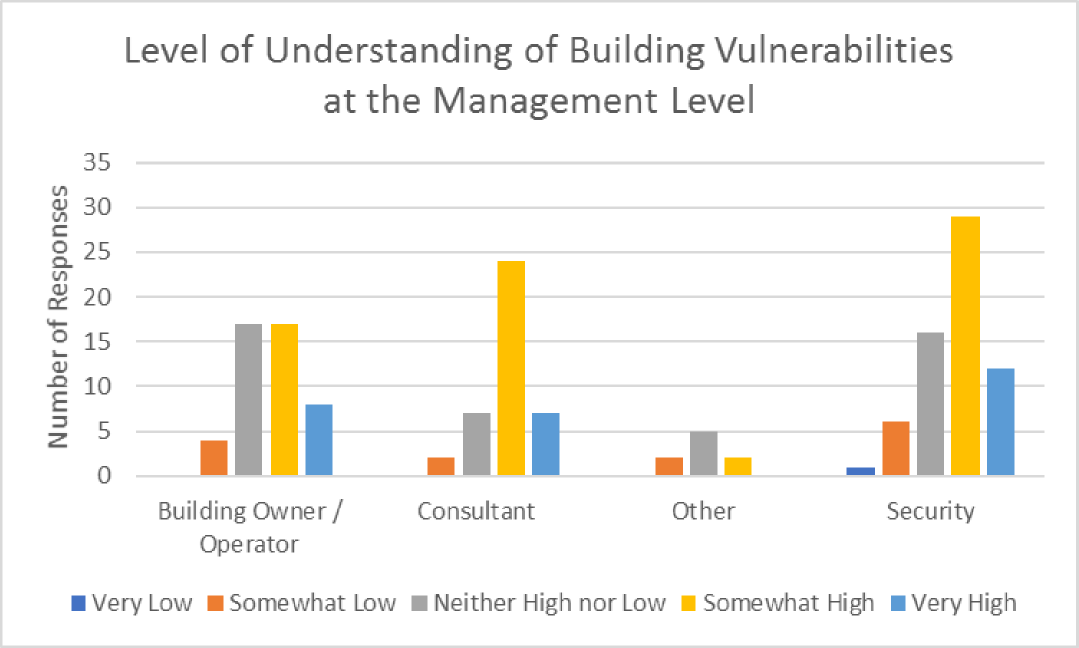


Figure F.8. Level of BACS understanding: Management level (n=159)

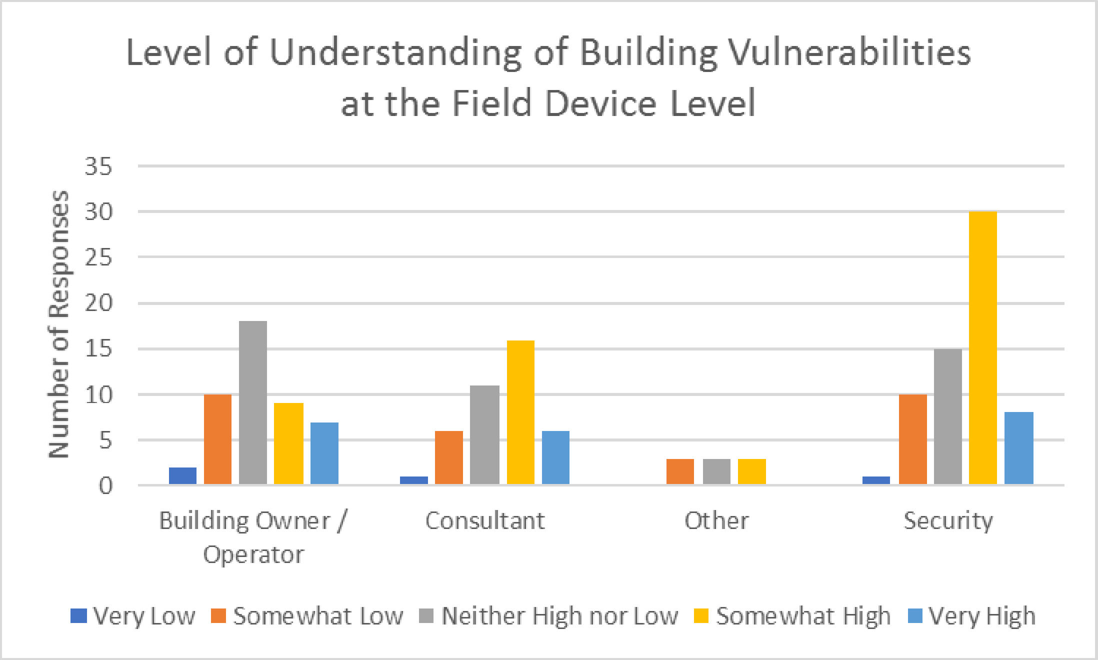


Figure F.9. Level of BACS understanding: Field level (n=159)

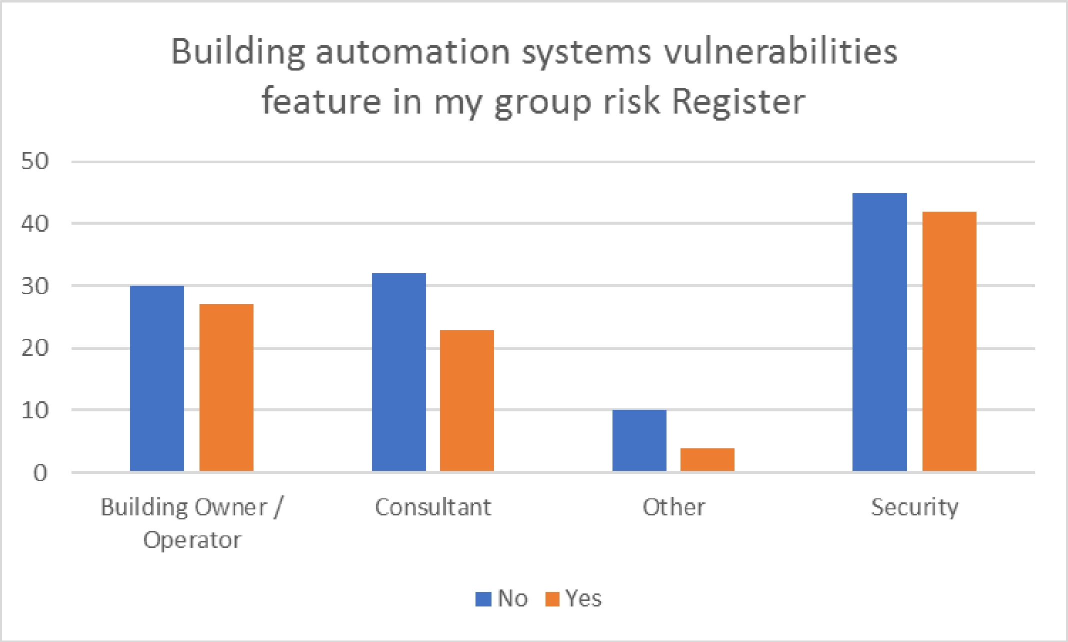


Figure F.10. Inclusion of BACS vulnerabilities in risk register (n=213)

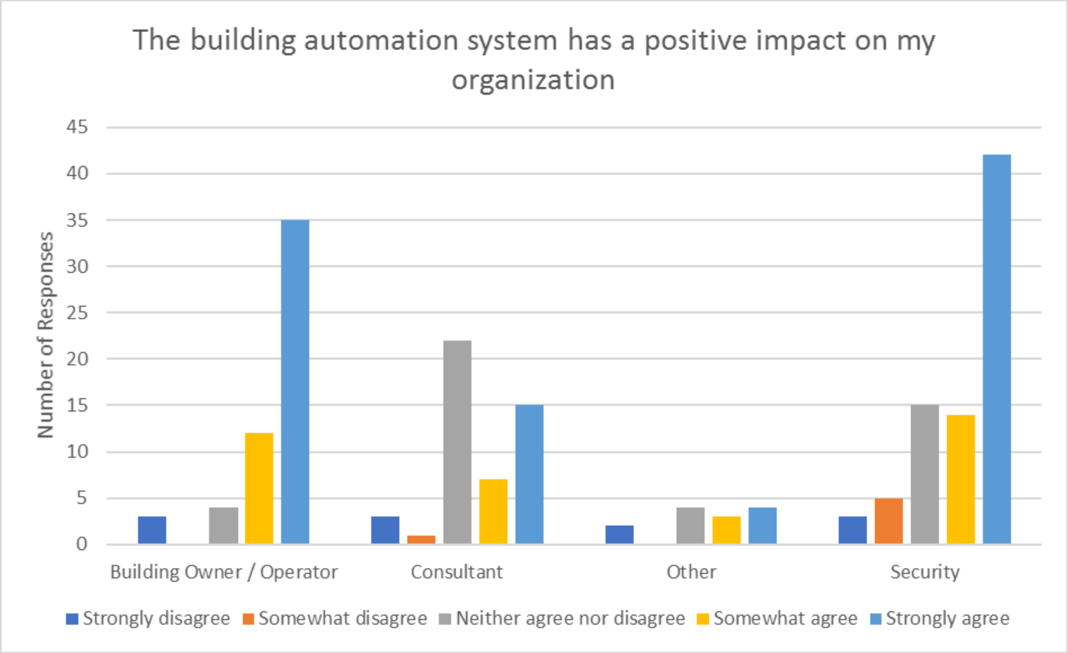


Figure F.11. Perceptions of BACS positive impacts by role function (n=194)

Table F.5

Positive and negative BACS impacts – Building Owner Operators

Positive Impacts of building automation systems – Building Owner/Operators (n=34)	Negative Impacts of building automation systems – Building Owner/Operators (n=29)
Building temperature, lighting control, security,	access controls, additional equipment
comfort for tenants = tenant retention energy management building engineer time management = lower operating expenses meter reading abilities = engineering time and billing efficiencies	Complicated, training
Controlled energy usage costs.	Complicates the process for my existing crews in the field.
costs savings-	concerns over "hacking"
Data gathering and anaysis	Cost
efficiency, accessibility, control, benchmarking	Cost of maintenance
employee peace of mind flexibility in controls	Cost to furnish and install.
Energy and Equipment efficiencies that lower the costs of fuels including electricity	Cost, failure, training
Energy cost management Central control management across buildings integrated systems into one management console	Difficult to troubleshoot programming related issues, expensive ongoing maintenance agreements, software stops being updated or supported when new software is released, proprietary systems don't integrate well or at all.
Energy efficiency and operational efficiency. We are working on using the technology for fault detection and predictive measures, but are not yet there as an organization.	employee turn over - threat of tampering
Energy efficiency, tenant satisfaction	expense to install and maintain, lack of knowledge to be able to optimize
energy management, budget management	failures
energy mgmt, tenant comfort, perceived as first class building	Glitches cause issues with card access.
Energy savings	It is never a solve all for everyone's comfort or lighting issues
Energy savings and speed in reporting service calls.	It takes jobs away from the workforce
Energy savings, control of lights and cooling systems for building.	Key system for malware and hacker attacks Must be managed on separate data circuits which increased cost Finding talent to manage solutions.
Immediate shut down in case of emergency and notifications to outside resources	Multiple, disconnected systems. Usually due to legacy systems that need replacement/ integration.
Input to MES, input to asset management, maintenance of environmental conditions	None
Instant response time	none
It helps control and manage program needs for our HVAC system; and provides for efficiencies in our overall operating plan.	None
It helps us to operate facilities efficiently and diagnose issues witht he operations of eqipment	
It provides tenants with a sense of security after hours and on weekends.	
less time spent going to the source of the call. Able to handle after hours A/C from an internet line, do not have to come into the building after hours.	
Lower asset operating costs. Better equipment efficiency.	
Manage multiple functions in multiple portfolios, keep appropriate controls in place, benchmark performance, manage facilities from remote locations, ensure customer satisfaction	
N/A	
operational efficiencies	
Our BAS efficiently controls all HVAC systems in this skyscraper, it is primary to our mechanical operation.	
Overall building operations - HVAC, lighting, tenant condenser loop are key components	
Providing efficiencies for management team, tenants and energy.	

Quick response times, tenant access to remote alarming, tenant access to scheduling, energy efficiency	
reduced energy, reduced risk	
reduction of energy and cost.	
Tenant comfort, energy savings	

Table F.6

Positive and negative BACS impacts – Consultants

Positive Impacts of building automation systems – Consultant (n=17)	**Negative Impacts of building automation systems – Consultant (n=17)**
Allows for remote monitoring of systems in a virtual environment.	Although the systems are relatively secure, they can allow for a remote breach if not carefully monitored causing a disruption to our computer and other systems.
allows standards to be used uniformly takes away signifcant human error allows better monitoring of systems	Automation systems can't replace rational thinking.
BAS provides an opportunity to educate clients of consequences of missed planning and risk scenarios.	Compatibility
Compile data, lower utility costs, and improved security	Cost, some unpredictable failures.
Controlled, effective work environment; cost control, elimination of human operating errors; backup support and notifications for various type emergencies	End user considerations for override.
Danger of Hacking and DDOS attacks on the system controls	For my organization there are no negative business impacts
economy of resources for increased system monitoring.	Increased capital cost, maintenance
efficiency	Increased complexity of management
Energy Efficiency Ease of Use via web page interface Improved Comfort and Control of Space Energy Management & Savings	Mangement can become complacent and not pay attention to detail Significant time needs to set programming parameters More alarms More security risks Expensive
Energy usage, system management, remote system monitoring, early intervention.	N/A
Increased security for employees, access control, and visitor management.	Nil
Integrated controls, real-time information, reduced labour costs	None
Lower usage of electricity for lights and HVAC. Additional capability comes from automated systems providing feedback to management systems of usage outside of normal hours.	Over reliance on system and tendencies to stretch out service and inspection processes
N/A	Same
Reduce human error	unavailability
Total integration	vulnerability to single points of failure which can have critical impact.

Table F.7

Positive and negative BACS impacts – Security

Positive Impacts of building automation systems – Security (n=40)	**Negative Impacts of building automation systems – Security (n=34)**
1. Secure workplace environment	System maintenance costs. Need of continuous formation of the operators. Lack of flexibility to make changes or extensions. Frequent software update.
Access control	1. Negative customer on occaisions
Access control - CCTV -	automated security has one flaw that is constant without physical monitoring can be breached.
access system during an emergency situation	budget allocation, focus on ROI and not on maintenance / performance savings, not building life cycle focus
as it states, 'automation' takes out human error	Building automation inherently forces the IT, physical security and facility operations to interact in a very intimate manner. To achieve maximum benefits of automation, an organization must closely manage the cyber security risk while providing the benefits of a highly interconnected facility and departments.
Associate comfort, ease of operation, improved productivity	Building too hot - persons leave office. Building too cold - persons contract illnesses. Mold in environment - Asthma sufferers impacted heavily
Automated centralized control of the buildings management systems.	Cost to maintain, changes required, automation upgrades don't always go smoothly
automated systems provide standard levels of security across the board. when properly installed it creates a uniformed security presence.	Efficiency increases vulnerability to attack and the consequences of such an attack.
Building automation generates much of our income.	Has vulnerabilities
Central hands-on control of the complex and its security, earlly warning of potential equipment failures, alarm systems tied in.	High cost of maintenance Requires an expert to understand the system Requires a dedicated operator.
Centralized control of essential systems - utilities, hvac, fire and security.	If not documented and maintained properly - and with a high level of understanding - the system will end up working against your objectives.
Comfort of employees - at the least. People productive and happy.	Initial cost of implementation.
Controlling limited access	Initial setting up, and ongoing, costs, need to recruit/retain technically competent operators, potentially vulnerable to attack by hackers.
Done correctly, building automation reduces both energy consumption and physical security risk. limiting the amount of time personnel need to turn lights on and off, automatically locking areas down and collecting feedback information make management and decisions more effective.	Maintenance costs is high given that some of the components are aged, there is a gap in technical skills for maintenance of the systems.
ease access control and record of who is present	no
Easily detects the fire and other hazards	none
energy efficiency =&gt; cost reduction	None, save cost of maintenance.
Facilitates building access	None.
General comfort of work space, cost control benefits	not many people know the "ins and outs" =&gt; select group of people =&gt; dependancy
Good metrics and driving the sustainability agenda	Only when the technology malfunctions.
high	Opposite of the above
I don't manage the facility in terms of infrastructure. However, in these days of cost cutting the BAS I believe puts the controls in your hands to regulate to ALARP cost accruing from running the facility.	possible hacks, etc
improved safety for students, staff and visitors. Greater awareness of security by stakeholders. Cost effective.	Potential of cyber attack.
Increases daily operational efficiency.	the system needs specialized and expensive maintenance
interoperability, less manual, automated reporting & functions. less physical manpower	to manual; loosing the man
It increases the efficiency of the security function, and boost management's perception of the function.	Unknown
It results to efficient operation of our equipment It also improved equipment performance	unsure

It increased equipment life circle	
It help reduced cost	
It also help in safety operations	
loss prevention, Employee data, Production tracking	Where the system is compromised every arm of the building goes down.
Much more efficient and timely notification and response to equipment malfunction issues.	With any automation it can malfunction and sometimes creates disturbances with utilizations of certain access points creating disruption with traffic flow
Provides a higher sense of security and control of the building occupants, which has increased moral.	
Reduction of costs. High level of integration. Ease of documentation and maintenance.	
Rely on expected climate working conditions, and cooling of equipment	
Satisfies our customer's basic needs.	
Savings, total control, integration with security & safety, better performance, tenant comfort and performance	
The automation and management of the physical security of the installation.	
unsure	
we have a more efficient building	

Table F.8

Positive and negative BACS impacts – Other role functions

Positive Impacts of building automation systems – Other (n=7)	**Negative Impacts of building automation systems – Other (n=6)**
Access control and monitoring. Lockdown/lockout. Emergency messaging.	Complexity and breakdowns
Entergy Management, Access Management	Initial,costs and cost of infrastructure
Fire control and suppression. Automated locking for secure areas	Knowledge up gradation lacks
Improved visibility	Many times the interfacing between BAS systems and security can be difficult and time consuming.
Low manpower	
Our company works in conjunction with BAS routinely, to provide security solutions	No specific disadvantages
Reducing time to process visitors	Potential dependence on electronic systems in a high-threat/low-tech, austere and non-permissive environment.
Return on investment	

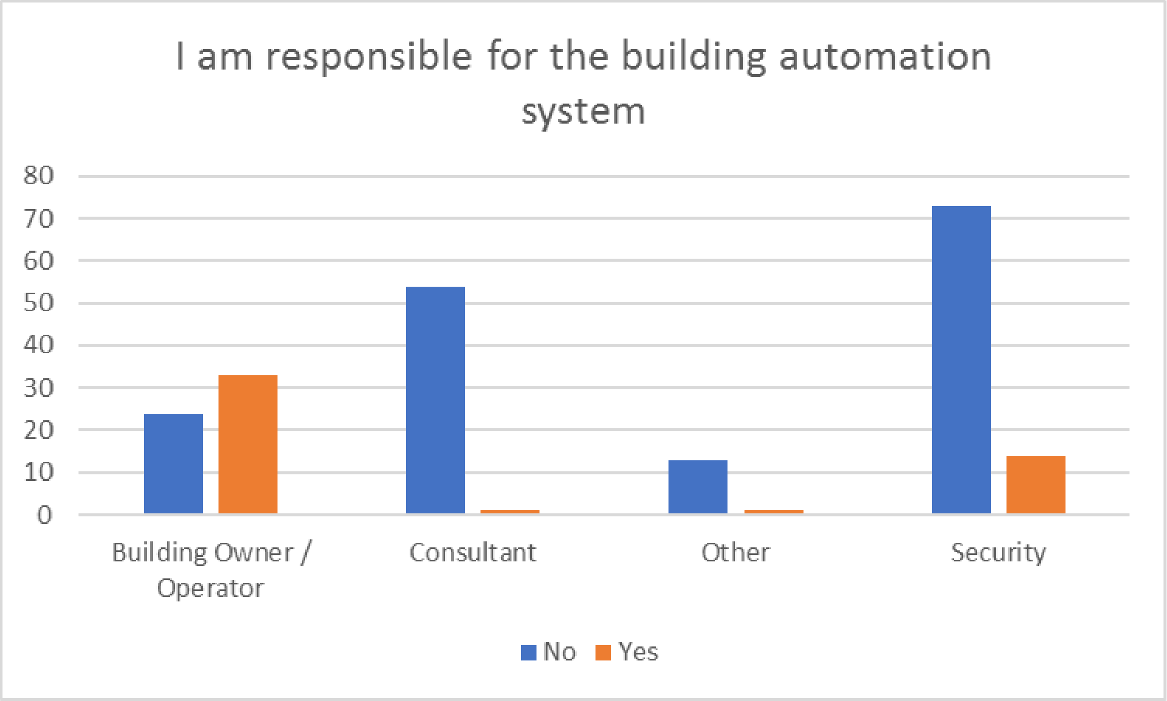


Figure F.12. BACS responsibility by role function (n=213)

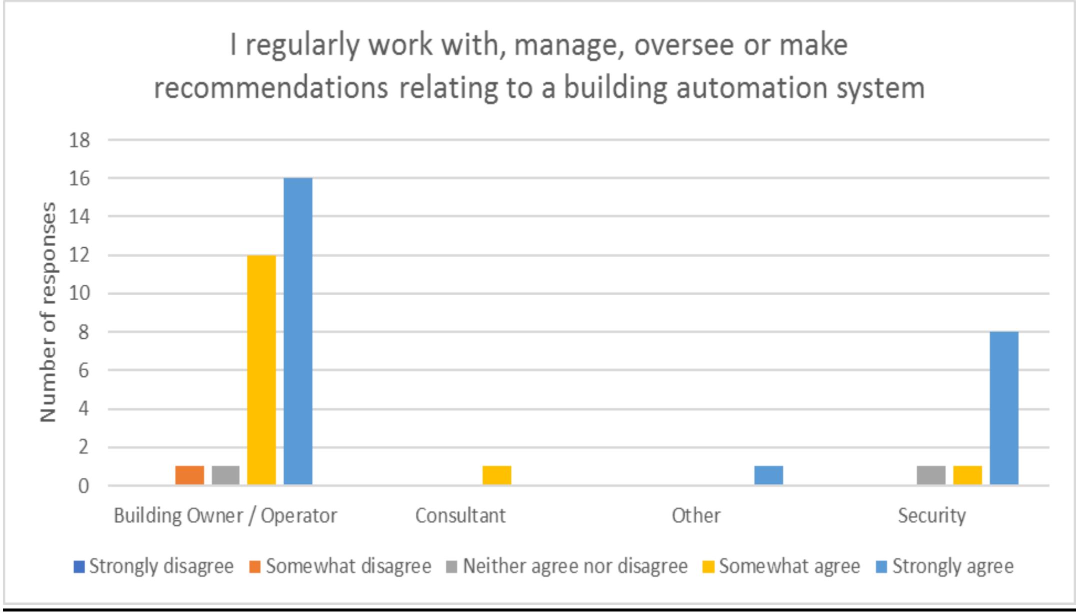


Figure F.13. BACS – Regular recommendations by role function (n=42)

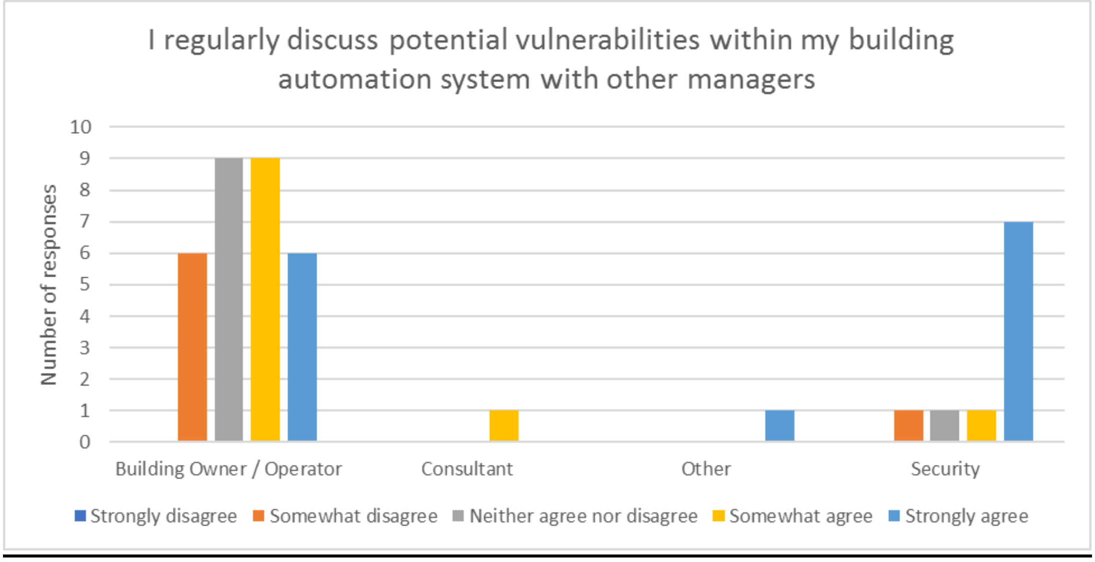


Figure F.14. BACS – Regular discussion by role function (n=42)

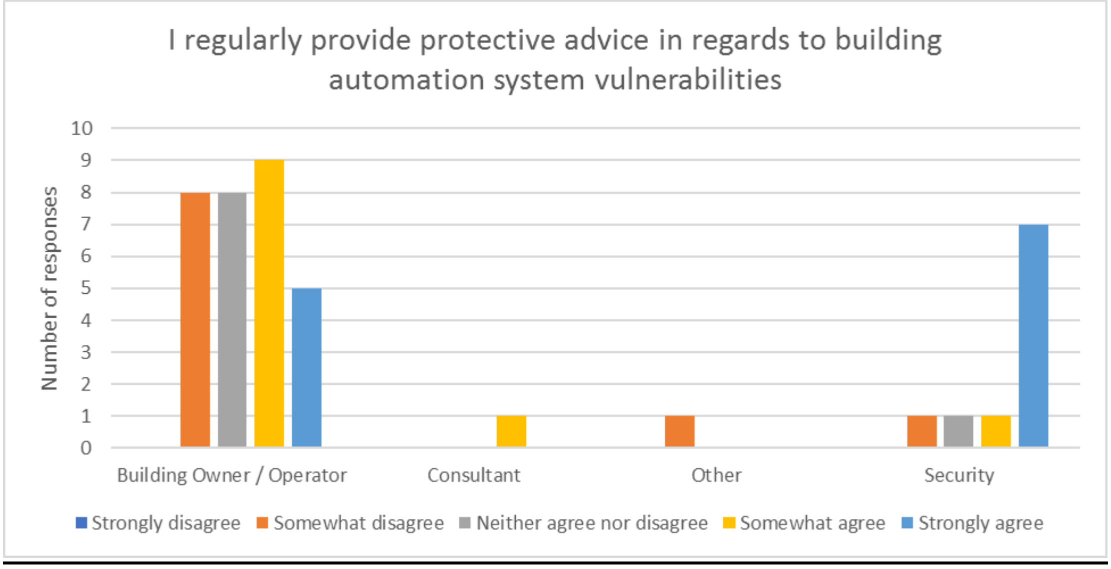


Figure F.15. BACS – Regular protective advice by role function (n=42)

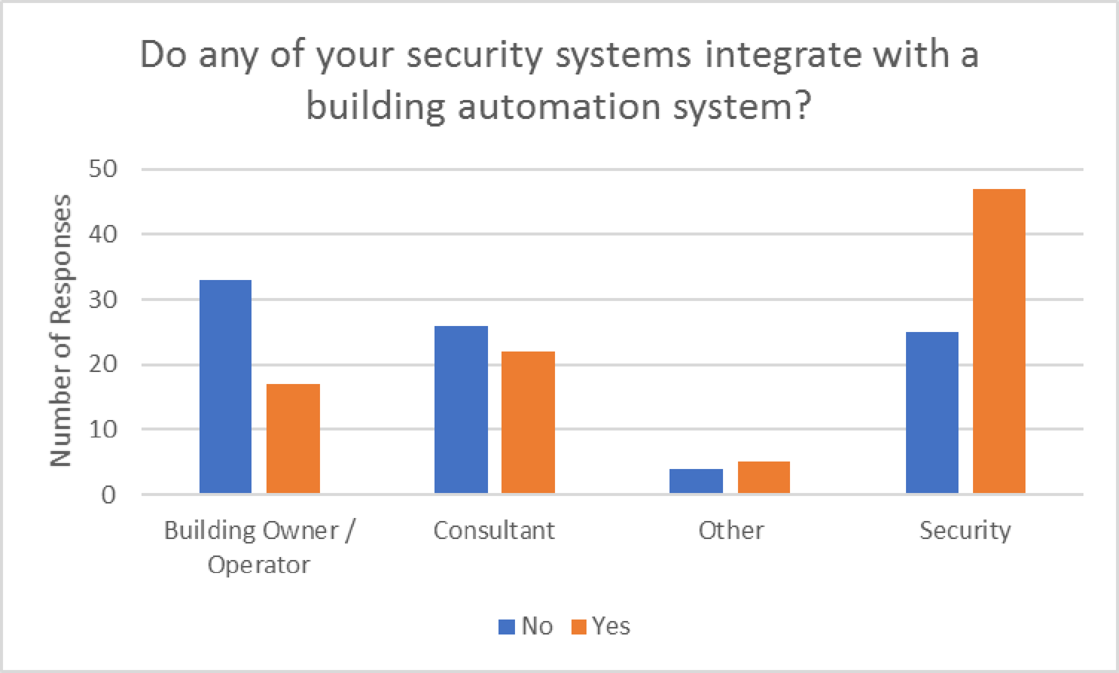


Figure F.16. Perceptions of BACS/Security systems integrations by role function (n=179)

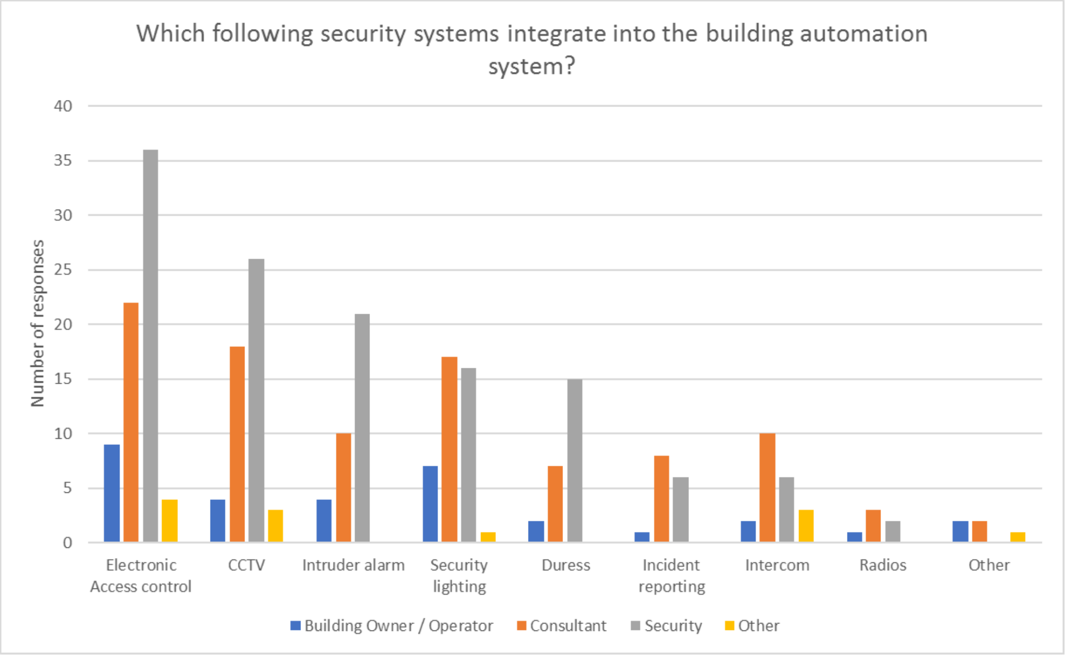


Figure F.17. Types of BACS/Security systems integration by role function (n=144)

Table F.9

Relative percentage of BACS/Security systems integration by role function

	Building Owner/Operator	**Consultant**	**Security**	**Total**
Electronic access control	19%	31%	51%	**26%**
CCTV	14%	35%	51%	**19%**
Intruder alarm	11%	29%	60%	**13%**
Security lighting	19%	41%	39%	**15%**
Duress	8%	29%	63%	**9%**
Incident reporting	7%	53%	40%	**6%**
Intercom	24%	48%	29%	**8%**
Radios	17%	50%	33%	**2%**
Other[1]	60%	40%	0%	**2%**

Note: 1. *Other systems reported: HVAC, fire systems and lift control*

Table F.10

Other Security Systems reported as integrating into building automation systems

Role Function	**Other reported system integrating into BACS**
Building Owner / Operator	Fire Alarm The BAS and security systems are all connected to the intelligent riser which has protective firewalls
Consultant	Fire HVAC Lift control

Vulnerabilities

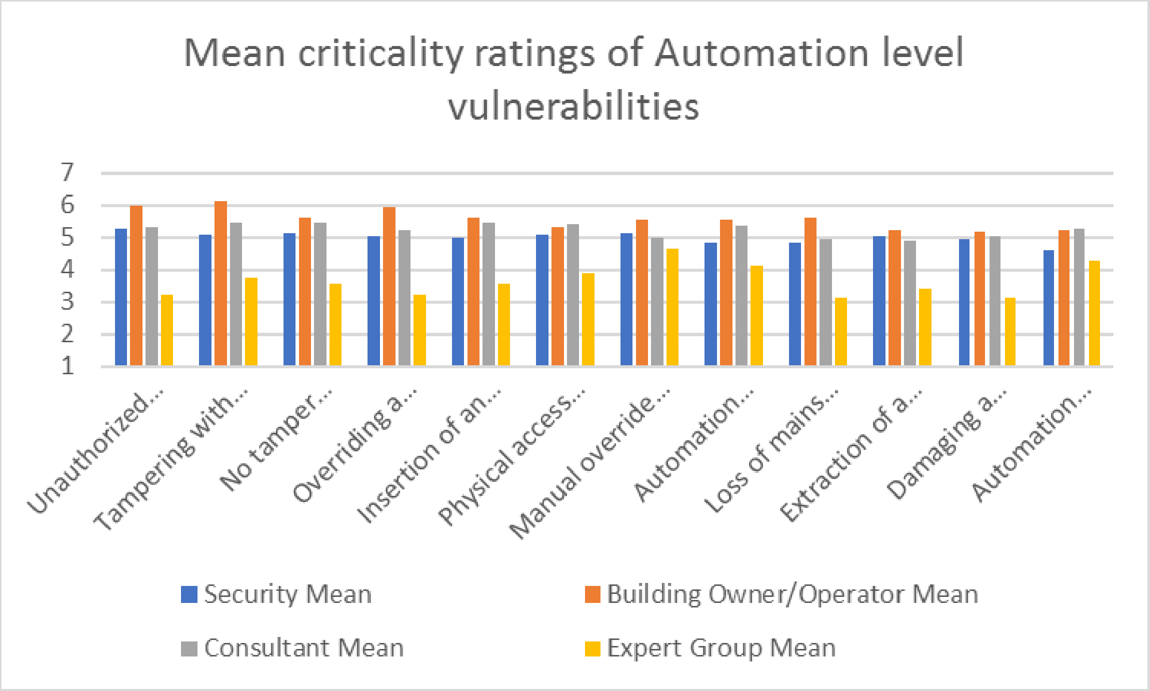


Figure F.18. Mean significance of automation level BACS vulnerabilities by role function

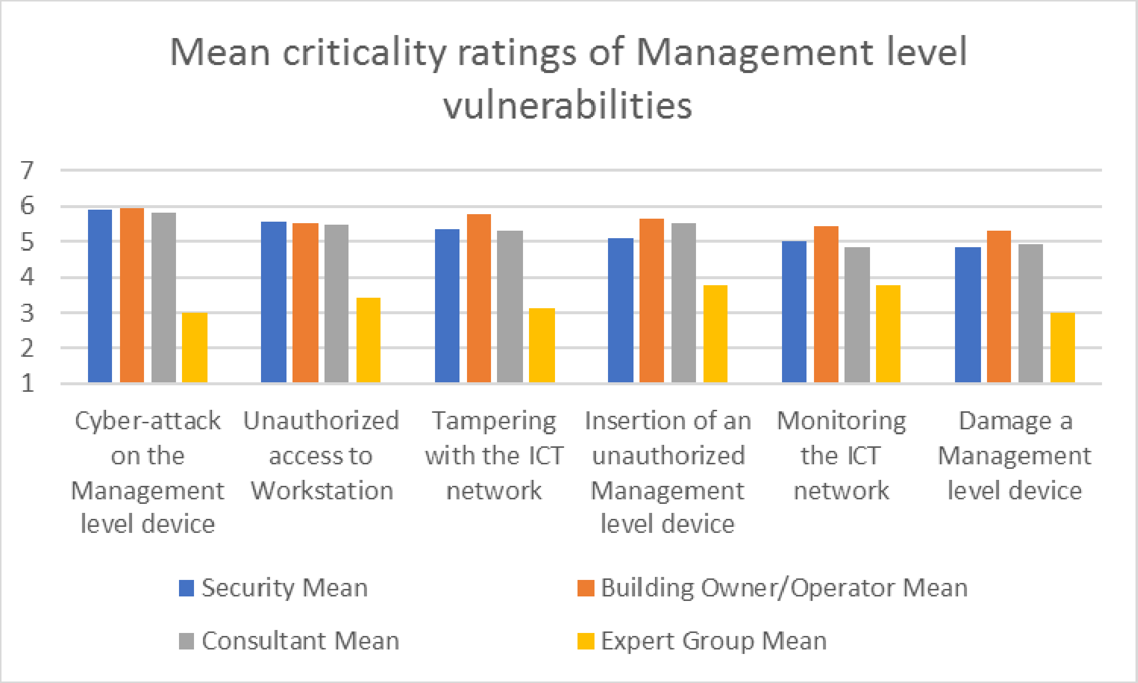
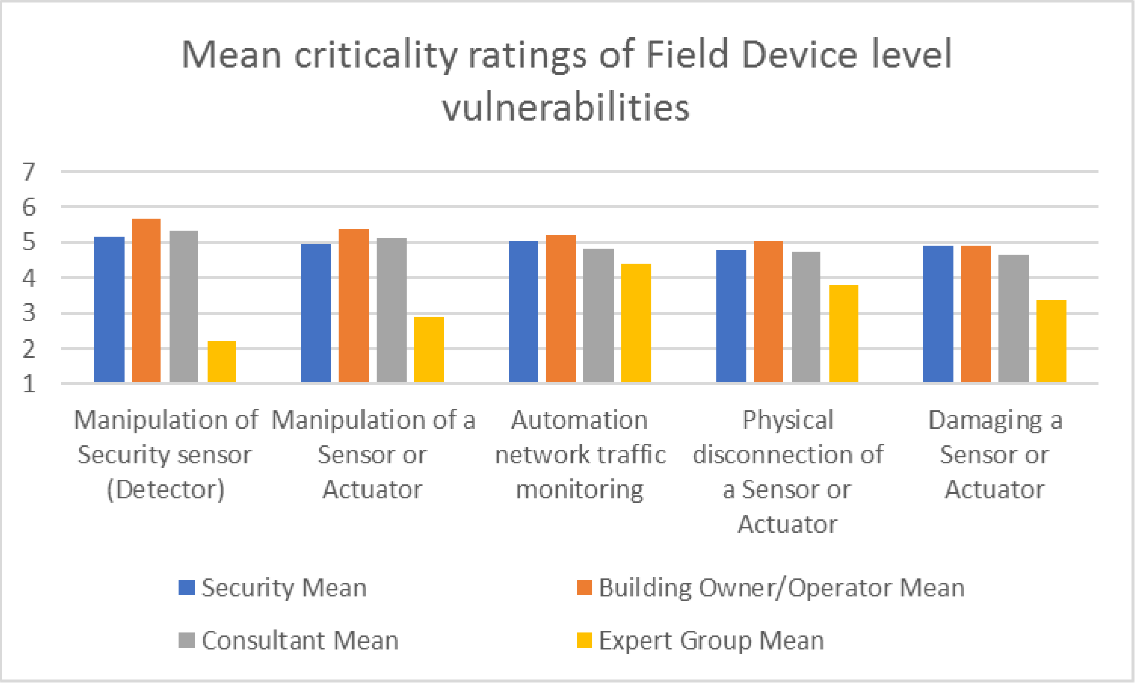


Figure F.19. Mean significance of management level BACS vulnerabilities by role function



n

Figure F.20. Mean significance of field level BACS vulnerabilities by role function

Table F.11

Mean and median ratings of the level of criticality of BACS vulnerabilities by function type

		All			**Security**			**Building Owner/Operator**			**Consultant**			**Expert Group**		
Level		***Mean***	***Median***	***SD***	***Mean***	***Median***	***SD***	***Mean***	***Median***	***SD***	***Mean***	***Median***	***SD***	***Mean***	***Median***	***SD***
Management	Cyber-attack on the Management level device	**5.82**	**7**	*1.73*	**5.90**	**6.5**	*1.67*	5.97	7	*1.68*	**5.80**	**6.5**	*1.63*	3.00	1	*2.26*
Management	Unauthorized access to Workstation	5.52	6	*1.76*	5.55	6	*1.63*	5.54	6	*1.94*	5.50	6	*1.71*	3.44	5	*2.22*
Automation	Unauthorized programming of a Controller	5.46	6	*1.79*	5.25	6	*1.86*	6.00	7	*1.74*	5.31	6	*1.67*	3.22	4	*2.04*
Management	Tampering with the ICT network	5.43	6	*1.66*	5.34	5	*1.59*	5.76	6	*1.65*	5.32	6	*1.69*	3.13	2.5	*2.20*
Automation	Tampering with the Automation network	5.40	6	*1.85*	5.09	6	*1.98*	**6.14**	**7**	*1.53*	5.45	6	*1.63*	3.75	4	*2.38*
Management	Insertion of an unauthorized Management level device	5.33	6	*1.88*	5.11	6	*1.89*	5.65	7	*1.97*	5.54	6	*1.66*	3.78	5	*2.15*
Automation	No tamper detection on Controllers	5.33	6	*1.87*	5.13	6	*1.89*	5.60	6	*1.90*	5.48	6	*1.76*	3.56	4	*1.95*
Automation	Overriding a Controller outputs or inputs	5.29	6	*1.80*	5.02	6	*1.90*	5.94	6.5	*1.41*	5.24	6	*1.77*	3.22	3	*2.20*
Field	Manipulation of Security sensor (Detector)	5.28	6	*1.82*	5.17	6	*1.77*	5.67	7	*1.75*	5.33	6	*1.82*	2.22	1	*1.69*
Automation	Insertion of an unauthorized Controller	5.26	6	*1.97*	5.00	6	*2.06*	5.58	7	*2.03*	5.45	6	*1.66*	3.56	4	*1.95*
Automation	Physical access to a controller	5.23	6	*1.89*	5.07	6	*1.91*	5.32	6	*2.05*	5.41	6	*1.69*	3.89	4	*1.91*
Automation	Manual override of Controllers output switches	5.19	6	*1.84*	5.12	6	*1.75*	5.57	6	*1.90*	4.97	5	*1.85*	**4.63**	6	*2.12*
Automation	Automation level open source network programs	5.16	6	*1.75*	4.83	5	*1.87*	5.53	6	*1.48*	5.38	6	*1.62*	4.11	5	*2.08*
Field	Manipulation of a Sensor or Actuator	5.09	5	*1.71*	4.96	5	*1.71*	5.39	6	*1.80*	5.13	5	*1.59*	2.88	2.5	*1.90*
Management	Monitoring the ICT network	5.06	6	*1.85*	5.00	6	*1.78*	5.43	6	*1.99*	4.84	5	*1.81*	3.75	4	*2.05*
Automation	Loss of mains power	5.06	6	*2.03*	4.86	5	*1.97*	5.62	6	*1.95*	4.93	6	*2.09*	3.11	1	*2.47*
Automation	Extraction of a Controller's latent memory	5.05	6	*1.84*	5.02	6	*1.87*	5.21	6	*2.08*	4.87	5	*1.58*	3.43	4	*2.19*
Automation	Damaging a Controller	5.02	6	*1.83*	4.95	6	*1.86*	5.17	6	*1.96*	5.05	6	*1.68*	3.11	3	*2.08*
Field	Automation network traffic monitoring	5.01	6	*1.77*	5.02	5	*1.74*	5.22	6	*1.83*	4.84	5	*1.76*	4.38	4.5	*2.23*
Management	Damage a Management level device	4.99	6	*1.79*	4.86	5	*1.85*	5.29	6	*1.77*	4.92	5	*1.61*	3.00	3.5	*1.73*
Automation	Automation network traffic data injection	4.98	5.5	*1.89*	4.59	5	*2.00*	5.23	6	*1.84*	5.26	6	*1.76*	4.25	4.5	*1.85*
Field	Physical disconnection of a Sensor or Actuator	4.81	5	*1.88*	4.79	5	*1.92*	5.03	6	*1.94*	4.75	5	*1.76*	3.78	4	*1.81*
Field	Damaging a Sensor or Actuator	4.81	5	*1.76*	4.91	6	*1.78*	4.89	5.5	*1.95*	4.64	5	*1.49*	3.38	3	*1.93*

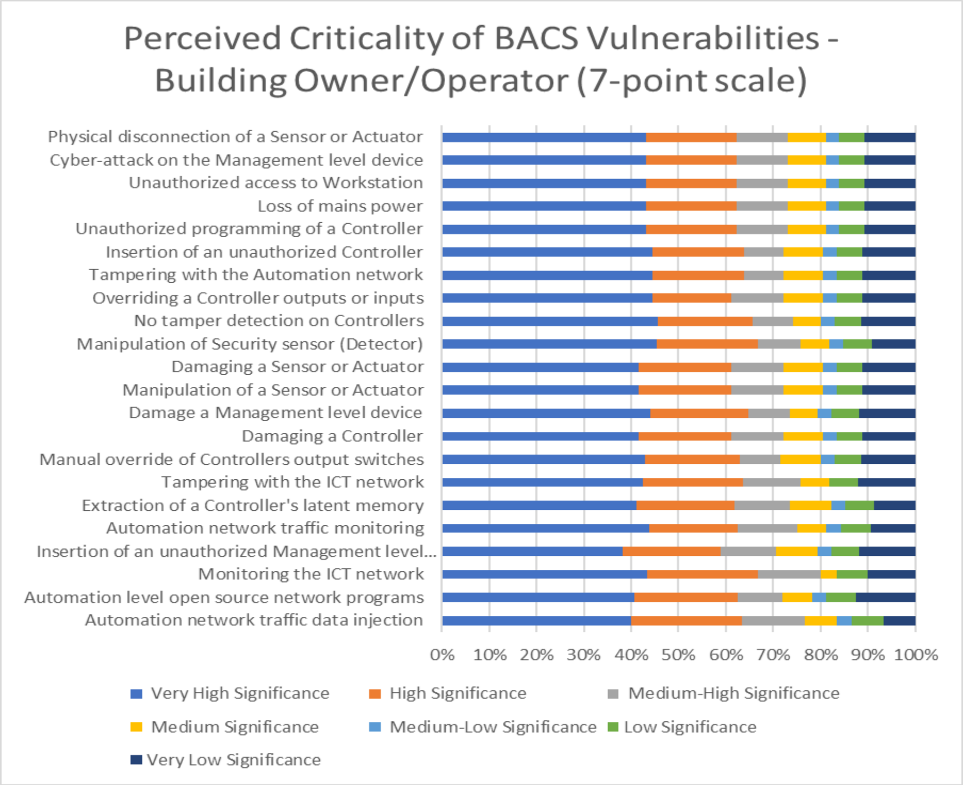


Figure F.21. Perceived criticality significance of BACS vulnerabilities: Building owner/operators (7-point Likert scale)

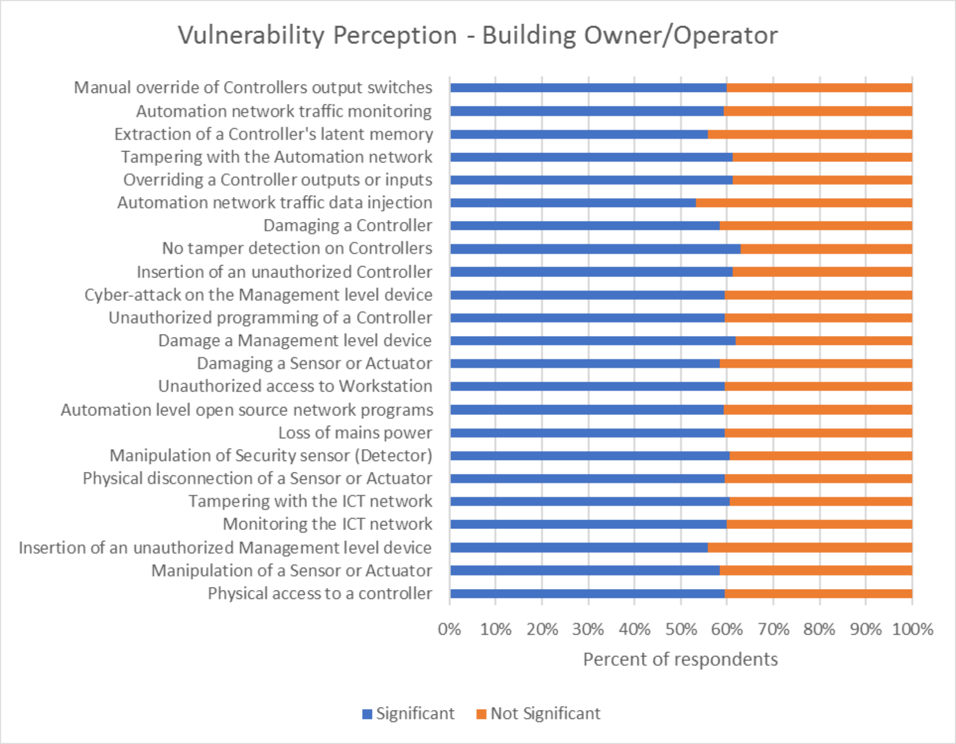


Figure F.22. Perceived criticality significance of BACS vulnerabilities: Building owner/operators (Simplified)

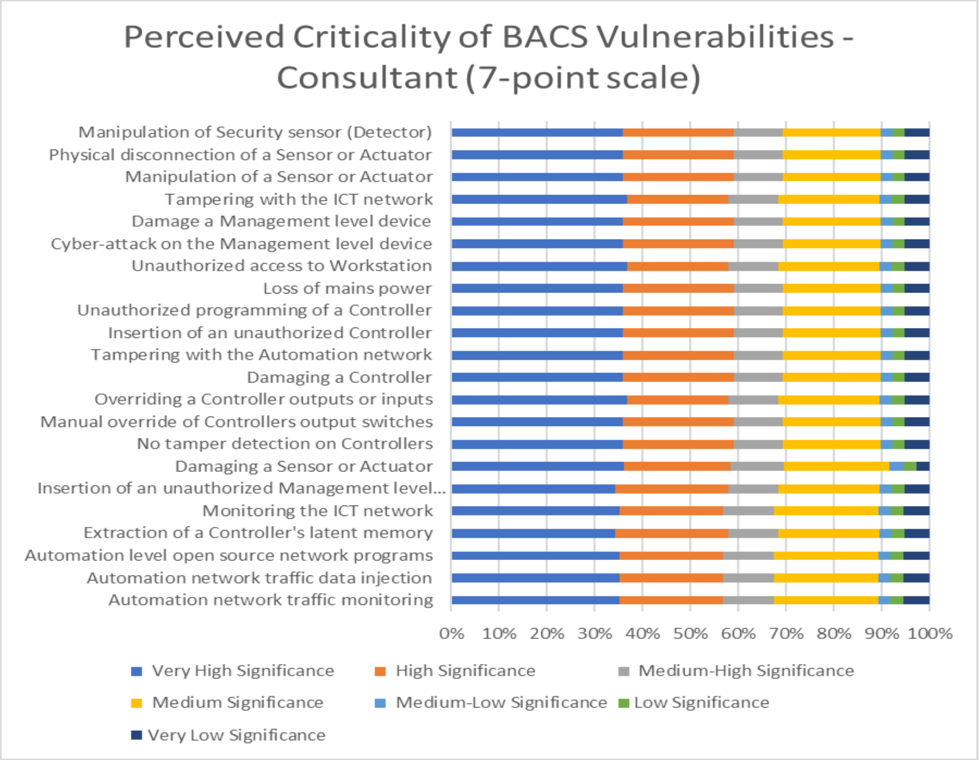


Figure F.23. Perceived criticality significance of BACS vulnerabilities: Consultants (7-point Likert scale)

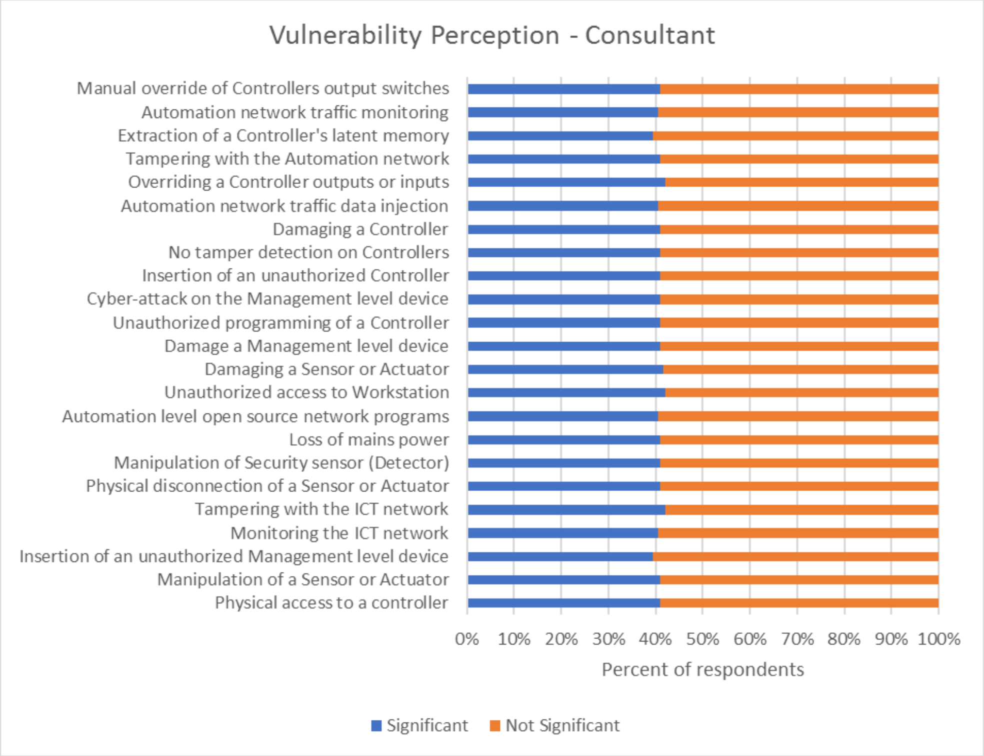


Figure F.24. Perceived criticality significance of BACS vulnerabilities – Consultants (Simplified)

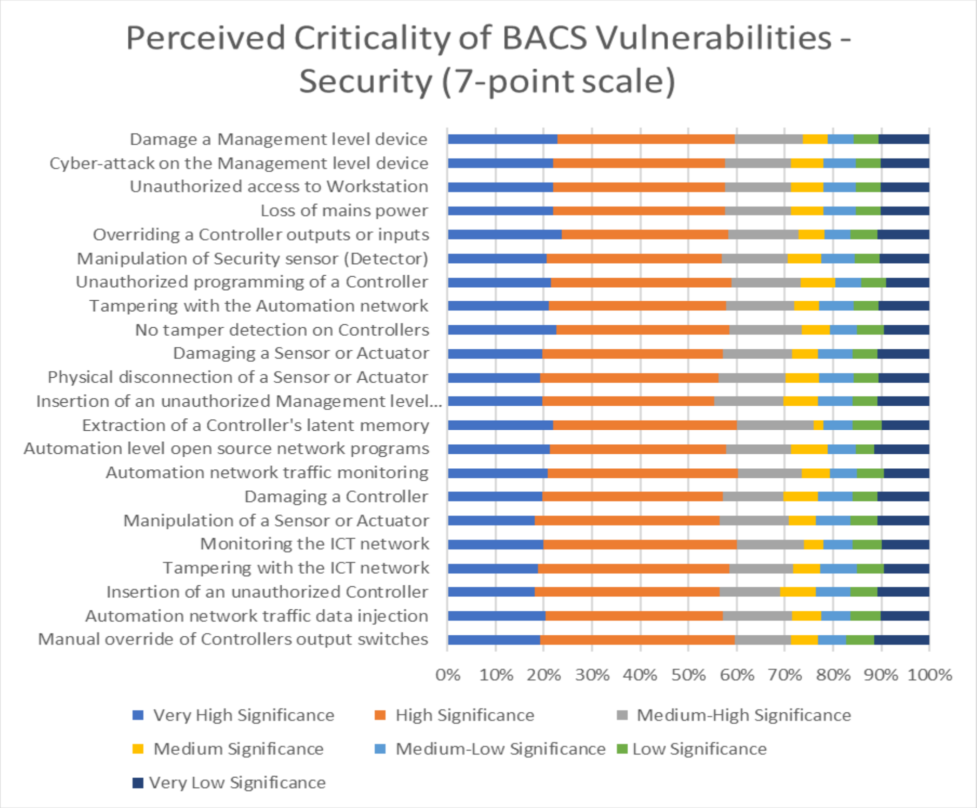


Figure F.25. Perceived criticality significance of BACS vulnerabilities: Security (7-point Likert scale)

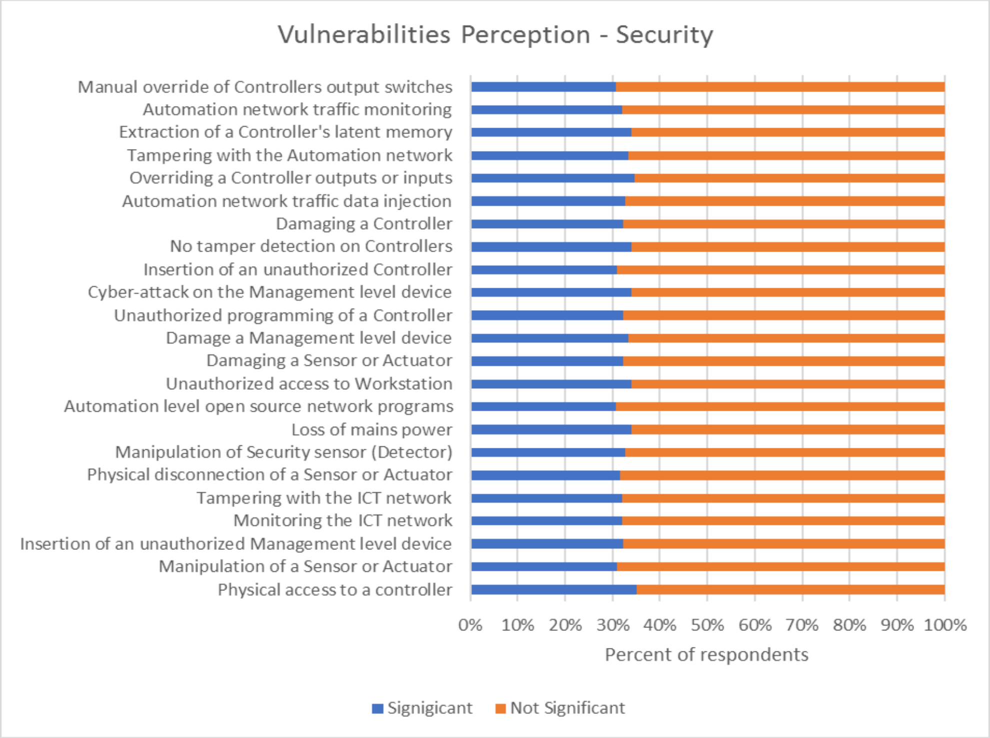


Figure F.26. Perceived criticality significance of BACS vulnerabilities: Security (Simplified)

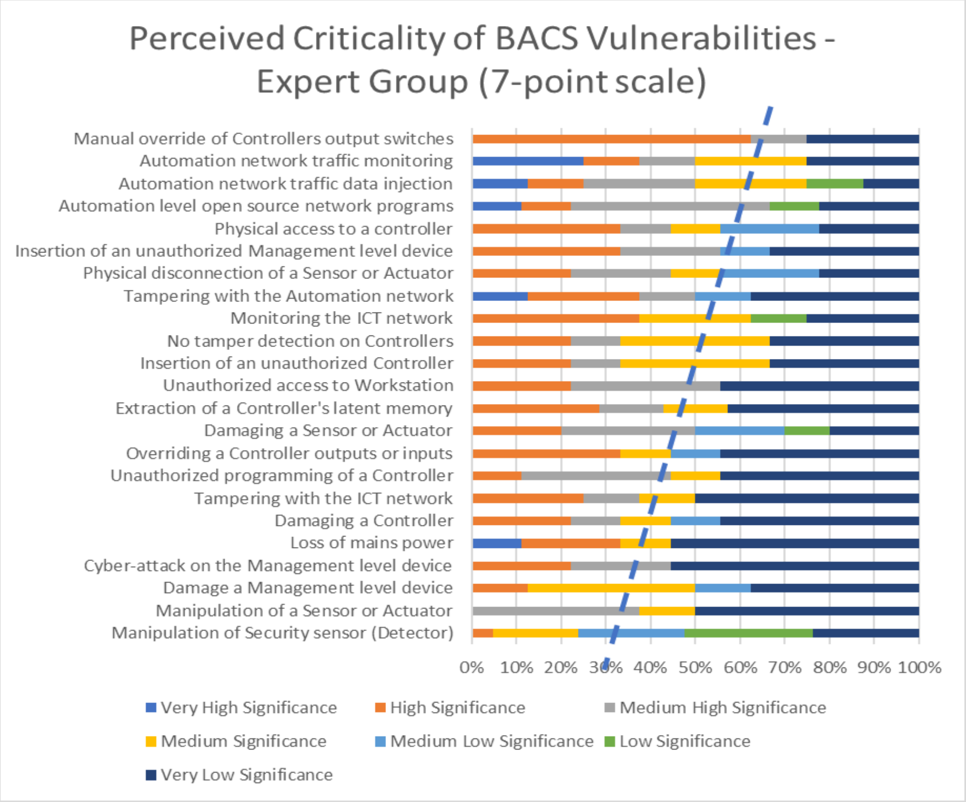


Figure F.27. Perceived criticality significance of BACS vulnerabilities: Expert Group (7-point Likert scale)

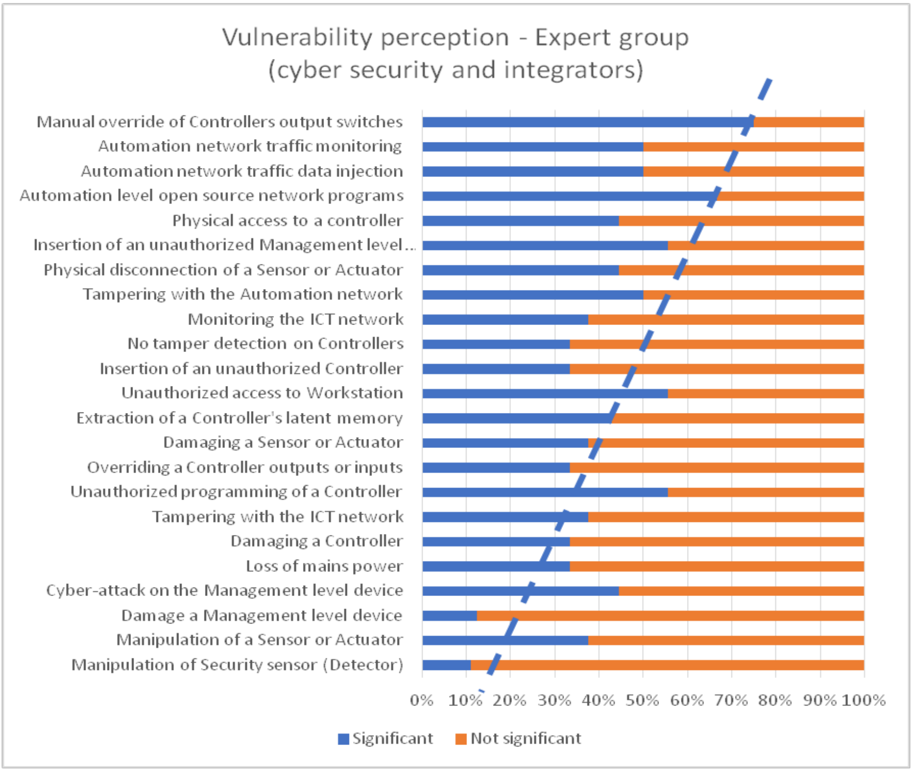


Figure F.28. Perceived criticality significance of BACS vulnerabilities: Expert Group (Simplified)

Table F.12

Expert Group mean and median ratings of the level of criticality of BACS vulnerabilities in highest order

Level	Expert Group	Mean	Median	SD
Automation	Manual override of Controllers output switches	**4.63**	6	*2.12*
Field	Automation network traffic monitoring	4.38	4.5	*2.23*
Automation	Automation network traffic data injection	4.25	4.5	*1.85*
Automation	Automation level open source network programs	4.11	5	*2.08*
Automation	Physical access to a controller	3.89	4	*1.91*
Management	Insertion of an unauthorized Management level device	3.78	5	*2.15*
Field	Physical disconnection of a Sensor or Actuator	3.78	4	*1.81*
Automation	Tampering with the Automation network	3.75	4	*2.38*
Management	Monitoring the ICT network	3.75	4	*2.05*
Automation	No tamper detection on Controllers	3.56	4	*1.95*
Automation	Insertion of an unauthorized Controller	3.56	4	*1.95*
Management	Unauthorized access to Workstation	3.44	5	*2.22*
Automation	Extraction of a Controller's latent memory	3.43	4	*2.19*
Field	Damaging a Sensor or Actuator	3.38	3	*1.93*
Automation	Unauthorized programming of a Controller	3.22	4	*2.04*
Automation	Overriding a Controller outputs or inputs	3.22	3	*2.2*
Management	Tampering with the ICT network	3.13	2.5	*2.2*
Automation	Loss of mains power	3.11	1	*2.47*
Automation	Damaging a Controller	3.11	3	*2.08*
Management	Cyber-attack on the Management level device	3	1	*2.26*
Management	Damage a Management level device	3	3.5	*1.73*
Field	Manipulation of a Sensor or Actuator	2.88	2.5	*1.9*
Field	Manipulation of Security sensor (Detector)	2.22	1	*1.69*

Table F.13

Significant results from one-way between groups ANOVA on role function and mean vulnerability perception

Vulnerability	***df***	***F***	**CI**	***p***	***n^2***	**Direction**	**Magnitude**	***p***	***d***
No tamper detection on Controllers	2, 94	4.02	[4.75, 5.56]	.021	.08	Building > Expert	2.04	.017	.58
Overriding a Controller outputs or inputs	2, 97	8.79	[4.81, 5.57]	< .001	.15	Building > Security	0.93	.048	.49
						Security > Expert	1.8	.02	.56
						Building > Expert	2.72	< .001	.82
Damaging a Controller	2, 98	4.14	[4.47, 5.26]	.019	.08	Security > Expert	1.84	.03	.53
						Expert > Building	2.06	017	.57
Tampering with the Automation network	2, 98	6.47	[4.96, 5.75]	.002	.12	Building > Security	1.05	.032	.52
						Building > Expert	2.39	.005	.65
Insertion of an unauthorized Controller	2, 97	3.54	[4.66, 5.5]	.033	.07	Building > Expert	2.03	.03	.53
Unauthorized programming of a Controller	2, 99	8.19	[4.95, 5.73]	.001	.14	Security > Expert	2.03	.009	.61
						Building > Expert	2.78	< .001	.81
Loss of mains power	2, 97	3.54	[4.57, 5.39]	.033	.1	Building > Expert	2.51	.004	.67
Unauthorized access to Workstation	2, 103	5.48	[5, 5.73]	.042	.09	Security > Expert	2.11	.005	.64
						Building > Expert	2.1	.008	.61
Cyber-attack on the Management level device	2, 104	11.49	[5.31, 6.05]	< .001	.18	Security > Expert	2.9	< .001	.91
						Building > Expert	2.97	< .001	.89
Damage a Management level device	2, 96	5.02	[4.48, 5.24]	.008	.09	Security > Expert	1.86	.026	.55
						Building > Expert	2.29	.006	.65
Tampering with the ICT network	2, 91	7.76	[4.93, 5.67]	.001	.15	Security > Expert	2.22	.003	.72
						Building > Expert	2.63	< .001	.82
Insertion of an unauthorized Management level device	2, 96	3.27	[4.77, 5.57]	.042	.06	Building > Expert	1.87	.038	.52
Manipulation of a Sensor or Actuator	2, 96	6.51	[4.57, 5.32]	.002	.12	Security > Expert	2.09	.008	.63
						Building > Expert	2.51	.001	.74
Manipulation of Security sensor (Detector)	2, 96	13.39	[4.67, 5.47]	< .001	.22	Security > Expert	2.95	< .001	.94
						Building > Expert	3.44	< .001	1.05

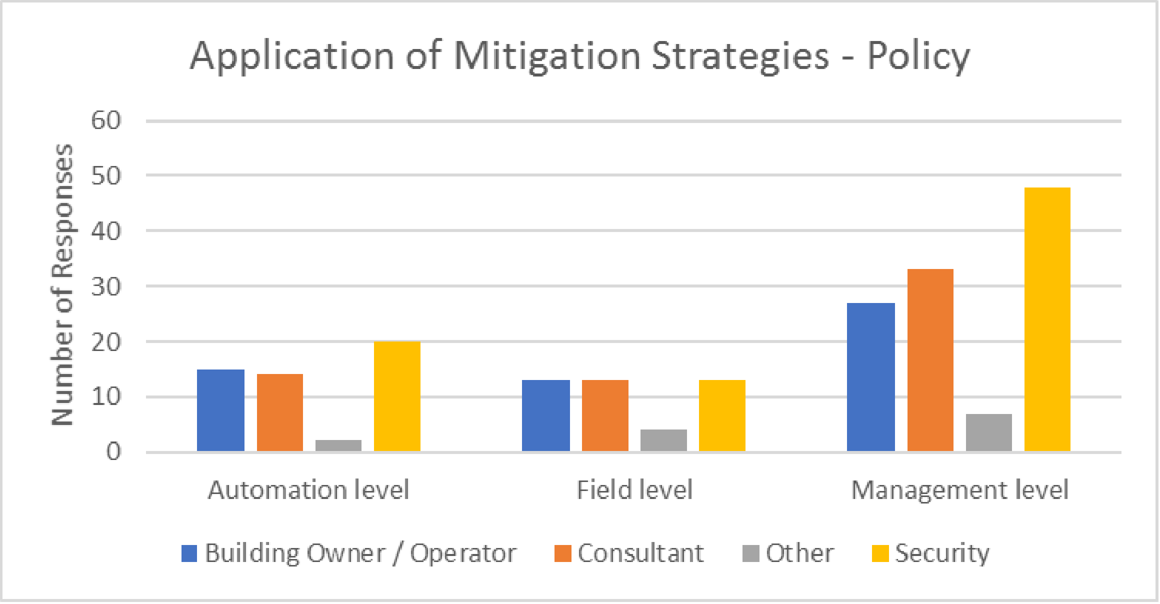


Figure F.29. Application of mitigation strategy by Job function: Policy (n=128)

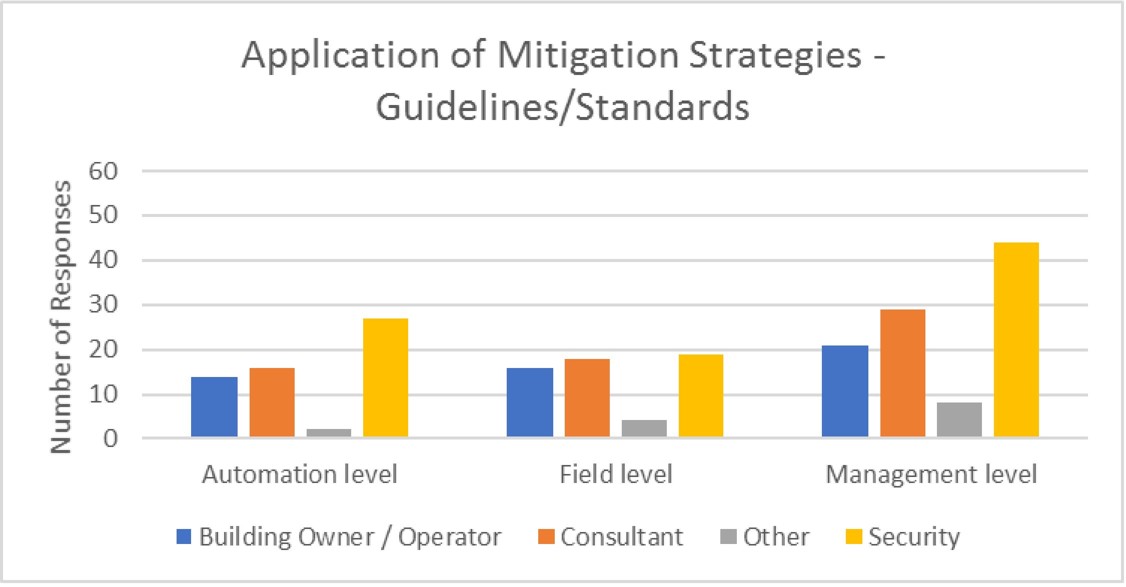


Figure F.30. Application of mitigation strategy by Job function: Guidelines/Standards (n=127)

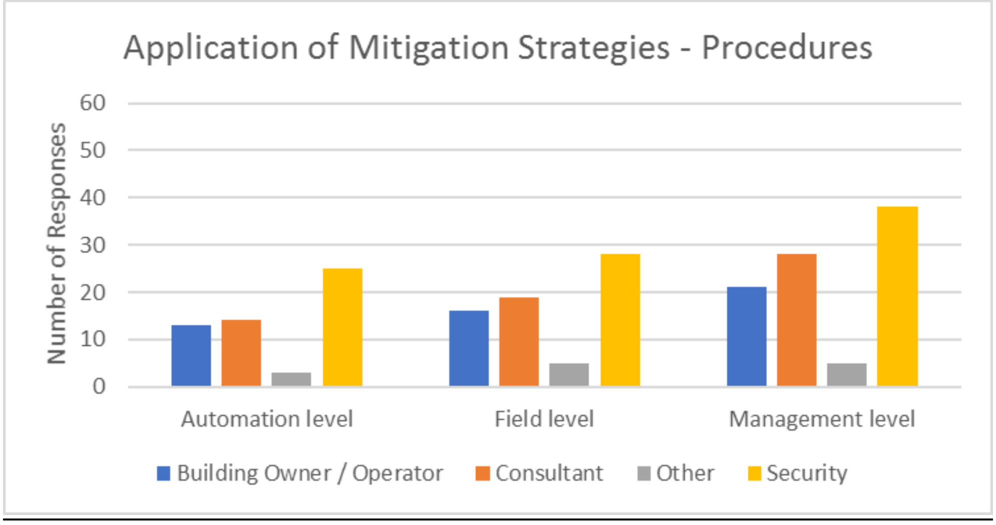


Figure F.31. Application of mitigation strategy by Job function: Procedures (n=130)

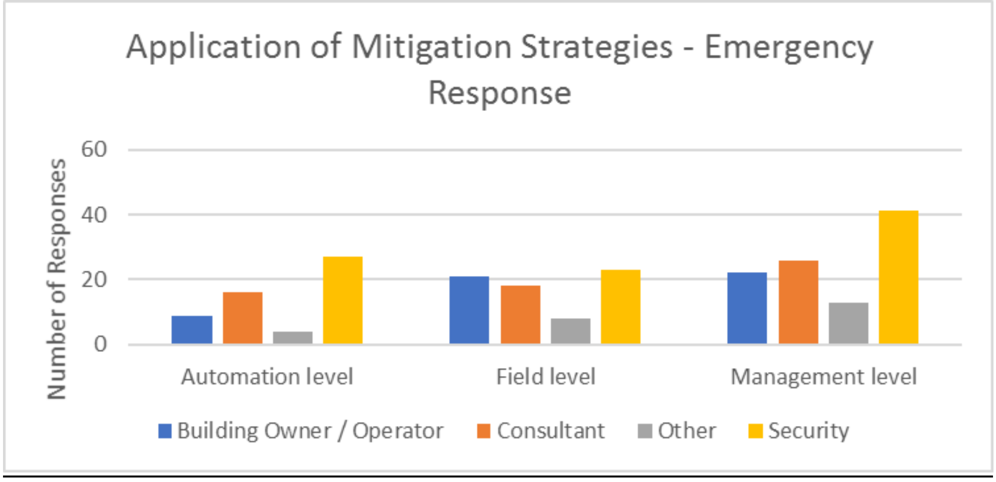


Figure F.32. Application of mitigation strategy by Job function: Emergency Response (n=129)

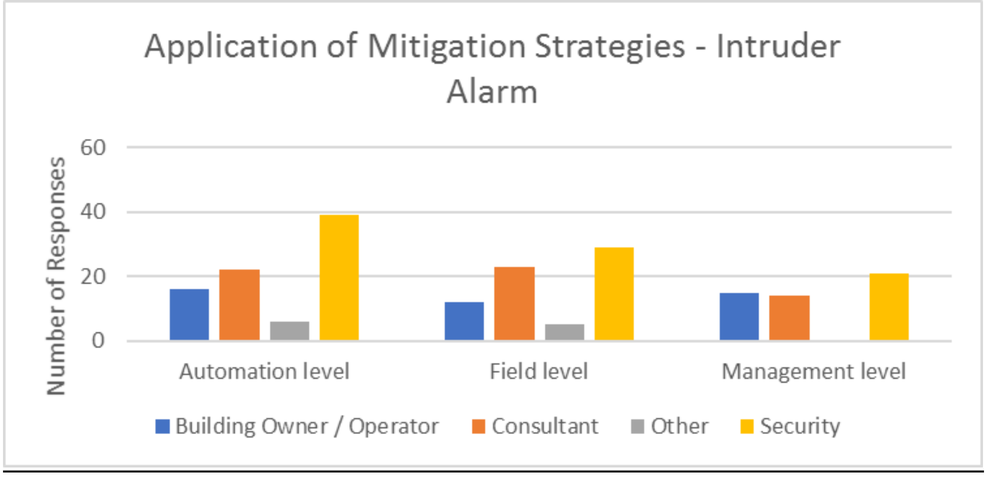


Figure F.33. Application of mitigation strategy by Job function: Intruder Alarm (n=127)

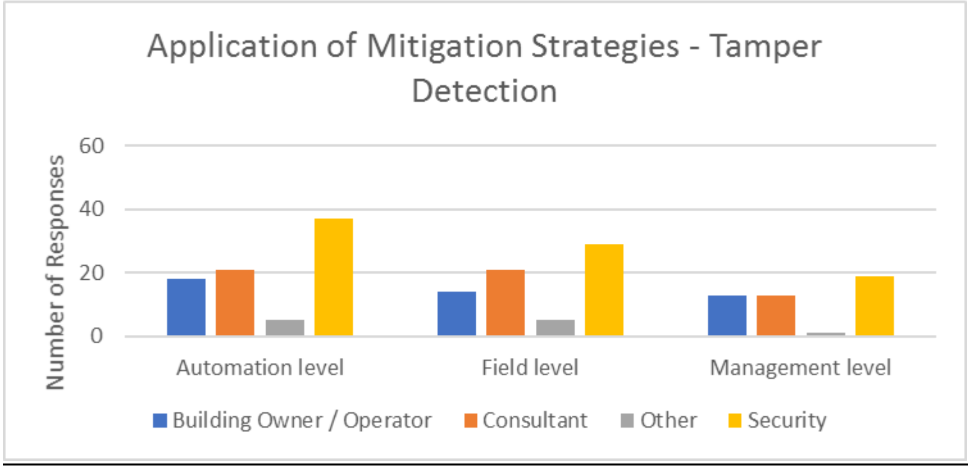


Figure F.34. Application of mitigation strategy by Job function: Tamper Detection (n=126)

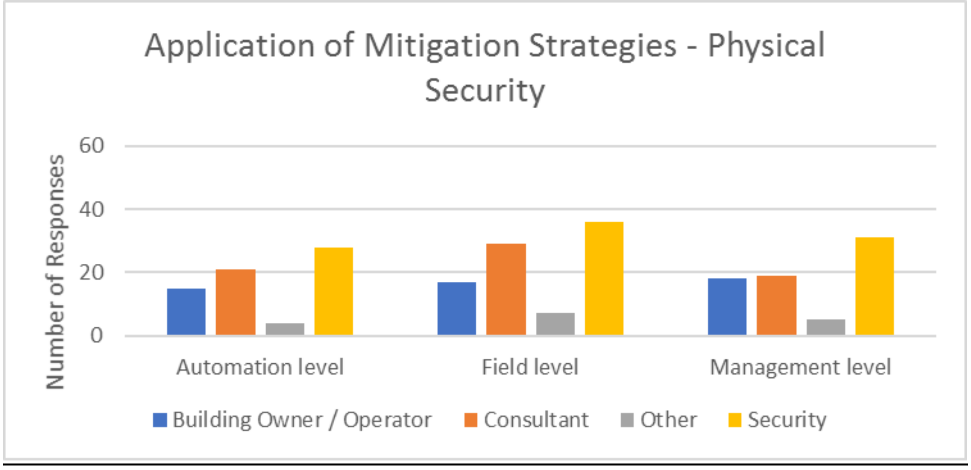


Figure F.35. Application of mitigation strategy by Job function: Physical Security (n=132)

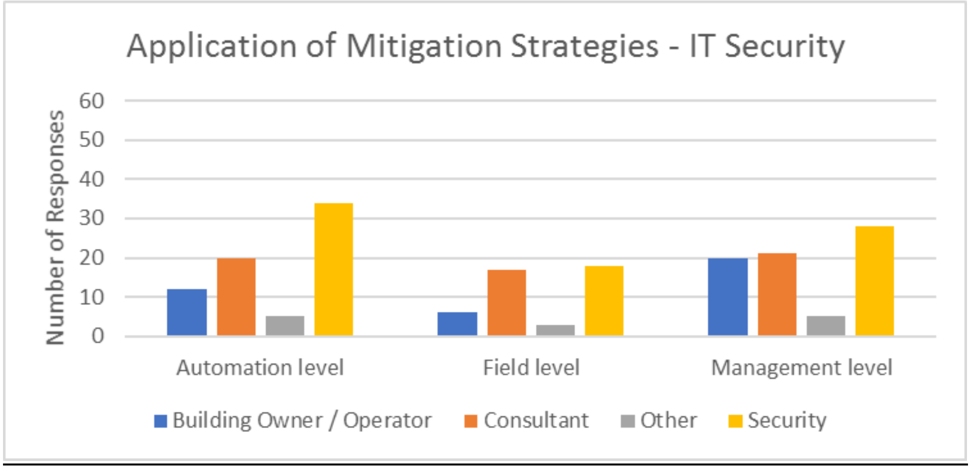


Figure F.36. Application of mitigation strategy by Job function: IT Security (n=114)

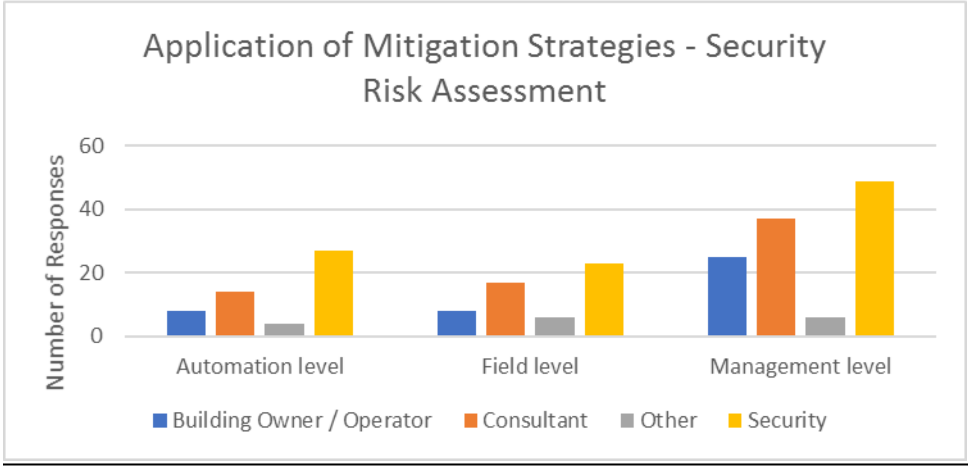


Figure F.37. Application of mitigation strategy by Job function: Security Risk Assessment (n=133)

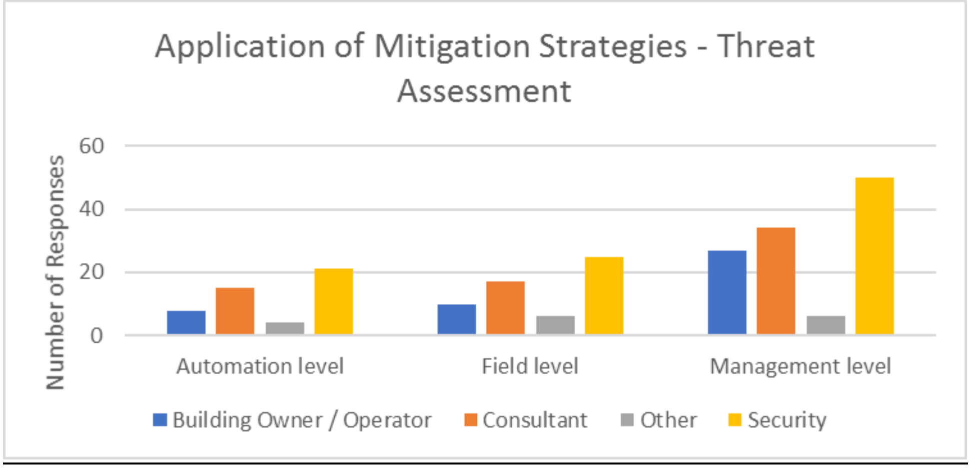


Figure F.38. Application of mitigation strategy by Job function: Threat Assessment (n=131)

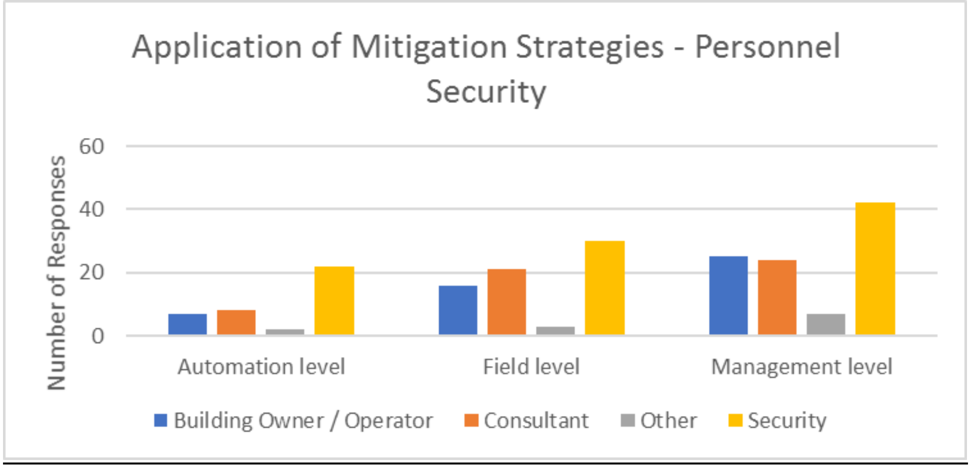


Figure F.39. Application of mitigation strategy by Job function: Personnel Security (n=128)

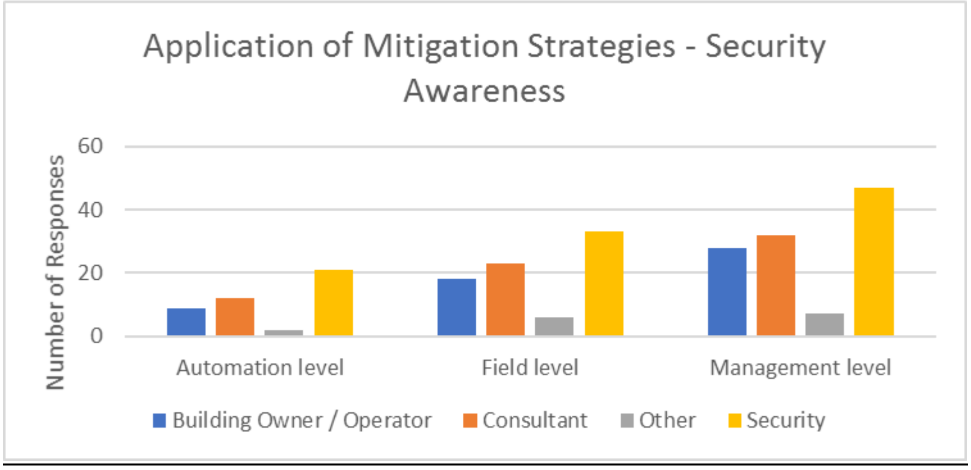


Figure F.40. Application of mitigation strategy by Job function: Security Awareness (n=133)

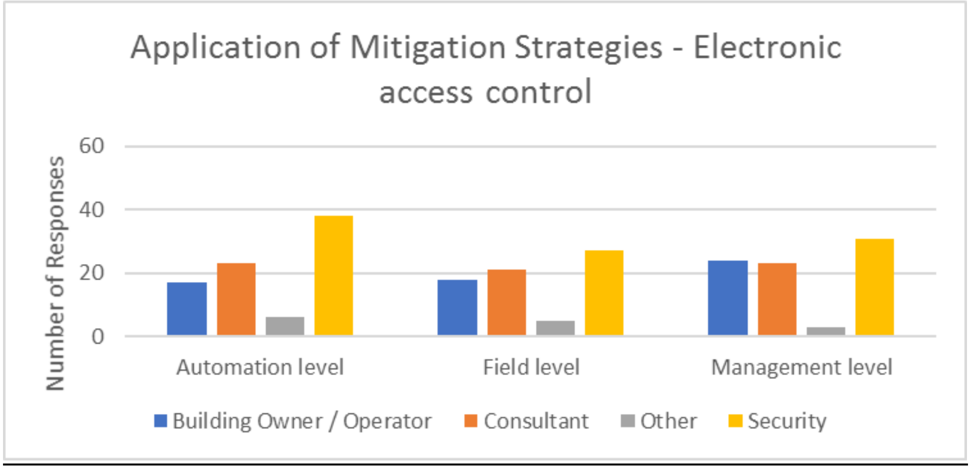


Figure F.41. Application of mitigation strategy by Job function: Electronic Access Control (n=134)

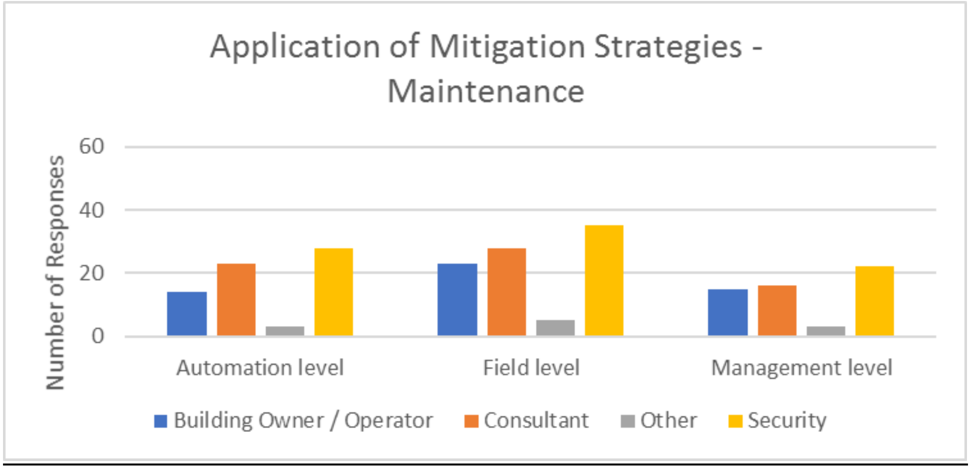


Figure F.42. Application of mitigation strategy by Job function: Maintenance (n=130)

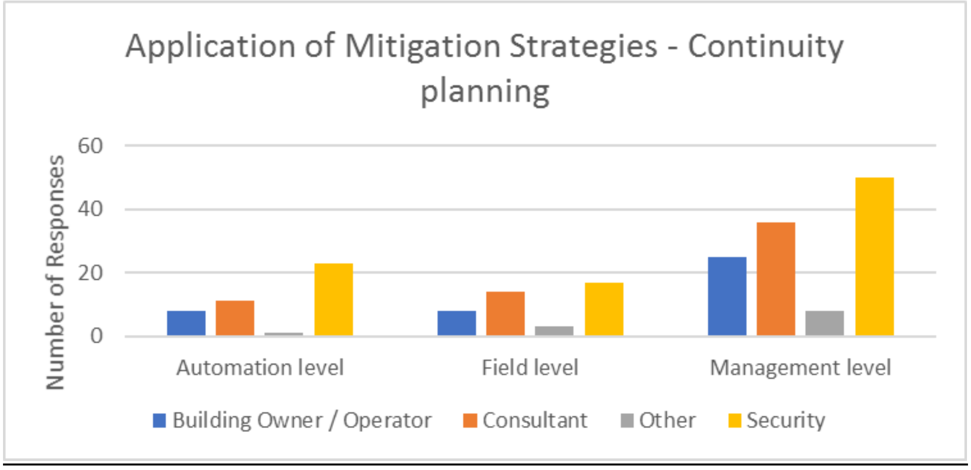


Figure F.43. Application of mitigation strategy by Job function: Continuity Planning (n=130)

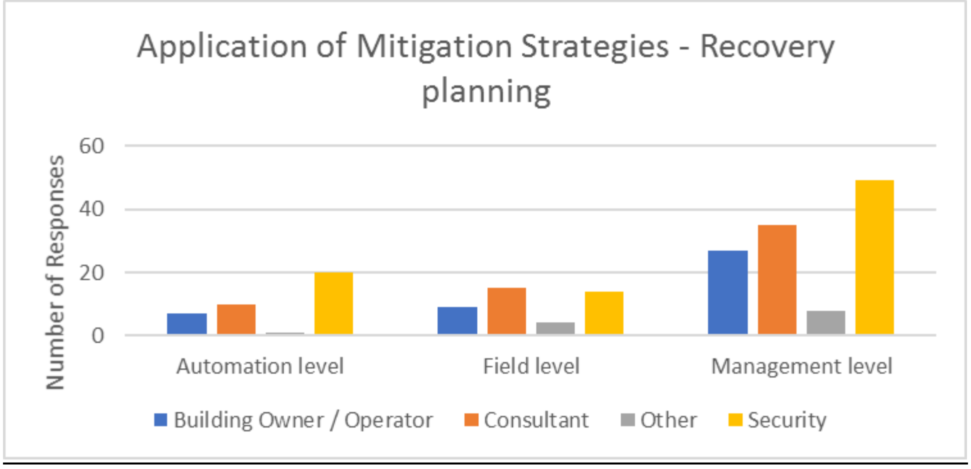


Figure F.44. Application of mitigation strategy by Job function: Recovery Planning (n=130)

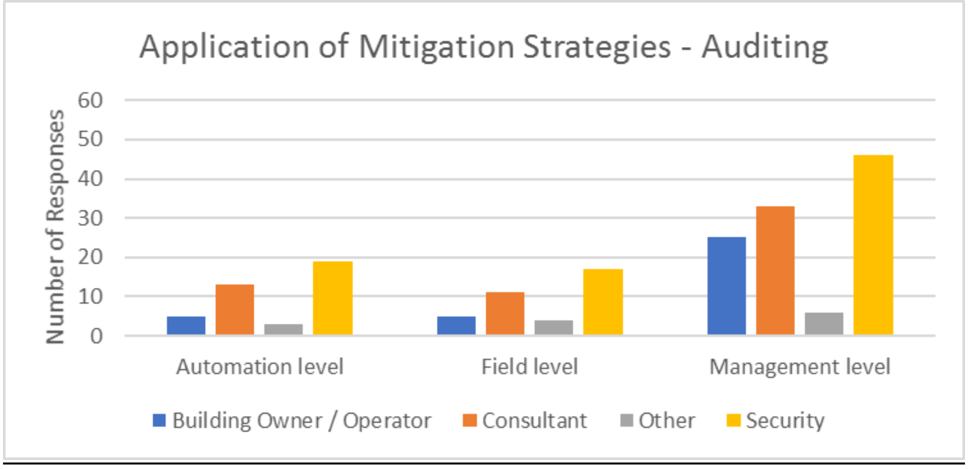


Figure F.45. Application of mitigation strategy by Job function: Auditing (n=126)

Table F.14

Other mitigation strategies applied bytext responses

Mitigation Strategies – Other (Text) (n=2)
Fire Detection
Layered security policy and procedures for personnel, data and physical protection measures

Table F.15

Stakeholders engaged with BACS by Building Owner/Operator text responses

Building Owner/Operator – Stakeholders engaged with BACS (n=14)
Asset Management, Property Management, Engineering, IT
BAS vendor; building engineering team; building ownership; intelligent riser management company;
Building ownership, maintenance staff, security staff, outside contractors
Corporate engineering, onsite management staff, vendor partners
engineering
Engineering, Property Manager, Building Owner, Vendors
IT Security, Facilities
Management and Ownership
Owner and maintenance tech
owners, engineering, tenants, IT, management
Ownership
Property management, IT, Security, Business Continuity
Property Owner Property Manager
Quality, department heads, IT
Registrars, Security, Engineering, Visitor services
Tenants, Hospital Administration (we're 100% medical)

Table F.16

Stakeholders engaged with BACSby Consultant text responses

Consultant – Stakeholders engaged with BACS (n=17)
All Employees and Management
All groups have role in keeping the systems safe and secure.
Architect, Owner, Engineer, Contractor
As a Tenant of the building, I am invited to attend no Stakeholder Group events.
Board directors, Senior management (FM, IT, Resources), Systems maintainers/operators
CIO's, CEO's and Risk Management team members
Corporate Facilities, IT, Network, IT Security, all VP level management
Facilities and End-user groups
Facilities, HR , IT
In high-rise buildings, the building management company. In buildings occupied and owned by a corporation, it depends on corporate structure. I could be dealing with Security, Facilities, upper management or all three.
Industry groups, employer groups and service providers
Management Operations Field Operators IT
Property manager, building engineer, security, risk manager,, vendor/service provider, IT
Property Managers, tenants.
Real estate group, HQ services
Security, Operations, C-Suite, HR, Risk Management
tenant (front line, IT, middle management, senior management personnel), landlord, alarm monitor co., police, fire.
Tenant, Owner, critical vendor

Table F.17

Stakeholders engaged with BACS by Security text responses

Security – Stakeholders engaged with BAS (n=26)
Securitas - Prosegur
C-level management, mainly CIO, CEO and COO. Suppliers.
Director of Engineering. Corporate IT Security. Vendor Standards.
Do not engage day to day with any BM contacts.
Don't Know
ENCS, Emergency Management, EH&S
Facilities
Facilities Management and maintenance.
Facilities managers, security personnel, ICT personnel, integrators, EAC & ESS personnel, Company Managemnet
Facilities, IT and physical security
Facilities, CIO, Control Systems Engineering, Executive
facilities, conservation, collections and security departments
Facilities, IT, physical security, risk management, auditing
Facilities, security, building users

Facilities, tenants and stakeholders.
Facilities/
facility management, maintenance, IT, security & safety, tenant commitee
Facility managers and security directors
Global Security Management, Corporate Security, IT, Facility Maintence, Senior Leadership
Infrastructure, IT, Emergency response team, Security Operations, Fire Services, Systems designer; Architect etc
None
none
Post security group, techinal security group
Real Estate, Facilities Management, IT, Physical Security Management
Security Technology Group, Information Technology Group, Facility Management Group, Supply Chain Management.
Security,. Operations,. Property Management

Table F.18

Stakeholders engaged with BACS: Other roles text responses

Other Job roles – Stakeholders engaged with BAS (n=5)
Building Management, Company Management, Finance, Building Engineer, Procurement, C Suite Management, Systems Integrator and Distributors
C level, ICT, Physical Security,
Facilities Management
Operations & Maintenance; physical security security subcontractor
Vendor

Table F.19

Further Comments

Further Comments (n=9)
For the more advanced systems that have accessibility remotely and are tied with other buildings, the "internet of Things" takes on a larger role. If the system is designed to operate outside of or behind the companies firewall is a major factor.
I am not in this field and only have cursory knowledge of the subject matter
It is very important to manage the building as holistic as possible. Investment in the building and is equipment is just 25% of the total investment, 75% is operations & maintenance through the years
Only involved in Security System design - in 30 years have never integrated with a BAS system (other than point monitoring, e.g., data center high temperature
The management team is indifferent or not knowledgeable as to automation system security.
The meaning of several questions was unclear
This is a great topic to consider as IoT comes into the horizon with end-user areas versus the traditional manufacturing and PhySec systems.
We are in the process of upgrading our BAS system and ensuring it is protected behind the intelligent riser to mitigate the potential for destructive "hacking" into the system
You get what you pay for.

Appendix G. Stage 3 Letter of Consent

INFORMATION LETTER TO PARTICIPANTS

Building Automation & Control Systems: An investigation into Vulnerabilities, Current Practice and Security Management Best Practice

Dear Participant

You are invited to participate in a research project "focus group", being conducted in partnership between *ASIS Foundation, BOMA, SIA* and *Edith Cowan University* (ECU). The research is an investigation into building automation and control systems (BACS) vulnerabilities, current practice and security management best practice.

The focus group seeks to gain an understanding of BACS and security practice, plus the suitability of developed BACS Guidelines. The focus groups will take approximately 1.5 hours during the upcoming:

63rd Annual Seminar & Exhibits, Dallas, September 26-27, 2017

The focus group will be recorded and transcribed; however, participation will be anonymous, with no personal or your organization's information collected. Only the researchers will have access to the focus groups discussions. Participates must be at least 18 years of age.

Access to collected data will be restricted to only the ECU project researchers. Data will be securely stored for a period of five years, when it will be formally destroyed.

Participation in this project is voluntary and you are free to withdraw at any time.

If you have any questions or require any further information about the project, please feel free to contact either myself or the ASIS Foundation contact.

If you have any concerns or complaints about the research project and wish to talk to an independent person, you may contact ECU's Research Ethics Officer:

Thank you

David Brooks, PhD
Principal Investigator
Edith Cowan University
Joondalup, Australia
d.brooks@ecu.edu.au
+618 6304 5788

Other Contacts

Pat Hussey
ASIS Foundation Program Manager
ASIS International
Pat.Hussey@asisonline.org
+1 703.518.1457

Research Ethics Officer
Edith Cowan University
100 Joondalup Drive, JOONDALUP WA 6027
research.ethics@ecu.edu.au
Phone: +618 6304 2170

PARTICIPANT CONSENT FORM

Building Automation & Control Systems: An investigation into Vulnerabilities, Current Practice and Security Management Best Practice

I, [name] ___________________________________, on this day [date] ___________________________, have:

- Been provided with a copy of the Information Letter, explaining the research study
- Read and understood the information provided
- Given the opportunity to ask questions and had any questions answered to my satisfaction
- Is aware that if I have additional questions, I can contact the research team
- Understands that participation in the research project will involve participation in this Focus Group, which is audible recorded and later, transcribed
- Understands that information provided will be kept confidential
- That my identity or my organization will not be disclosed without my express consent
- Understands that the information provided will only be used for the purposes of this research project
- Understands how the information is to be used
- Understands that I am free to withdraw from further participation at any time, without explanation or penalty
- That I freely agree to participate in this project

Signature: ____

Given the time and support you have provided as a participant in this focus group, would you like to be acknowledged as a supporter of the project in the final research Report? You will not be identified as a focus group participant.

If so, please sign here: _______________________________

Appendix H. Stage 3 Focus Group Questionnaire

FOCUS GROUP QUESTIONS

Building Automation & Control Systems:

Investigation into Vulnerabilities, Current Practice & Security Management Best Practice

Dear Participant

First, thank you for supporting this research project. Your time is most appreciated.

Given the nature of BACS threats and associated risks, and without specific environmental context, developing generalizable mitigation strategies is complex. The intent of the focus group is to draw on your knowledge and experience to assist us in developing more robust building automation and control systems (BACS) Guidelines, to aid both the security and facility professional.

The focus groups are being held over a two day period, with each session lasting 1.5 hours. You have been scheduled for one of these groups.

To be as efficient as possible, we have attached pre-reading materials for you. These material include:

1. BACS Guideline (draft)
2. BACS Stage 3 Focus group questionnaire (these pages)

Regards, Dave

Dave Brooks, PhD
Principal Investigator
Edith Cowan University
Joondalup, Australia
d.brooks@ecu.edu.au

FOCUS GROUP QUESTIONNAIRE

GENERAL INFORMATION

Please complete the following general questions about yourself:

What is your Job title: ________________________

Describe your primary area of work: ____

How long have you been in this or similar areas of work? ______________________________

List your qualifications: ____

Relevant Certifications: ____

A brief description of your previous work, roles or functions:

____
____
____
____
____

The following questions are for "guided" discussion during the Focus Group

FOCUS GROUP QUESTIONS

During our online survey, we found only 8% of respondents had BACS responsibilities. Within this group, the majority of those responsible for BACS were facility professionals. Is this your personal experience in regard to BACS?

The survey indicated that security professionals have limited or no BACS responsibility. Is this your experience?

Our survey results suggested that 75% of security and facility professionals felt they had an awareness of the different BACS architectural levels; however, on analysis the majority displayed limited understanding in their vulnerabilities? Why do you feel that these professionals believed that they understood BACS architecture, yet perhaps do not?

Results identified that Security Integrators (including cyber) displayed a high level of understanding of BACS criticalities. Is this your experience as well and if so, why?

The survey results indicated a significant divergence between security and facility professionals on what degree of security systems integrate into BACS. Security professional suggested a higher proportion of security systems integration, compared to facility professionals. Why do you think there is such divergence?

In your view, what does integration mean in the context of BACS and security systems from a security and/or facility professional view? Do these views differ?

When we surveyed 23 BACS vulnerabilities, we found a neutral response i.e., there was little difference between the criticality of the 23 vulnerabilities. Why do you believe that most security and facility professionals rated the criticality of BACS vulnerabilities relatively equally?

BACS GUIDELINE REVIEW QUESTIONS

In general, do the Guidelines provide enough (in plain English) information to give you an appropriate understanding and awareness of:

1. BACS
2. BACS architecture
3. BACS vulnerabilities and
4. BACS mitigation strategies

Are the Guideline instructions clear and easy to follow?

Acknowledging that all facilities are not equal in risk, do you support the level-based approach developed?

Are the BACS case studies (pages 2 to 3) useful and do they support your understanding?

Do the criticality categories (see Appendix A) make sense and could you apply these?

Do the BACS mitigation questions (see Appendix B) make sense and could you apply these?

Would you like to see any modifications (additions or removals) to the Guidelines?

Any final comments?

CONCLUDE

Please provide a summary of any other aspects, issues or factors you feel have not been discussed during this focus group. In addition, note any items that you feel are important to this project.

____

____

____

____

____

Appendix I. BACS Guideline

Building Automation & Control Systems:

A Security and Facility Professionals Guide To Protect Their Organization

GUIDELINE

David J Brooks, Michael Coole & Paul Haskell-Dowland

Insert ASIS International; BOMA; SIA logos

SCOPE

The Guideline provides advice to help ensure that a facility's Building Automation and Control Systems (BACS) are, where necessary, protected from risks that may impact the organization. The intent of the Guideline is to provide a tool to aid decision-making, whereby security or facility professionals can address relevant questions to gain a level of assurance in protecting their organization.

SUMMARY OF THE GUIDELINE

The Guideline provides both the security and facility professional with the necessary information and framework to protect their organization against risks associated with Building Automation and Control System (BACS) vulnerabilities. The Guideline aims to support such decision-making, with direction to standards, guidelines and other relevant resources.

BACS are prone to many generic vulnerabilities across all parts of their architecture. BACS comprises of three levels of technical architecture with the majority of BACS risks at the automation level (critical to high), followed by the management level (moderate) and due to limited and isolated functionality, the field device level (low).

The Guideline provides a method to assist the decision-maker in assigning a risk-based criticality or impact to their facility and therefore, protect against vulnerabilities associated with BACS. Risk is informed by the organization, its functional criticalities, environmental context and assessed threats. Once the criticality level is defined, from low to critical, directed security questions assist the decision-maker in developing mitigation strategies. Organizational mitigation strategies range from diagnosing the security problem to inferring the most appropriate solution for the application of treatment.

HOW TO USE THE BACS MITIGATION GUIDELINE

The Guideline's methodology identifies and mitigates BACS risks through a facility level questionnaire approach. Dependent on the criticality of the facility, BACS security questions (Appendix B) should be answered. Questions are divided into criticality levels, from level 1 (low) to level 5 (critical).

To use the BACS Guideline:

1. Identify your organizational criticality level, using Appendix A;
2. Commencing from Level 1, hierarchically respond to the BACS security questions (see Appendix B) for your identified criticality level. For example, if you rate your facility as a Level 3 (high), answer the questions from Levels 1 through to 3;
3. Annotate compliance with each question, with supporting comments as required; and
4. Where compliance is not achieved, define a responsible person and date of action.

PURPOSE

Building Automation and Control Systems (BACS) are growing at approximately 15 to 34 percent each year, due to the demand for energy-efficiency, reduced maintenance, and the greater control and operability. By 2022, the BACS industry will be worth an estimated $104 billion. Such growth highlights the current and expected impact that BACS will have in most future built environments, which if security is not considered will expose organizations to harm.

The growth of the BACS market is driven by the medium to long term requirement to save resources with improved efficiencies and environmental targets imposed by governments. With global rises in energy costs, pollution sanctions and green government incentives, BACS initiatives are at the forefront of the majority of future facility projects.

BACS are integrating a greater number of building technologies and functions of business. Technology is converging and this, amongst other aspects, drives an increased integration of other business and building systems into BACS. Integration includes security systems, such as intruder detection, access control and CCTV. These aspects will affect the security professional in their ability to effectively protect against the increase in BACS vulnerabilities.

WHAT ARE BUILDING AUTOMATION & CONTROL SYSTEM?

A Building Automation and Control System (BACS) is an automated building system that converges and integrates the many building technologies and information flow processes to a central decision point.

BACS are also known by many other terms, such as a Building Automation System (BAS), Facilities Management System (FMS), Energy Management System (EMS), Building Management System (BMS), Intelligent Building (IB) and today, Smart Buildings. However, the core principles of BACS remain the same, regardless of its name.

The scale of BACS vary from an automated home heating system to a high rise Intelligent Building, which centrally automates and controls all functions including HVAC, lighting, elevators and life safety systems, along with maintenance, administrative and business functions. Today, security is also becoming embedded within the function and business of BACS.

With the advent of the Internet of Things (IoT), BACS will continue to expand into more diverse and complex areas of everyday life. Connectivity through the IoT means, in simple terms, that anything will be linked and incorporated.

BACS Case Studies

BACS are modular and formed to meet an intended purpose of control and monitoring the facility. Therefore, there are many examples of BACS:

A small BACS:

> The building has a security access card system. The employee of an approved access card swipes an external card reader to gain entry to their building. Upon swiping, the entry door automatically opens to allow the employee access and entry lights are automatically turned-on. The door automatically closes and later, lights turn-off as the employee moves to their work space through the building entry.

A large BACS:

> The Human Resource (HR) and Payroll system transfers personnel data to the security access card system, authorizing access to certain work spaces in the building. This approach facilitates single data entry for all employees of the organization. As the employee swipes their access card, the door opens based on their authorized HR work space. Information gathered from that card swipe is linked back to Payroll to monitor time and attendance. Lighting and heating/cooling systems are turned on as the employee moves through the facility to reach their work space. BACS monitors the external and internal environment, to ensure that the internal environment is comfortable whilst minimizing utility usage.

A BACS incorporated into the Internet of Things:

> The lighting and heating/cooling systems all operate as above; however, the security access credential is the employee's personal Smartphone. As the employee drives to the vicinity of their building, they are directed by their Smartphone into alternative parking at a neighboring building. The building has wireless connected cashless vending machines. The employee access credential is used at the cashless vending machines and parking fees are charged back through Payroll for automate deduction.

Whilst the efficiencies and potential savings for organizations embracing these systems are manifold, the vulnerabilities created through the use of these systems are potentially brand damaging and life threatening. The ability to "enter" these systems at their physical or logical weak points results in not only access to BACS itself, but also potentially access into the entire organizational enterprise system. Such access exposes not only the physical building, but also company data and information.

BUILDING AUTOMATION & CONTROL SYSTEM THREATS

Consequences of realized threats can be divided into three categories: loss, denial and manipulation (Figure 1). These consequences pose a risk to the confidentiality, integrity and availability (CIA) for organizations, with possible cascading affects.

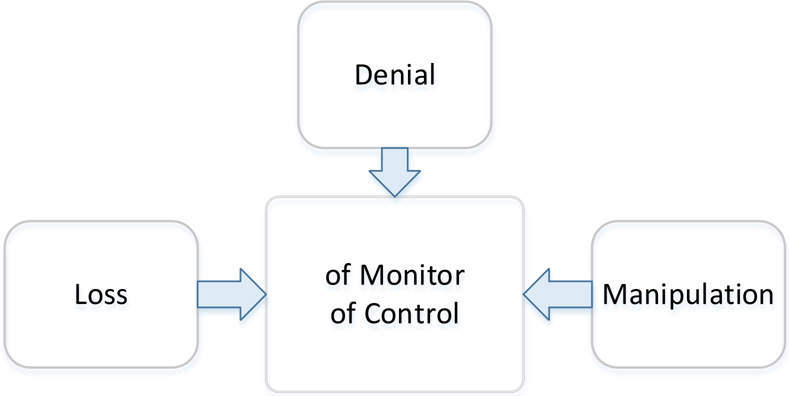


Figure 1 Consequences of Realized Threats to BACS

BACS risks are contextual, aligned with the facility's threat exposure and their functional criticality; nevertheless, as with all security vulnerabilities there are generic mitigation strategies that can be taken to protect these systems.

BUILDING AUTOMATION & CONTROL SYSTEM FUNDAMENTALS

Building Automation and Control Systems (BACS) are modular in nature, formed from the integration of a number of devices, equipment and common communication platform networks. BACS architecture is based on three levels: Management, Automation and Field devices (Figure 2).

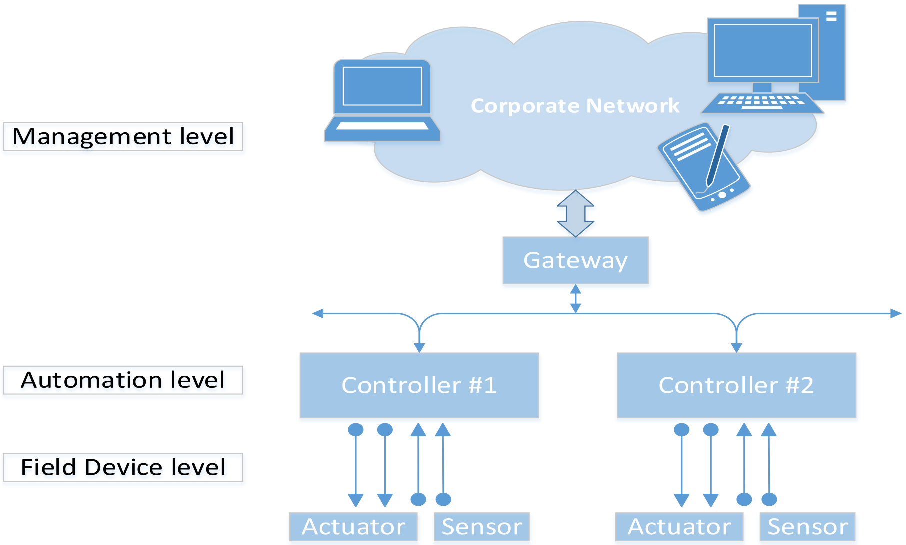


Figure 2 BACS Architecture

Management Level

The management level contains the human interface, connected via the enterprise software and communication network i.e., the Information Technology network. Management level equipment includes workstations, network switches and servers. BACS manufacturers provide software packages allowing designers and users to select what suits their facility. The management level software packages range from simple information processing systems that control a single room to complex whole of facility services that monitor and control plant and equipment, and providing functions such as energy management, lighting, maintenance, etc.

Automation Level

The automation level provides the various primary control devices, connected via networked controllers and operating via open source communication protocols. They provide the interface between the BACS physical field devices and the management level human interface. Examples of automation equipment includes controllers and routers.

Field Device Level

The field device level provides physical devices, such as sensor or activators connected to specific plant and equipment. These devices connect the BACS to its physical environment. Examples of field level devices include light switches, PIR detectors, fans, temperature sensors, valves, etc.

Communications Networks

For BACS to function, there is a requirement for connectivity and common language communication. Connectivity is achieved via various communication networks that integrate the many discrete devices. Communication is achieved through standardized logic code. Such a requirement has led to a number of building automation network and communication protocols being established. Currently, no particular protocol or standard exists for all building automation; however, some common protocols include BACnet, LonWorks, Internet Protocol and Hypertext Transfer Protocol, to name a few.

Connectivity forms the platform and resulting functionality of BACS, hence is a significant element. The technical architecture facilitates connectivity, which in turn supports communication and decision-making, and automated control functions. The many BACS vulnerabilities lie in this architectural level of connectivity and common communication protocols. Consequently, security and facility professionals need to understand this architecture to understand BACS vulnerabilities and mitigation strategies.

BUILDING AUTOMATION & CONTROL SYSTEMS VULNERABILITIES

BACS generic vulnerabilities have been broken down into the three architectural levels of automation, management and field device levels. A BACS is prone to attack (Figure 3) at all levels, although the automation level could be considered the most vulnerable. It should be noted that vulnerabilities are situational, better understood through understanding the facility's threats, criticalities and context.

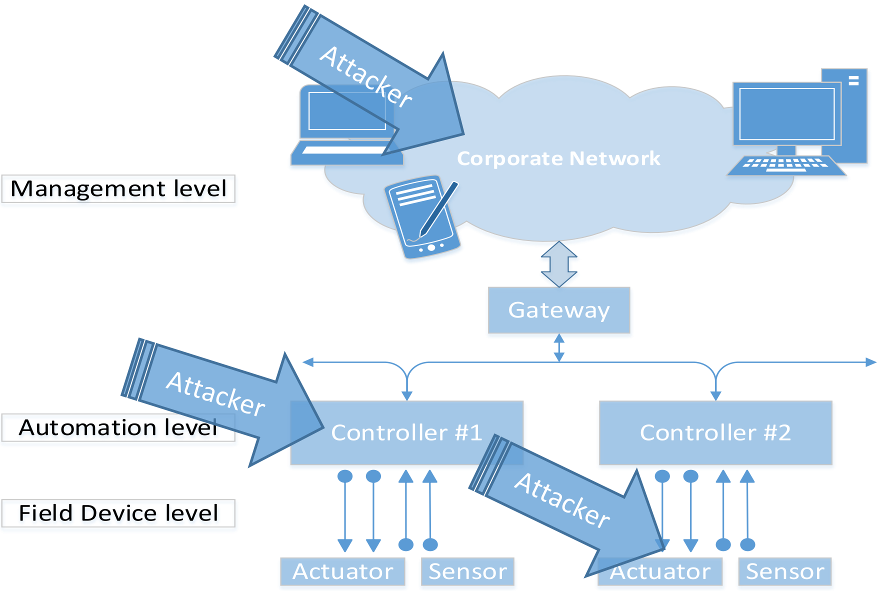


Figure 3 BACS Attack Points

BACS Vulnerabilities Case Studies

Case Study 1: Automation level vulnerabilities

A contract maintenance worker is granted access to all plant rooms and electrical risers throughout the facility. The plant rooms contain BACS automation network cabling and Controllers, which control and monitor the local HVAC, lighting, access control and security detectors for that floor. The maintenance worker wants to gain illegal access to the facility after hours and knows that the BACS monitors the security detectors. The Controllers are mounted on the wall in an open enclosure, which allows the worker to plug their laptop into the Controller's service port rather than take the time to strip the network cable to connect a wiretap. Once plugged into the Controller, they find that there is no security restrictions on viewing the automation level program and network traffic. They reprogram the Controller inputs, being the security detectors, to automatically turn off at night. In addition, they set the outputs, being the door locks, to open. They arrive that night, with clear and open access into and out of the facility.

Case Study 2: Management level vulnerabilities

An organized crime group targets a retail company, with the intent to steal credit card information. They send an email with an embedded virus, to an account at the BACS integrator. The integrator maintains BACS for a number of different organizations, including the targeted retail company. The BACS maintainer has remote access to many of their client's BACS systems to provide fast and efficient 24/7 technical support. On opening the email, a virus configures third party access to the BACS management software, providing access to the target organization's information technology network. The crime group gains unauthorized access to the credit card details, which are then on-sold.

Case Study 3: Device level vulnerabilities

A disgruntled dismissed employee want to get back at their employer by causing the business some harm but without being identified. The business operates in a facility that has a public foyer, shared by other organizations. The dismissed employee has open access to the foyer that has a HVAC temperature sensor, with a cover fixed by a simple screw. Standing in front of the sensor, the dismissed employee removes the cover and places a resistor across its output terminals. This change results is the BACS Controllers sensing that the foyer is far warmer than the actual room temperature, which commands the HVAC to cool the foyer. This excessive cooling makes the foyer uncomfortable to use and causes a disruption of service as well as raising operational costs. It takes the technician a number of hours to track down the cause of the misreading sensor at a cost and inconvenience to the organization.

Table 4 provides oversight to where the more significant BACS risks lie. As indicated, the most significant critical and high risks (red and orange) lie within the automation level, followed by moderate risks (yellow) at the management level and finally, low (green) risks at the field device level.

Table 4 BACS Generic risks

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

APPENDIX A: ORGANIZATIONAL CRITICALITY OR IMPACT CATEGORIES

Level	Rank	Government Operations	Business Operations	Board / Executive	Financial[1]	Reputation	Personnel / Safety	Regulatory	Information	Occupancy
Critical	5	Expected to cause exceptional grave damage to national security	Impact across all critical business functions, vital to business operations, loss of function will have extreme effect on the ability to maintain operations	Immediate Board intervention required	Financial loss of >10%	Significant and long term loss of trust across all parts of the business	Multiple deaths and/or permanent total disability of >3 personnel	Loss of statutory accreditation to operate for an extended period	Significant commercially sensitive information exposed	Unable to occupy the whole facility for an extended period
Extreme	4	Expected to seriously damage national security	Impact on multiple critical business functions, loss of function will effect the ability to maintain parts of operations	Immediate senior executive intervention required	Financial loss of >5%	Significant but short term loss of trust across all parts of the business	Permanent partial disability, injuries or illness that result in hospitalization of >3 personnel	Loss of statutory accreditation to operate for a short period	Significant commercial information exposed	Unable to occupy the whole facility for a short period
High	3	Expected to damage national security	Substantial degradation of operations Impact on multiple business functions	Substantial executive intervention required	Financial loss of >3%	Measurable reputational loss to multiple parts of the business	Partial disability, injuries or occupational illness that result in hospitalization of > 1 personnel	Record of non-compliance against statutory accreditation, with some operational impact	Restricted commercial information exposed	Unable to occupy major parts of the facility for an extended period
Moderate	2	Expected to damage government agency operations, commercial entities or members of the public	Moderate degradation of parts of operations, loss of function will have limited effect on ability to maintain operations	Executive intervention required	Financial loss of <2%	Some measurable reputational loss to some parts of the business	Injury or occupational illness resulting in 1 or more lost work day(s)	Limited effect on statutory accreditation, with no operational impact	Restricted operational information exposed	Some effect on parts of the facility to occupy
Low	1	Expected to harm government agency operations, commercial entities or members of the public	No measurable operational impact	Local management intervention required	Financial loss of <1%	No measurable reputational loss	Injury or occupational illness not resulting in a lost work day	No effect on statutory accreditation or operations	Limited operational information exposed	No effect on occupancy
Unknown		Expected harm is unknown	Operational impact is unknown		Impact unknown	Reputational loss unknown	Safety of personnel impact unknown	Regulatory impact unknown	Information consequence	Occupancy effect unknown

Note 1: Assessor to provide suitable framework of financial values to suit situation.

APPENDIX B: BACS SECURITY QUESTIONNAIRE

LEVEL 1 (LOW)	Complies?	Comments
MANAGEMENT		
Do you have a written and endorsed Security Policy?		
Do you have written and endorsed security procedures?		
Is BACS formally assigned to the facility manager's portfolio and if so, who?		
Do you have a committee or working group of relevant BACS stakeholders that meet regularly?		
SECURITY RISK MANAGEMENT		
Does your facility have a designated criticality or business impact rating?		
Are your BACS risks captured in your Security Risk Management Risk Register?		
PERSONNEL SECURITY		
Do you have personnel security policies and procedures in place?		
Are your personnel security policies and procedures current?		
Do your personnel security practices include pre-employment screening?		
Do you have an auditable procedure to authorize access to the BACS?		
PHYSICAL SECURITY		
Do you have policies and procedures for assigning physical access rights?		
Do your physical security strategies protect the facility's BACS infrastructure?		
Is physical access to all BACS infrastructure controlled?		
Are the facility's BACS Controllers, routers and network switches physically protected?		
Are BACS Enclosures in a secure and protected area?		
Are BACS Enclosures locked?		
Do you have a procedure for ensuring (mechanical) keys related to BACS are controlled at all times?		
CYBERSECURITY		
Do you have policies and procedures to authorize and assign BACS logical access privileges?		
Is logical access to your BACS restricted and authorized based on role?		
Is there a register of who has logical access to your BACS?		
Do you have an auditable access log for all individual BACS users and/or maintainers?		
Do you control your BACS remote and/or external logical access?		

Does your BACS logical access have rules of password complexity?		
Does your BACS have session time out lock?		
Does your BACS have the most current software patches?		
Are your BACS master access codes, PINs or IDs held in a secure location?		
Have the factory or default password or other access means been deactivated?		
Do you know who is responsible for updating your BACS logical and configuration back-ups?		
Is your BACS logical program and configuration details held in a secure location to enable recovery and reconstitution?		
INCIDENT RESPONSE		
Is your BACS able to maintain capably during a routine or non-routine incident to support an emergency response?		
Are your routine or non-routine incident response plans tested through desk-top exercises' to a defined schedule?		
CONTINUITY PLANNING		
Does the BACS feature in your continuity plans?		
Are you able to take manual control of your facility sub-systems from BACS, such as heating/cooling, lighting, etc., to maintain operations?		
MAINTENANCE		
Does your BACS have a scheduled maintenance plan?		
Is your BACS maintained by a known BACS Maintainer?		
Do you have policies and procedures that authorize connection to BACS communication network cable or its devices, including Controllers, routers, network switches, etc?		
Is your BACS part of the facility's asset tracking system?		

LEVEL 2 (MODERATE)	Complies?	Comments
MANAGEMENT		
Do you have a written and endorsed Security Guideline or Basis of Design document, which define security zones?		
Is physical access to security zones based on role and personnel screening?		
Do you have a written and endorsed facility Security Policy?		
Are BACS workstations positioned according to security zoning policies?		
PERSONNEL SECURITY		
Do your personnel security policies and procedures include signed acceptable expectations of conduct, terms and conditions of employment and entry, legal rights and responsibilities?		
Do your personnel security policies cover access to BACS?		
Do you have policies and procedures for authorizing access to individual BACS equipment or devices?		

Are BACS access authorizations audited and anomalies investigated?		
Are new personnel inducted with security awareness training?		
PROCEDURAL		
Are access authorization procedures followed before a person, either employee or third-party contractor, is given access to BACS network infrastructure?		
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?		
Do you have policies and procedures to control the use of mobile storage devices?		
Do you have policies and procedures to control the use of "bring your own" device?		
PHYSICAL SECURITY		
Are BACS Enclosures resistant to unauthorized access?		
Are the BACS Field level devices connected using supervised (monitored) cables between the device and its Controller?		
CYBERSECURITY		
Do you have "as built" BACS architecture schematics or drawings, including IP addresses, hardware, locations, etc?		
Is your BACS network integrated with external devices, such as cloud computing services?		
Do you have a database of logical access privileges for BACS users and maintainers?		
Can you identify and authenticate persons through events logs, etc., who have logical access to your BACS?		
Do you have an alert system for unauthorized logical access attempts?		
Do you have an alert system for unauthorized logical traffic?		
Do you have an appropriate level of protection for your BACS enabled wireless connectivity?		
Are there user and BACS Maintainer restrictions for BACS wireless connectivity?		
Is your BACS logical program and configuration details held in a secure off-site location?		
INCIDENT RESPONSE		
Are your incident response plans tested through desk-top exercises' to a defined schedule?		
CONTINUITY PLANNING		
Are your continuity plans tested through desk-top exercises' to a defined schedule?		
MAINTENANCE		

Has your BACS Maintainer demonstrated an understanding and compliance to maintaining BACS security?		
Are all BACS hardware and software changes authorized and documented?		
Do you have a BACS legacy plan?		

LEVEL 3 (HIGH)	Complies?	Comments
MANAGEMENT		
Is BACS specifically included in your Security Policy		
Do you undertake and propagate environmental scanning to stay informed on best practice to protect BACS?		
Do you maintain liaison with external agencies, departments, industry groups and other organizations for BACS security?		
Do you undertake periodic audits to ensure that all security strategies are applied and operating as intended?		
Are BACS security audits undertaken?		
How often do you meet with BACS stakeholders, such as facilities, Information Technology, cybersecurity and BACS Maintenance, in regard to the security of BACS?		
Are your BACS security meetings documented?		
Are proposed and/or changes to BACS reviewed by relevant stakeholders?		
SECURITY RISK MANAGEMENT		
Do you undertake vulnerability assessments of your BACS?		
Are BACS risks updated in the risk register?		
PERSONNEL SECURITY		
Are personnel who will have direct access to BACS Management level workstations, terminals and networks screened for access?		
Do you undertake pre-employment screening (including third parties and contractors) of your BACS Maintainer personnel?		
Are regular audits of BACS Maintainer's security status undertaken?		
Do you have formal review policies and procedures in place for when a person moves roles?		
Is the BACS part of the security awareness training process documented?		
Are regular audits of BACS Maintainer access undertaken, for example ensuring that access credentials align to a person, etc?		
PROCEDURAL		
Do you have formal procedures for security breaches involving suspected unauthorized BACS access?		
Are exit interviews undertaken for staff using or maintaining your BACS?		
PHYSICAL SECURITY		
Are the BACS physical vulnerabilities documented?		
Are the BACS Automation level communication network cables protected?		

Do the BACS Enclosures have door and rear-mount tamper detection?		
Are your BACS Field level devices connected using a three-state supervised circuit (monitored) cable between the device and its Controller?		
Are your BACS intruder and/or fault alarms monitored on a real time basis?		
Are BACS logical access points located in a secure room or zone?		
CYBERSECURITY		
Is your BACS network logically separated from your enterprise network?		
Do you control remote wireless BACS connectivity through restricted and managed access points?		
Do you have appropriate protection over embedded BACS wireless connectivity?		
Does your BACS logical access have multi-factor Secure ID Key?		
Does your BACS logical access passwords have unsuccessful login attempts, automatic lock out and access attempt rules?		
Are your BACS device configurations audited to a defined schedule?		
How often is your BACS unauthorized logical access alert detection system updated?		
INCIDENT RESPONSE		
During incident response training, is the facility's BACS included in response strategies?		
Are your incident response plans tested through physical exercises to a defined schedule?		
In a routine or non-routine incident when site power is lost, does your BACS maintain capability to support the emergency response?		
Following a routine or non-routine incident, do you undertake a post incident investigation?		
CONTINUITY PLANNING		
Have you tested you BACS logical program and configuration to exercise recovery and reconstitution?		
MAINTENANCE		
Does your BACS have a predefined response and recovery period to a defined schedule?		
Does your BACS have an auditable log of all hardware and software changes and alterations?		
Does your BACS Maintainer securely store and control authorized and accountable access of your BACS knowledge, for example documentation, configurations, etc?		

LEVEL 4 (EXTREME)	Complies?	Comments
MANAGEMENT		
Does your Security Guideline or Basis of Design document explicitly include BACS and its sub-systems?		

Do you have security zoning for BACS Automation and Management levels?		
Are mobile recording or storage devices subject to restricted access into defined security zones or areas?		
SECURITY RISK MANAGEMENT		
Do you have a security context (threat) statement for the facility?		
Does your security risk assessments specifically capture BACS risks?		
PERSONNEL SECURITY		
Do you categorize and assign a risk to all positions that use and/or have access to your facility's BACS?		
Are your BACS Maintainer (including third parties and contractors) managed as an internal employee?		
Do you have a procedure to positively identify and log BACS Maintainer prior and during BACS access?		
For BACS users and maintainers, is ongoing suitability for employment undertaken?		
Is the BACS security awareness training package assessed and results documented?		
PROCEDURAL		
Do you have escort policies and staff for your BACS Maintainer?		
PHYSICAL SECURITY		
Is physical access to all BACS hardware and software strictly controlled?		
Do the BACS Enclosures have security tamper seals to detect actual or attempted manipulation?		
Are the BACS Controllers, routers and network switches protected by a volumetric security detector?		
Do the BACS (mechanical) access keys remain onsite and are not removed from site at any time?		
Are your BACS Field level devices connected using a four-state supervised circuit (monitored) cable between the device and its Controller?		
Does your BACS supervised (monitored) cable detect both fault and tamper when unarmed?		
CYBERSECURITY		
Do you monitor the BACS logical access from the enterprise network?		
Is logical access authorization to your BACS gained through positive identification and authentication?		
Is BACS information flow between other connected systems or networks documented, controlled and authorized?		
Do you enforce the "least privilege" for BACS users and maintainers?		
Do you have policies and procedures to restrict the use of "bring your own" device?		
Are your BACS logical program and configuration details regularly audited by authorized persons?		
Do you undertake BACS penetration (PEN) testing on a scheduled basis?		
INCIDENT RESPONSE		

Following a routine or non-routine incident, do you undertake a post incident investigation?		
Do you have a continuity plans for the compromise (fire or similar) of workstations or other central control points used by BACS during an incident response?		
Is your BACS connected to an uninterruptible power supply system to maintain critical operational functions?		
CONTINUITY PLANNING		
Are your continuity plans tested through physical exercises to a defined schedule?		
Do you have remote BACS control room capability?		

LEVEL 5 (CRITICAL)	Complies?	Comments
SECURITY RISK MANAGEMENT		
Do you undertake a BACS specific threat assessments?		
PROCEDURAL		
How often are BACS equipment or device security tamper seals audited?		
PHYSICAL SECURITY		
Does your physical protection of BACS equipment or devices provide evidence of attempted or actual unauthorized access?		
Are clear conduits used for all BACS Automation level connection cables and components?		
Are the BACS Controllers, routers and network switches protected by a two over-lapping volumetric security detectors?		
Are your BACS Field level devices connected using a two-way polled 56 bit DES key encryption supervised (monitored) cables between the device and its Controller?		
Do you carry out technical surveillance counter measure evaluations on your BACS on a regular, but random schedule?		
CYBERSECURITY		
Do your scan for unauthorized wireless BACS connectivity to a defined schedule?		
Are all wireless connectivity devices disabled?		
MAINTENANCE		
Are your BACS Maintainer escorted at all times whilst on-site?		
Is your BACS equipment, devices or software verified prior to installation and/or replacement?		