Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

TC 11 Briefing Papers

Security of Building Automation and Control Systems: Survey and future research directions

Vitor Graveto[a], *Tiago Cruz*[a,*], *Paulo Simões*[a]

University of Coimbra, CISUC, DEI, Departamento de Eng. Informatica Polo II da Universidade de Coimbra, 3030-290 Coimbra, Portugal

ARTICLE INFO

Article history:
Received 5 April 2021
Revised 20 September 2021
Accepted 23 October 2021
Available online 29 October 2021

Keywords:
Home automation
building automation and control systems
BACS
smart building
security
safety
privacy
KNX

ABSTRACT

Building Automation and Control Systems (BACS) designate the mechanisms that are used to automate buildings' operations such as climate control, lightning and access control. As such, traditional BACS encompass extensively automated buildings managed in an integrated manner, with the support of Supervisory Control and Data Acquisition (SCADA) systems and specialized industry standards such as BACnet and KNX. More recently, the increasing adoption of IP-connected, *IoT-like* devices for automating single tasks led to a substantial increase in the number of automated building functions (especially for the smart home domain), although rarely with extensive or integrated automation levels. The interconnection with the building local area network (LAN) and even the Internet, comes with the cost of a wider exposition to attacks, that can either begin inside of the building or be initiated from anywhere outside of it.

In contrast with other domains that recently received substantial attention (e.g. industrial control and automation systems), the security of BACS has been addressed in a somehow more superficial and less structured manner. Nevertheless, recent security incidents, combined with the fact that these systems are becoming more interconnected with the building networks and the Internet, are raising security concerns.

This paper provides a systematic survey of recent research and industry developments related with the security and safety of building automation and control systems. It also presents an overview of the existing threats and known attacks against BACS, as well as open issues and future research directions.

1. Introduction

Technological evolution, as well as the search for increasing energy efficiency and occupancy comfort, have pushed for the introduction of building automation and control systems (BACS). Early classic BACS, introduced in the 1970s, were designed to be autonomous and isolated by nature. Their security was supposedly based on such isolation and on the use of proprietary technologies, both in the communication channels and in the operation of the micro controllers involved in related control processes.

Meanwhile, the BACS community has joined efforts in standardizing and evolving related technologies. These ef-

* Corresponding author.
E-mail address: tjcruz@dei.uc.pt (T. Cruz).
https://doi.org/10.1016/j.cose.2021.102527
0167-4048/

forts eventually led to the creation of protocols such as BACNet (2020), in the early 1980s or EIB (European Installation Bus) Goossens (1998) in the late 1980s. EIB, which was developed by the European Installation Bus Association EIBA (2020), later became the basis for the KNX specification, maintained and developed under the scope of the KNX Association (2020), which was established in 1990s (with EIBA being one of its founders). In parallel, general SCADA protocols such as Modbus (MODICON, 1996) were also used to control heating, ventilation and air conditioning (HVAC) systems.

Since the 1990s, personal computers and the Internet evolved rapidly, becoming widely accessible. Information technologies have developed and remote management has become a reality. Ethernet and IP communications became widespread and, due to practical and economical reasons, they were gradually adopted in BACS environments, encapsulating the legacy protocols over Ethernet and/or IP. The interconnection between control and IT networks became a reality, enabling reduced costs and added convenience.

More recently, a noteworthy evolution of BACS is the increasing adoption of wireless communications (using both BACS-specific solutions such as wireless KNX and general purpose technologies such as ZigBee Connectivity Standards Alliance (2021)), for convenience and cost reduction. In parallel, we have witnessed the increased adoption of consumer-grade commercial off-the-shelf (COST) IoT devices for functions such as energy measurement, lighting, remotely controlled power outlets and blind control. While these IoT devices are often used in a less structured and integrated manner (when compared with classic traditional BACS), they have significantly lowered the entry barriers for the consumer market. More recently, cloud-based smart home solutions such as digital voice assistants (e.g. Amazon's Alexa (Amazon, 2014) and Google Home Assistant (Google, 2016)) have brought some sort integration to the consumer-focused IoT landscape, although still far from the sophistication of the best professional-grade BACS solutions. Nevertheless, as these solutions are sometimes viewed as building automation systems, this paper will address them as part of the BACS landscape, though with less detail.

A common factor among all building automation solutions available nowadays is the lack of satisfactory security mechanisms. On the side of conventional BACS, this has mostly to do with the reliance on isolation and the lack of widespread knowledge about related protocols and technologies. Despite the recent introduction of security-oriented features such as encrypted communications, it is still relatively easy to maliciously interfere with the communications channels and bypass existing encryption and authentication mechanisms. Additionally, BACS sensors and actuators are prone to physical tampering, and the remote management features are often outdated and vulnerable to more sophisticated attacks. Moreover, there is also a general lack of security monitoring and management tools for BACS.

Regarding consumer-grade IoT equipment, there is also a considerable number of known issues and vulnerabilities, which have been at the source of recent security incidents (such as the Mirai botnet (Peterson, 2019)). Moreover, the increasingly narrow frontier between building automation and personal user space introduced by these IoT-based scenarios (e.g. always-on microphones for voice assistants; widespread adoption of video-cameras inside the home) also raises substantial privacy concerns.

These security concerns are not exclusive to the BACS domain. Looking at areas with some similarities, such as Industrial and Automation Control Systems (IACS), the existence of legacy and/or highly specialized systems and their interconnection with the IT networks substantially increased the exposure to various threats. However, while for IACS such security issues have been the subject of intensive study, research and industry developments, the same does not apply to BACS. The security community has been paying much less attention to BACS ecosystems, which is often considered as a niche of IACS. This lack of attention reflects not only in noticeable less research efforts, but also in the absence of structured analysis of such research and open research issues.

Despite the attention it has received in the last years, there is a general lack of systematic literature reviews covering this topic. An extensive report sponsored by the ASIS Foundation Brooks et al. (2017) includes an analysis of BACS vulnerabilities and security management best practices (among more general aspects, such as a general BACS industry and market analysis and BACS standardization), but focuses more in the mainstream industry landscape than on recent industry and research advances. An introduction to smart buildings security has been provided by Wendzel et al. (2018). However, it is more a tutorial-style overview than a systematic literature review. Finally, a preprint from Ciholas et al. Ciholas et al. (2019) does provide a literature review of security for smart buildings, but it is not exhaustive enough, probably due to the author's ambition of covering a broader spectrum of topics around the concept of smart buildings. In this paper we bridge this gap by providing a comprehensive survey of research and industry developments specifically addressing the security of BACS.

The rest of the paper is organized as follows. First, we describe the methodology used for our systematic research (Section 2). Next, we provide the reader with an introductory overview of BACS and related topics (Section 3). Next, we discuss the relevance of safety, security and privacy for BACS and overview a few representative known attacks (Section 4). Next, we review proposals for improving BACS security (Section 5) and discuss open issues and research directions (Section 6). Finally, Section 7 concludes the paper.

2. Methodology of the literature review

The main objective of this paper is to gather and organize information about research and industry developments in the field of BACS security, in order to characterize the current state of the art. A wide systematic search was conducted as source of information, based on five databases: IEEE Xplore, Science Direct, Springer, ACM and Wiley, complemented with other sources such as search engines and specialized conferences.

The query pattern used for search was: *(((smart AND building) OR (Building AND Automation) OR (home AND automation) OR (Domotics) OR (building AND management)) AND (Safety OR Security OR Attack OR Threat) AND NOT(energy))*. This pattern was adapted to the different database engines in order to get the best results. For some databases, additional filters such as *com-*

Table 1 – Documents processed in this study.

Database	Total retrieved	After applying inclusion criteria	After title selection	Used after abstract selection
IEEE	4896	1966	53	33
Science Direct	10,604	2089	24	9
Springer	36,665	1450	23	9
ACM	785	340	12	7
Wiley	2821	1335	12	8
Other Sources			138	50
Total				116

puter science or *communication networks* were also used, to refine the search. The adopted inclusion criteria were:

- Publication in the last five years.
- Studies published in English.
- Inclusion of the relevant papers referred by included studies.

As exclusion criteria, we chose to eliminate all documents whose full text was not available and those that dealt mainly with energy issues, as our focus is domotics and building or residential automation, in a broader sense.

In order to complete this search, we've added an extra search to retrieve privacy-related studies in BACS.

The selection of records was then made through the analysis of documents whose titles and/or abstracts were retrieved through the search strategy and that met the inclusion criteria mentioned above (see Table 1).

3. An overview of BACS

In this section we provide a brief overview of BACS and related topics, in order to familiarize the reader with the subject.

3.1. *General overview of BACS*

Smart buildings are automated buildings designed to increase safety and comfort, save costs and be environmentally friendly, while being able to interact with other smart buildings and service grids. These buildings are supported by control systems designated as Building Automation and Control Systems (BACS).

EN ISO 16484 (EN/ISO, 2016) specifies the phases required for BACS projects and the hardware needed to perform the tasks within a BACS, as well as the requirements for overall functionality and communication. According to these specifications, the building automation and communication is organized in three distinct layers: *Management, Automation* and *Field* (Section 1).

The *Management Level* corresponds to the Information Technology and Communication (ICT) network. This level entails the operation stations, monitoring and programming units, that process data and support the monitoring and management of the automation system. (Fig. 1).

The *Automation Level* normally represents a dedicated communication network used to interconnect the devices that have as main purpose the control (automation) of the building. This layer groups global building controllers such as chillers, energy production systems and air handling units.

The *Field Level* groups all the devices that are connected to the physical systems under control. These devices are generally self-contained physical units like sensors and actuators. In some situations they are connected to controllers in the Automation Level, communicating using specific protocols. In other situations they have their own processing and decision capabilities, to control local processes.

The Join Research Centre of European Commission recently published a report with a good State Of the Art (SoA) (Serrenho and Bertoldi, 2019) that complements this brief overview with an introduction to the whole smart home ecosystems, with a focus on their energy implications. Several recent challenges are identified, with the *do it yourself* (DIY) mindset being one of the most important, since it enlarges the number of buildings with some sort of automation but eventually hampers the introduction of professional-grade, integrated BACS solutions.

In 2017, the Building Performance Institute Europe (BPIE) evaluated how ready was Europe for Smart Building Revolution (Groote et al., 2017). It also associated the word *smart* with the concern of optimizing energy consumption and the use of clean renewable energy sources (see Fig. 2). It created a function with several parameters for that evaluation, designated as Smart Build Environment Indicator.

Smart buildings include mostly two kinds of solutions: those that integrate the existing building automation systems (that we will generally refer to as *BACS*); and those that only have mostly independent assets that automate a specific task or device on the building (that we will designate, in the scope of this paper, as *IoT-like*). This last one is mainly out of scope in the present paper and only briefly reviewed in Section 3.3.

The most commonly used standards and protocols in BACS are BACnet (Building Automation and Control Network (BACNet, 2020)), LonWorks (Local Operating NetWorks ANSI (2010)), KNX and Modbus (MODICON, 1996).

BACnet was created in 1987 at Cornell University, to address the needs of building automation and control systems. It uses the Open System Interconnection (OSI) model and it became an ANSI (American National Standard Institute) standard under the auspices of American Society of Heating, Refrigerating and Air Conditioning Engineers (ASHRAE).

LonWorks was created in 1989 by the Echelon Corporation, and was accepted in 1999 as a standard for control networking by ANSI (ANSI/CEA 709.1-B) (ANSI/CEA, 2010).

KNX resulted from the association of the European Home Systems Protocol (EHS), BatiBUS and Installation Bus (EIB or Instabus), and has been standardized through

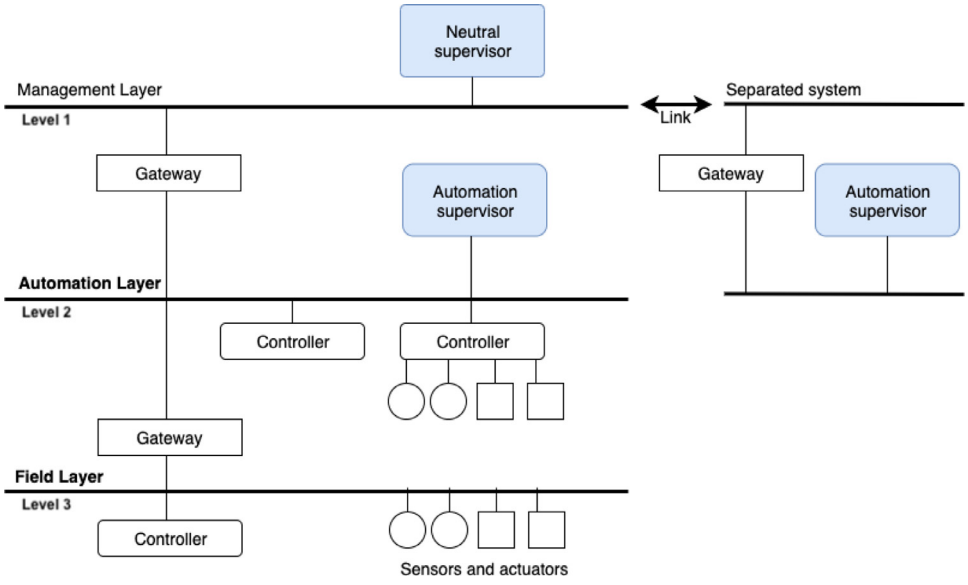

Fig. 1 – Three-layer BACS Architecture (adapted fromBrooks et al. (2017)).

EN50090 (CENELEC, 2012b), ISO/IEC 14543 (ISO/IEC, 2006) and EN13321 CENELEC (2012a), then extended to Chinese standard GB/T 20965 (China Machinery Industry Federation, 2013) and ANSI/ASHRAE 135 ASHRAE (2016). It is also based on the OSI model and extends the communication protocol to incorporate system commissioning and parameterization to allow interaction between devices from different manufacturers.

Modbus was developed in 1979 by Modicon (now Schneider Electric), as a serial communication protocol for Programmable Logic Controllers (PLCs), it was released as an open protocol in 2004. It is based on a master/slave architecture, using simple function codes, together with a plain data model. It is widely used in industrial automation for Supervisory Control and Data Acquisition (SCADA) systems. In building automation it is mostly used in control equipment such as chillers, boilers and fans.

EEBus (EEBUS-Initiative, 2019) is also worth mentioning. It is a relatively recent effort with the prerequisite of exchanging information to coordinate and shift the energy between an intelligent power grid and the individual components in the households and buildings (e.g. photovoltaic system, battery storage, heating and electric vehicle) with the aim of creating a standardized language for energy. Its main objective is helping to achieve the climate goals by enabling transparency of energy demand; avoidance of load peaks and grid bottlenecks; use of flexibility on the supply and demand side and use of decentralized energy generation. EEBus architecture is based on the Smart Grid Architecture Model (SGAM CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids (2012)) and represents a data communication standard forming the interface between in-house communication and energy supplier.

Besides these standards, there are many other standards and protocols with some relevance in the scope of BACS (some of them originally intended for different purposes), as illustrated in Fig. 3. Nevertheless, for sake of conciseness, we will not address them in this paper.

Fig. 4 is a diagram, proposed by Siemens Brooks et al. (2017), that represents the distribution of the most used protocols and standard and their relation with the building automation and communication layers. The bar *Web* represents all the different web services that exist either for the Automation and Management layers.

Domotics systems were initially designed to function autonomously and isolated from other systems. This is also true in BACS systems. However, the paradigm has changed with the constant integration of different services and functionalities associated with the use of ICT to exchange information between different protocols. These systems can no longer rely on isolation and obscurity for ensure proper security. This carries the cost of threats and potential attacks, not just from interconnected networks but also from the Internet in general.

When compared with ICT systems, the lifespan of BACS devices and systems is considerably longer, Such components are expected to reliably operate in a continuous and 24/7 basis during decades, often regardless of any security issues that may be eventually found. Due to the increasing reliance on those systems to ensure critical building functions, customers often have no other choice than to keep using them despite knowing about existing security problems. This situation has been somewhat worsened by the encapsulation of BACS protocols in IP, which has resulted in the inheritance of known security weaknesses from the ICT domain.

3.2. *A review of BACS-related literature*

The BACS market is undergoing rapid expansion (Khedekar et al., 2016), with smart buildings being considered one of the main driving forces behind this trend. Conceptually, smart buildings are perfectly aligned with the scope of BACS, encompassing a series of requirements outlined in Hui et al. (2017), namely:

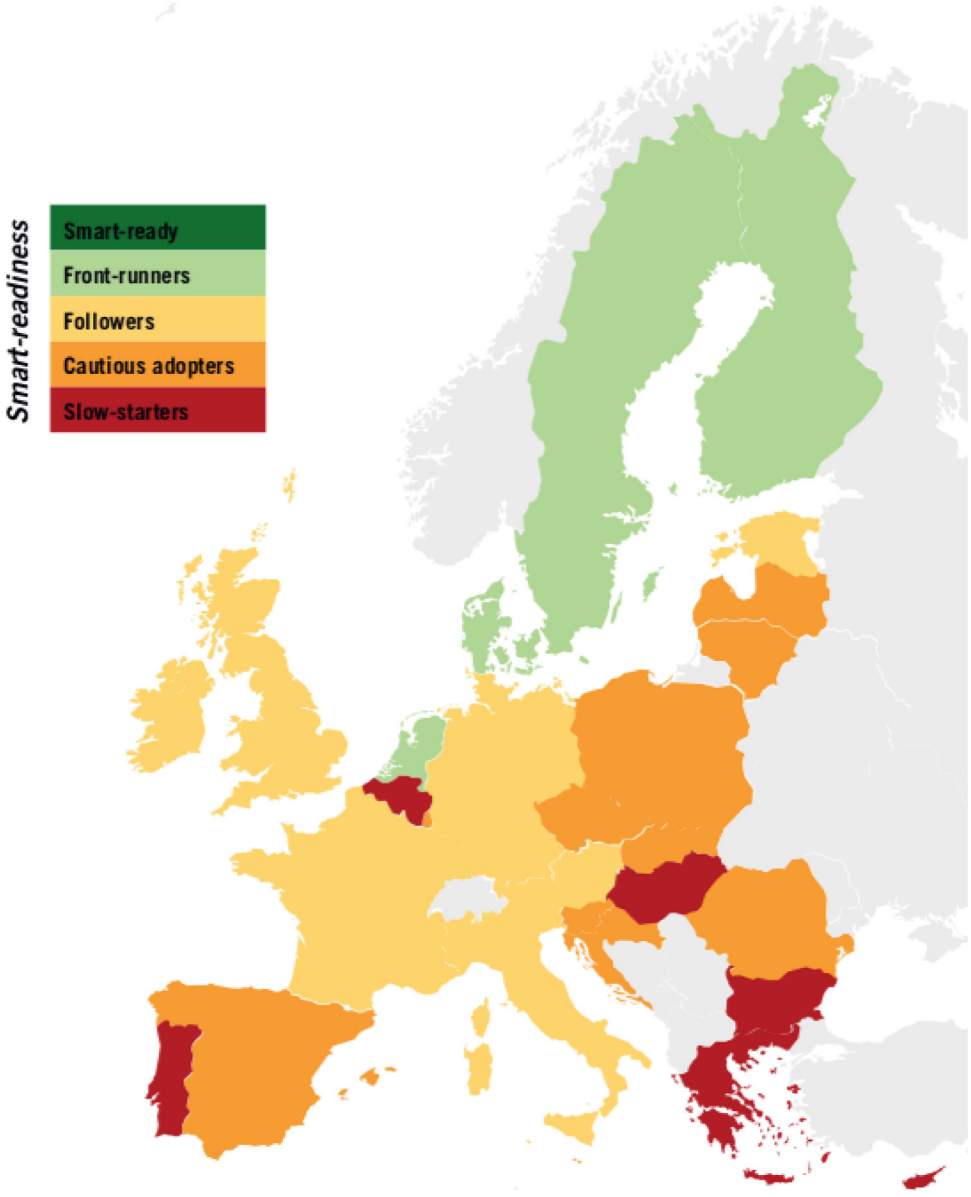

Fig. 2 – Smart-readiness across Europe (Groote et al., 2017).

- heterogeneity;
- self-configuration;
- extensibility;
- context awareness;
- usability;
- security and privacy protection;
- and intelligence.

While these requirements provide the groundwork for an encompassing definition (and, to a certain extent, a taxonomy) of what a smart building is, several other perspectives can also be found in the literature, some of which are going to be presented and discussed in the following paragraphs.

For instance, Lobaccaro et al. (2016) provides a systematic review of smart home technologies, grouping them into four categories: Integrated wireless technology (IWT); Home energy management system (HEMS); Smart home micro-computers (SHMC) and Home automation (SHS/HA). Toschi et al. (2017) provides a survey about network elements, definitions and standards used in Machine to Machine (M2M) communications for different BACS environments, with Domingues et al. (2016) providing an overview about concepts and technologies used in this domain. Also, a survey on ontologies in building automation was performed by Butzin et al. (2017).

Other works are more focused on BACS communications, from the physical medium to protocol-level aspects. For instance, Hallak and Bumiller (2016) provides an overview of powerline communication technologies used in home and industrial automation, also providing some application examples.

Experimental results were obtained by Zhibo et al. (2017) for the validation of IP Wireless protocols used for in-

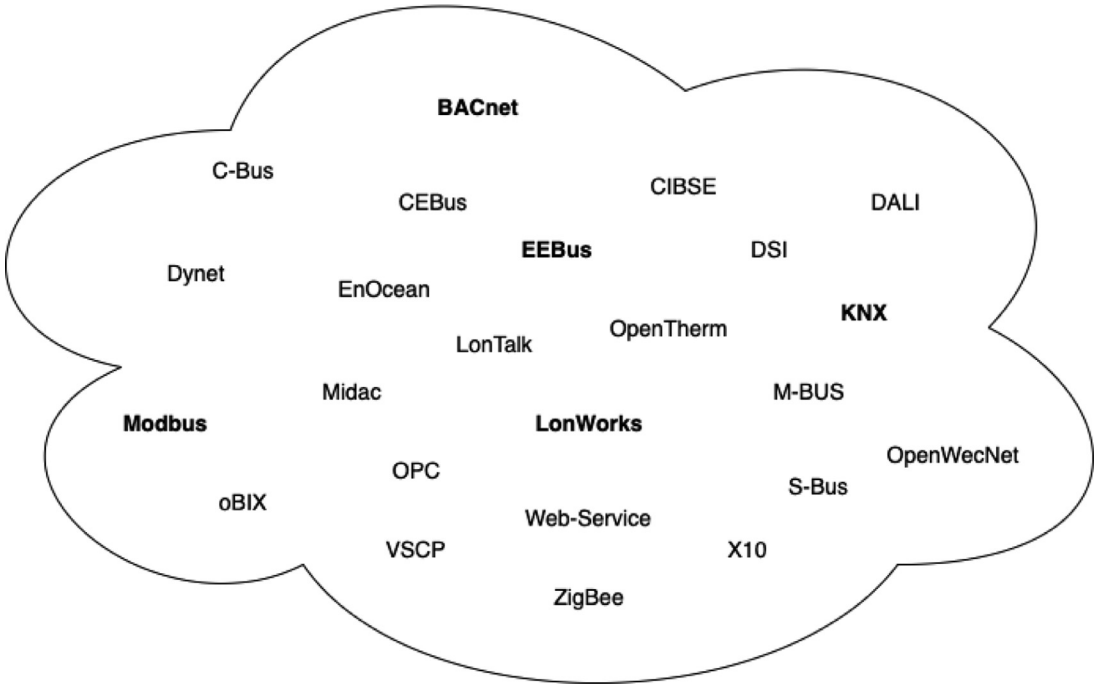

Fig. 3 – BACS Architecture Industry Standards and Protocols.

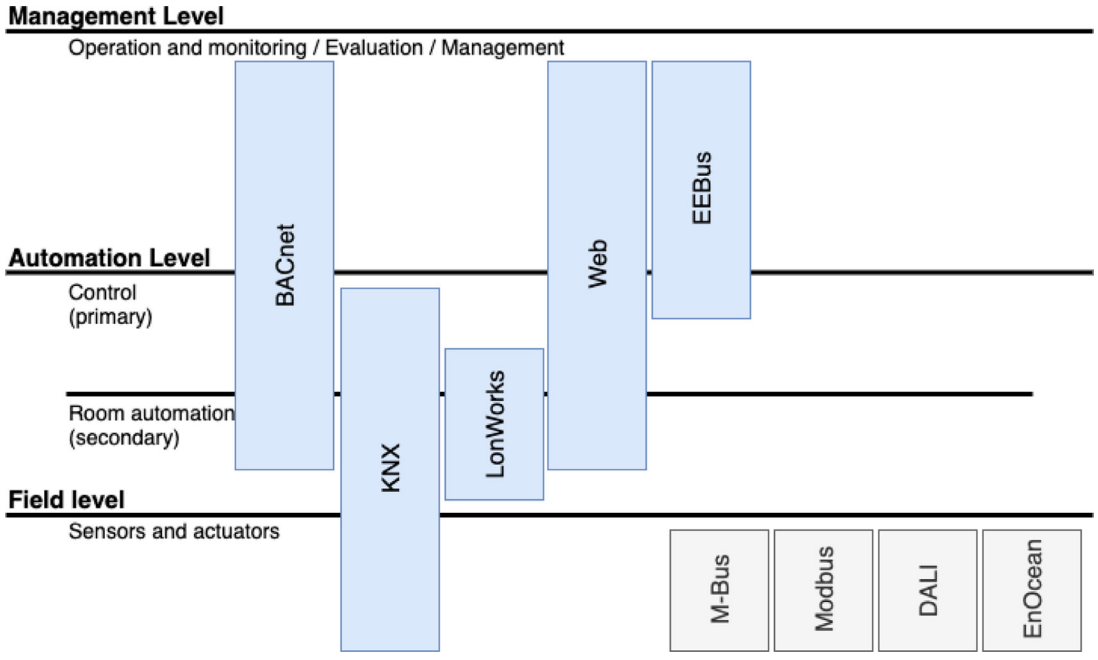

Fig. 4 – BACS Software Architecture (adapted from Brooks et al. (2017)).

telligent grid and smart homes. The study was mostly concerned with latency, packet delivery rate (PDR), coverage and power consumption metrics, having concluded that a PDR between 80–90 percent with a maximum 150 ms deadline can only be achieved with a 3-hop boundary.

A good review of the BACnet protocol is addressed by Hersent et al. (2012). This protocol is focused on the network layer and above, being used to orchestrate several other technologies (KNX, ZigBee, Webservices, etc) as it specifies interworking interfaces for each of them. Also regarding KNX, one of the most popular BACS standards for which only IPv4 interoperability is provided, Seifried and Kastner (2017) proposes a possible KNX IPv6 architecture, and also compares the recent KNX IP Secure initiative with IPSec network layer security.

The integration of BACS with the cloud and IoT devices is also addressed by Li (2018), which proposed the development of a smart home cloud server where the communication is

established through a Message Queuing Telemetry Transport (MQTT) broker.

More experimental aspects, such as the integration of Software Defined Networking (SDN) into smart buildings was considered by Usman et al. (2019). The study considered the adoption of SDN to be generally beneficial having also identified several SDN-related gaps/challenges in terms of network management, maintenance, east-west/southbound interface integration, traffic management, energy and automation.

Other works are more focused on architectural or development aspects. For instance, Fatehah (2018) proposes the use of a software engineering approach for the design of BACS, while Bugeja et al. (2018) has an overview of smart connected homes architectures (centralized or distributed) and with different communication models (device-to-device, device to cloud or device to gateway).

Regarding security aspects, a comprehensive industry study (Brooks et al., 2017) about vulnerabilities, current industry practices and security management best practices was undertaken in 2017, with support of the ASIS Foundation, Security Industry Association and Building Owners and Managers Association. It covered several different aspects, including a survey involving practitioners from 38 different nations and diverse areas (72 percent from security and the remaining from facilities), a survey review undertaken by a focus group of 14 experts, and the draft of BACS security guidelines for the industry. The report also provides an overview of BACS, its fundamental concepts, the BACS market and its industry landscape.

3.3. *IoT Vs BACS*

The usage of IoT for home automation has received considerable attention, both from a commercial point of view and from a research perspective.

A review of system architecture, software, communications, privacy and security of IoT based smart homes can be found in Mocrii et al. (2018). Another survey of the adoption of IoT for the development of smart buildings, within academic and industry contexts, is provided in Jia et al. (2019). The authors argue that a mature adoption of IoT technologies in building industry is not yet realized and still requires intensive research.

Some authors have proposed specialized Intrusion Detection Systems (IDS) for IoT. A good summary on this subject, that includes mobile ad hoc networks, wireless sensor networks, cloud computing and cyber-physical systems, can be found in Santos (2018). It covers works from 2009 to 2017, concluding that IDS for IoT are still in their infancy, cover just a few of the existing technologies and not being able to detect a large range of attacks.

Darabseh and Freris (2019) proposed software defined cyber-physical architecture for IoT applications. Software defined principles are used with the intention of decentralizing decision-making within IoT. This architecture entails three main domains: the physical space, the cyberspace and the structured control space, all of them described as software defined systems.

Some examples of low-cost DIY solutions used for home automation systems are provided by Asadullah and Raza (2016). A low-cost home automation system based on Wi-Fi wireless sensor networks is proposed by Vikram et al. (2017).

A discussion of security in existing IoT communication protocols (e.g. Bluetooth, BLE, ZigBee, NFC, Wi-Fi, Thread, LoraWAN) is presented in Ray (2017), supported by a previous survey from Granjal et al. (2015).

Dutta and Wang (2018) proposed an IoT-based security system for smart buildings using RFID and IMEI numbers for two-step authentication. An investigation of security requirements and solutions for an IoT-based smart home architecture is provided in Waqar et al. (2017).

The authors of Fischer et al. (2017a) proposed a security demonstrator for experimental evaluation, testing it with two attack scenarios using the Z-Wave protocol.

The smartFW framework (Ilieva et al., 2016) is proposed for integrating short range devices in smart home buildings. It acts as a mediator between IoT integration platforms, allowing end-users to control their smart homes.

Blockchain technology is proposed by Abunaser and Alkhatib (2019) to solve the centralized cloud drawback of IoT in smart homes. Blockchain may eventually help securing data and transactions, but more research is needed until such promises are materialized.

Figure 5 represents the typical architecture of current implementations of IoT for building automation. It shows the segregation that exists between the components locally deployed. In this particular use case scenario, integration between sensors, appliances and actuators takes place in the cloud service. Quite often, system integration services from different providers rarely communicate with each other, requiring another layer for interconnecting different systems from different providers. This clearly differs from classic BACS, which are locally deployed with full operation support and were designed to work in closed environments, though frequently supporting interconnection to the ICT layer and to the Web, a natural evolution introduced mostly for maintenance and support purposes.

Lilis et al. (2017) provides a good discussion of the opportunities and side-effects of fully IoT enabled and controllable intelligent buildings, when compared with the well-established classic BACS. One of the main points against IoT is that it is not possible to expect continued product development and support, indefinitely, from a single manufacturer. The only possible way to reassure the market is the existence of compatible products from multiple manufacturers. This is a key point in favour of BACS, with their standards. BACnet claims more than 800 vendors, LonWorks claims a range of more than 4000 products, and KNX claims more that 8000 compliant devices from more than 470 members (most of them manufacturers).

Qiu et al. (2018) introduced the concept of Heterogeneous Internet of Things (HetIoT), supported by the intrinsically heterogeneous architecture which is characteristic of IoT solutions. The authors propose a four-layer HetIoT architecture consisting of sensing, networking, cloud computing and applications. They also present and discuss a SoA in HetIot research and applications.

Vanus (2018) focuses on the functional interconnection of a KNX-based BACS system and IBM Watson cloud ser-

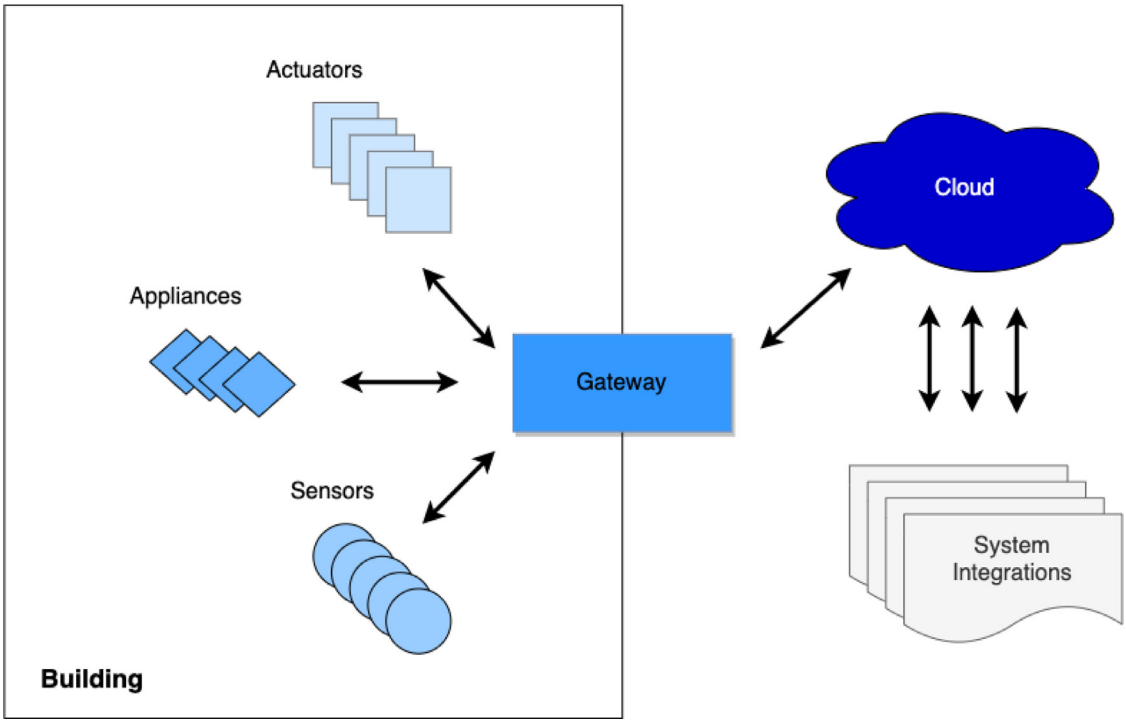

Fig. 5 – IoT Cloud-based architecture for smart home (adapted from Mocrii et al. (2018)).

vices, in order to enrich the system with a natural language interface.

A number of deployment-limiting issues currently impact the scope of IoT utilization, including: lack of comprehensive end-to-end standards, fragmented cybersecurity solutions, and a relative dearth of fully-developed vertical applications, as stated by the authors of Minoli et al. (2017), which review some of the technical challenges and opportunities related with the adoption of IoT for building automation. It was concluded that, from a technological perspective, the development of appropriate reference architectures and supporting standards is fundamental, fostering interoperability and equipment cost-effectiveness. It is also critical to develop and deploy strong system-wide IoT security capabilities, as it expected that the ongoing network softwarization trend, as well as the introduction of 5G communications will improve the support for IoT traffic. From this perspective, it is expected that the development of cloud-based analytics will become an enabler for efficient optimization, data mining, trending and forecasting capabilities.

The above arguments lead to the conclusion that the easier deployment and the lower cost of IoT devices will turn them into an extension of existing BACS systems. Their integration with the Cloud is one of their greatest assets, though at the cost of additional security concerns and challenges (Bajer, 2018).

4. Security concerns in BACS scenarios

In this Section we discuss the impact of security in typical BACS scenarios. First, we briefly overview the relevance of security (and safety) in such scenarios, identifying general risks associated with intentional or accidental failures of the controlled home automation processes and/or with loss of privacy. Next, we discuss previous works that analyze potential safety and security risks directly or indirectly related with BACS. Afterwards, we approach some studies related with privacy in BACS. Finally, we present a set of known attacks to BACS, both in laboratory testbeds and in real work systems.

The BACS facilities control and are controlled by devices which are often physically accessible to the users of the buildings. This way, malicious users can easily hamper sensors and controllers. More over, since many of those devices allow bidirectional access to the automation and management platform, they may provide an access path to BACS platforms. In parallel, BACS platforms may also be reached via the IT systems they are interconnected with, providing a remote attack path.

The unauthorised access to the data that circulates in the BACS systems opens the possibility of inferring knowledge about the usage and occupation of spaces, in a clear violation of the privacy of their users. The manipulation of these control networks makes it possible to block or confine users to certain spaces, or to change environmental conditions (e.g. by manipulating the HVAC, ventilation and lighting systems).

Intrusion into BACS systems creates a privacy issue. Building occupants' data and their habits can potentially be exposed. This potential exposure may lead to various forms of misuse.

The failure or malfunction of certain BACS equipment is also a safety problem, since it may cause improper functioning of the rest of the system. In this sense, monitoring and anomaly detection should also be a concern when analysing

BACS safety and security. Moreover, malicious access and manipulation of BACS platforms may lead to the excessive deterioration or even failure of building equipment, through forced operation outside the normal thresholds. Ultimately, this situation may even put the whole building at risk (e.g. fire, intrusion).

4.1. *BACS Security risks*

In this subsection, we discuss some of the most relevant previous work focused mostly on identifying and analysing security risks somehow related with BACS.

BACS security issues were already a concern in 2010, especially in the anticipation that insecure protocols would soon be opened to ICT networks. A few approaches to BACS safety and security have been proposed by Granzer et al. (2010), Novak and Gerstinger (2010), but had no impact in the real world. As of 2015, a study from the Gartner Group prediceted that, by 2018, 20% of smart buildings would suffer from digital vandalism in some way (Levy, 2015).

Similarly to IACS, BACS security breaches are often considered to be a consequence of using systems, protocols and standards that were originally conceived to operate in isolated environments, without any connection to ICT networks or the Internet. This is aggravated by the fact that many legacy devices cannot be patched, often meaning that only isolation or complete replacement might ensure adequate security (Wendzel et al., 2018). In general, most attack categories that are characteristic of IACS (Macaulay and Singer, 2011) may be somehow transposed to BACS scenarios. However, even though some the protection strategies used in IACS might somehow provide hints on how to keep BACS secure, there are considerable context differences that, eventually, require specific approaches to the problem of BACS security.

An overview of the most used BACS protocols, security issues and recent security research trends is presented in Wendzel et al. (2018). Authors summarize and compare some of the most used BACS communication protocols (e.g. KNX/EIB, BACnet, ZigBee and EnOcean (EnOcean GmbH, 2020)) and identify attacks as belonging to two different levels: network level (management and automation levels of BACS architecture) and device level (field level of BACS architecture). At network level, attacks are split into four different categories: traffic interception (network sniffing); malicious packet creation; network packet change (man-in-the-middle attacks); and outage or reduction of network service quality (denial of service). On device level, the attacks are grouped into three patterns: physical tamper; side-channel analysis (e.g. usage of monitoring to obtain cryptographic keys); and software attacks (such as code injection).

A review specifically focused on the intersection of smart grid and smart homes (in the sense that information is exchanged between them to optimize energy management) is provided in Komninos et al. (2014). Several scenarios are presented, accompanied by potential security countermeasures, based on a review of contemporary literature.

Lei et al. (2018) address the vulnerabilities of home digital voice assistants, which often rely on single factor authentication – a voice password like just some words (eg. "Alexa", "Hi, Google"). Authors provide a set of proof-of-concept attacks that send fake commands to the voice assistant, using both hacked Bluetooth speakers and smart TVs. Then, they implement and test the introduction of a second authenticated factor (only allowing commands if any person is detected nearby), using WiFi technology to detect indoor human motions.

Liu et al. (2018) propose a taxonomy for security assessment of IP-based BACS (see Fig. 6) and apply it to Thread (an IP-based protocol for IoT in building automation (Thread Group, 2019)).

The authors of Heartfield et al. (2018) propose a different taxonomy approach defining a causal relationship (see Fig. 7) between three different root criteria (attack vector, impact on domestic life and impact on systems) of the home cyber-threat taxonomy. Then a classification is provided for each of those root criteria (the diagrams are omitted from the provided figure for lack of space), considering the attack vector as well as the impact on systems and, consequently, on the occupants of a smart home.

A very simple taxonomy for classifying security threats is also proposed by Anwar et al. (2017), with three main groups of threats: unintentional, intentional/abuse and malfunctions.

Graveto et al. (2019) propose a taxonomy that, despite being originally developed for the IACS domain, can also be used to classify network attacks in BACS, as shown in Table 2.

The BACnet protocol and its vulnerabilities are presented in Valli et al. (2017). Denial of service, halt or buffer overflow of legacy network interfaces by the relative brute force represented by a 10/100 Mbit/s or a 1 GBit/s connection are reviewed. BACnet specifies AES 128 bits encryption and end-to-end authentication, but only the more recent devices with security-based objects and properties apply these specifications. They are optional in the standard due to the need of supporting legacy devices. The protocol has minimal session protections and, therefore, it is vulnerable to replay attacks and spoofing. Finally, the payloads are binary or even clear text, allowing trivial decoding and subsequent tampering. A description, simulation and testing of proof-of-concept protocol attacks on a BACnet system are provided by Peacock et al. (2018), which also presents a classification of known attacks according to the STRIDE matrix (Soopfing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of privilege) developed by Garg and Kohnfelder (1999).

Gai et al. tested home appliances (e.g. SmartTVs, smart home theatre, smart kettle, smart refrigerator, smart thermostat, smart lights or smart security cameras) and categorised vulnerabilities and attack surfaces (Gai et al., 2018).

An analysis of two use cases based on the field level on LON and KNX, using BACnet at the automation level, is provided in Mundt and Wickboldt (2016).

Coppolino et al. (2015) overview the risks resulting from the introduction of internet-enabled devices (e.g. smart home gateways) on BACS for supporting remote access and control. In the same line, Meyer et al. (2017) identify three new attack vectors in BACS related with internet connections: acquisition of local network access through a provider-supplied device; access to other existing user devices; and data access at remote storage providers.

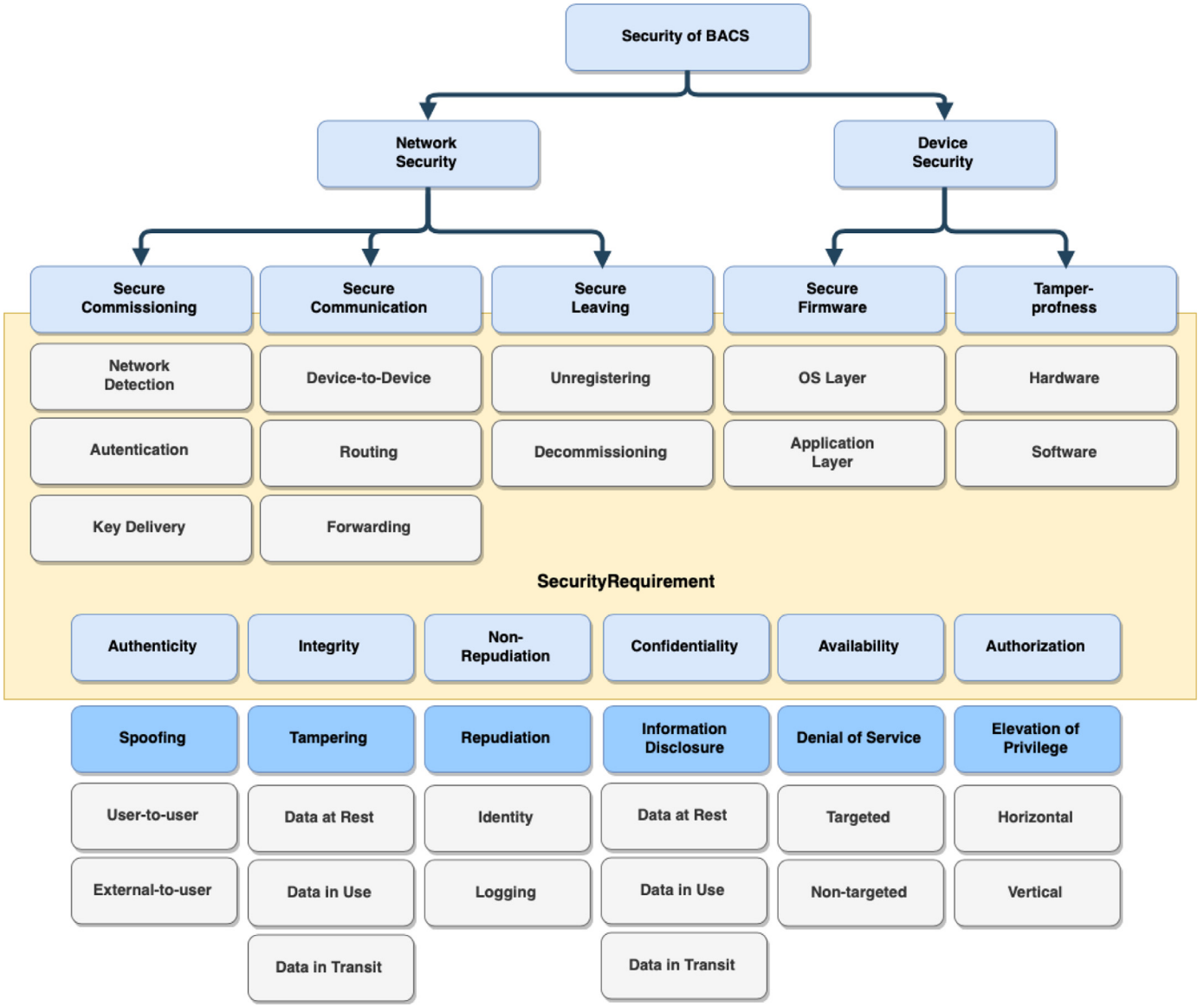

Fig. 6 – Security analysis taxonomy for BACS (adapted from Liu et al. (2018)).

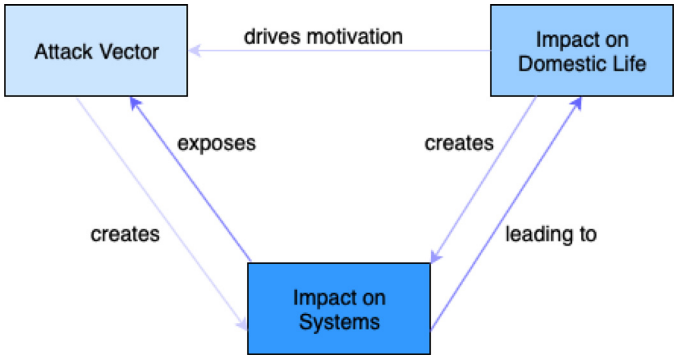

Fig. 7 – Causal relationship betweeen root criteria in smart home cyber-threat taxonomy (adapted from Heartfield et al. (2018)).

A set of network scan results for open, real world BACnet and KNX BACS installations was published in Praus and Kastner (2014). A summary of network attacks that may threaten BACS has been provided in Saxena et al. (2017).

A survey of software security requirements and software protection methods for distributed control applications is provided by Praus et al. (2016).

Looking specifically at BACS platforms that communicate over powerline, such as digitalSTROM AG (2019), Brauchli and Li (2015) provide an analysis of potential risks and mitigation strategies.

An overview of the Building Energy Management Open Source Software (BEMOOS) (2019), developed for energy load-balancing, is provided by Rathinavel et al. (2017). Security threats and their countermeasures in this context are also analysed.

Jia et al. (2017) discuss the vulnerabilities in a reference smart home architectures, proposing a semi-automatic vulnerability detection system for detecting vulnerabilities prior to factory shipment of BACS devices.

4.2. *BACS Privacy*

One of the first associations between privacy and buildings probably took place in 1964, when the Hamberger couple rented an apartment and the owner, Mr. Eastman, placed an audio recording device in the bedroom (Hamberger Carl; Eastman Clifford, 1964). This situation and subsequent legal actions led to the a legislation change focused on intrusion of privacy of personal quarters. The timeline of the privacy problem in residential buildings (and other scenarios) is discussed in George et al. (2020), addressing the system dynamics of data collection by building automation devices and IoT, as well as their technical and social integration, challenges and significance. As most users are not aware of the information that is collected and the risk to their privacy, this paper suggests a solution with two steps. First, the implementation of a packet tracer that displays the collected data, increasing people awareness and encouraging them to better preserve their privacy. This awareness will lead to a second phase in which new legislation could emerge, requiring manufacturers to implement algorithms that guarantee that devices and services are compliant with privacy regulations.

We only found a couple of papers addressing privacy in the scope of BACS, which forced us to further extend the search towards papers on privacy for so-called "smart buildings" (mostly linked with IoT and smart metering privacy concerns) that, somehow, are also relevant in BACS scenarios.

Kraemer and Flechais (2018) enumerate five steps to address the challenges of privacy research in smart homes, that could be also applied to BACS: data collection and processing; in-depth analysis of the context; longitudinal panel studies to gather empirical data and privacy behaviors; addressing the perspective of policy makers; and, finally, addressing the criticism that existing frameworks for product design are too vague. However, this vague and generalist approach is also demonstrative that almost everything remains to be done regarding research in the field of privacy in BACS.

Next, we group the surveyed works into five groups: studies based on users' feedback and perception of privacy; case studies on privacy in buildings with BACS; the usage of mathematical algorithms at the service of privacy; some IoT implementations that, by analogy, could be adopted in BACS; and, finally, the issue of smart energy meters and some solutions to enhance privacy in this context.

4.2.1. *User'S feedback and perception*

The authors of Zeng et al. (2017) conducted a set of semi-structured interviews with fifteen people residing in smart homes (twelve of them being administrators of these systems) to understand how they use their smart homes, their actions related with security and privacy, and their expectations. They found out, as expected, that users are little concerned with their privacy. The natural tendency of users is to trust device and service providers, even claiming that they have nothing to hide, or simply thinking that the existence of a password is enough to guarantee their privacy. When asked about mitigation methodologies, the answers were limited to the usage of independent Wi-Fi networks and the usage of secure passwords as problem mitigation techniques. Finally, they also verified that the existence of users with different levels of access may even lead to privacy issues between the various users of the same home.

A set of interviews to 97 UK-based users of smart assistant devices (Alexa or Google assistant), to gauge their per-

Table 2 – Simplified Taxonomy of BACS attacks.

Level	Class	Impact	Attack examples
Layer 2/3	Scanning/ Scouting	Getting information about network topology and devices	On KNX/IP and BACnet/IP, ARP or LLDP queries can be used to track devices; Probe for available services and protocols using a FIN or SYN scan. Simple sniff of KNX/TP messages (2nd and 3rd bytes represent the sender Individual Address)
	Attack on data integrity	Unstable and/or unpredictable behaviour	Corrupt inflight data through packet manipulation
	Denial-of-Service and/or service degradation	Loss of visibility and/or control	Overwhelm or crash device, via SYN or ICMP flooding; Employment of CAM table overflow to disrupt communications
Protocol/ service level	Scanning/ Scouting	Getting information about service and device capabilities	Brute force use of KNX *T_Connect_PDU* to discover existing devices, subsequent scan attacks for device profiling; Use of MITM to analyse used services and protocols
	Integrity	Unstable and/or unpredictable behaviour	Abuse of protocol specifications and features, such as the BACnet *ReadProperty* and *Whoami* or KNX *A_Memory_Write_PDU* attacks
	Denial-of-Service and/or service degradation	Loss of visibility and/or control	Exploit vulnerability to crash or disable service or device (such as a FTP buffer overflow); Introduce latency or communications failures through MITM attack; Use of managment commands to influence device operation
Process level/ semantic	Scanning/ Scouting	Reveal details about the nature of the process	MITM attack for scouting purposes or preparation of replay attack; Use of KNX instructions to download parameters and/or group address tables; Structural analysis of memory map thorugh probing using KNX *A_Memory_Read_PDU*
	Direct manipulation	Manipulation of process variables	Manipulation of process variables to alter behaviour, through direct device access (KNX *A_GroupValue_Write_PDU* or *A_GroupValue_Read_PDU*)
	Interception and fuzzing	Interception and manipulation of process values	Manipulation of process variables to alter behaviour, through command injection or protocol fuzzing, using a MITM (via ARP poisoning or CAM table) attack to intercept communications and conceal the intruder; Process-aware response injection or replay attacks
	Reprogramming	Process behaviour is modified and/or hijacked	Use of KNX instructions to upload firmware, parameters and/or group address tables

ception of these smart assistant devices when compared to other more familiar devices such as smartphones and computers, is presented in Lin and Parkin (2020). About half those users were unsure of how to address the privacy issues and settings, and 20 of them, when using shared devices, used sensitive information that should be kept private from other users. The reported transfer of privacy-related behaviors between previous used computing devices and newer smart home devices was low in the adoption of available privacy controls.

Kaaz et al. (2017) conducted a study on the installation and perception of privacy of users of IoT devices, having concluded that understanding how these devices operate is not trivial, making it difficult to perceive threats and the risks associated with their use.

Pathmabandu et al. (2020) propose an informed consent model to address the balance between privacy and convenience. This model is implemented using five steps: apply textual patterns to privacy policies; list privacy permissions; identify privacy infringements; track and log events; and recommend preventive actions that allow the user to control and mitigate emergent privacy issues that have occurred and/or my happen in the future. The proposed model enhances the user awareness, helps in the detection of privacy compliance

and infringement by devices, and improves the user's privacy-protecting behaviors in small steps.

4.2.2. *Use cases on BACS*

Across Europe, seniors want to live their old age in their homes, instead of retirement homes. Instead of providing care on scheduled appointments, there is the possibility of providing event-based services, improving costs and effectiveness. A case study is presented in Franke et al. (2016), analysing a house that uses the KNX standard as the basis of its BACS infrastructure. However, to guarantee the privacy of the occupants, all the information is processed on-premises, and only part of it is transmitted to remote care providers. Residents and their families can define the information to pass on to external entities (privacy by design), such as "the resident did not use the bathroom within the last 24 hours" or, for example, "the resident is not moving for more than 2 hours". These events allow the action without violating the privacy of residents.

The case study presented in Mundt et al. (2012), opposed to the previous example, demonstrates the possibility of violating the privacy of users of an office building to find out "who refuses to wash hands". The office building holds a BACS infrastructure, based on KNX, with motion sensors every 8 m, lighting control in all offices, laboratories and other divisions, and blind control in all convenient locations. The authors demonstrate that the sampling of KNX traffic, based on the collection of previous tests (asking some users to make their way from their office to the bathroom, with and without hand washing) allowed a posteriori, in an extended data collection, to infer the desired information. Accessing the information was easy by simply removing any switch with access to the KNX twisted-pair bus and then connecting there the collection system.

4.2.3. *Privacy-focused analysis of BACS data*

Xu and Agung Julius (2019) present the construction of a map of observations in the form of metric temporal logic formulas, which can be formally proved to allow the detection of faults in a switched system, while preserving certain privacy conditions. Two scenarios are considered: in the first, all room occupancy possibilities are private (unoccupied, one occupant or two occupants) and, in the second, only the room occupation by one person is private, considering it public when there are two or even no occupants. The entire mathematical formulation is presented and the inclusion of systems with both external and internal events, or even hybrid systems, are indicated as possible future works.

The usage of Gaussian noise in the corruption of measurements in a BACS system if presented in Alisic et al. (2020), as a way to mitigate unauthorized access to sensors data. This corruption of information aims at concealing the state of occupation in the apartment.

4.2.4. *Privacy issues in IoT implementations*

A system that uses infrared retro-reflection is presented in Santo et al. (2017), as an indoor positioning system that preserves the users' privacy. The device does not capture any details of the persons' appearance, despite using infrared images (if due care is guaranteed, such as placing the device avoiding to capture occupants near windows and avoiding their capture less than one meter from the places where residents spend most of their time).

The authors of Gao et al. (2020) use a Home Brain with a processing model, computing model and database to preserve the voice authentication for each IoT device, enabling privacy-preserving speaker verification. In an initial registration phase the features of the valid user voices/IoT pair are extracted and preserved in the database for future use.

As with BACS, most IoT devices have limited processing capabilities and patching to add security features is not allways possible. Thus, Iqbal et al. (2021) proposes to use software defined networks (SDN) in smart homes, by means of installing an Openflow switch, between the domestic gateway and the automation devices, as well as an SDN controller. This way, all requests from home users and even remote requests could be validated and even subject to authentication. The protocols necessary for authentication and privacy preservation are presented and discussed, as well as an evaluation and comparative analysis. The authors conclude that the protocol can be implemented in any smart system as it is based on lightweight nature of symmetric cryptography.

A framework based on spatio-temporal mining for efficient recognition of human activities in smart homes, accompanied by a technique to enhance privacy using micro-aggregation, is proposed in Samarah et al. (2017).

4.2.5. *Energy*

The intelligent control and measurement of energy consumption in buildings is a fundamental part of the smart grids vision. However, continuous submetering or sampling at tight intervals poses serious privacy risks to the users. The survey in Finster and Baumgart (2015) focuses precisely on these issues, starting by dividing the problem into two approaches: metering for billing and metering for operations. In the first situation, the continuous measurement is not important, but rather the accumulated consumption, sampling at longer intervals (in the limit extended up to the billing period) will allow the guarantee of privacy. In this case, the invoicing value being important, the problem can be reduced to a problem of trust, delegating the calculations to a third-party trusted by both (consumer and supplier); using a trusted platform; or the smart meter itself calculating the amounts due. However, in the second situation, regarding smart grid management, instantaneous measurements or at least at short time intervals are necessary, and four possible approaches for preserving privacy are analyzed: anonymization or pseudo-anonymization without aggregation; aggregation using trusted third party; aggregation without recourse to a trusted third party; and, finally, the submission of inaccurate information. In this last approach, the submission of imprecise information implies some coordination between the smart meters, so that the global accuracy is not too affected. The alternative to privacy issues will be to avoid generating information that creates privacy risks. For this purpose, two concepts are used: to use batteries; to determine the sampling rates of smart meters as a design parameter.

Pham and Mansson (2019) discuss in detail the use of energy storage systems as a technique for mitigating privacy

problems. Different types of storage technologies are analyzed, and the minimum storage/cost capacities are determined in cases of one or multiple users of the housing.

Sarbhai et al. (2019) also use batteries to obscure the data collected by smart meters, presenting three distinct algorithms as a solution for peak load reduction: random charging; random charging with linear response; and random charging with quick response (to avoid the risk of peak loads leading to outages, in case a large number of homes start charging their batteries at the same time).

Wu et al. (2016) provide a mathematical formulation of optimization for online privacy-aware cost-effective appliance scheduling. It should however be noted that the time needed for the calculations will grow according to the number of appliances.

Dasari et al. (2021) apply federated learning for energy load prediction approaches that enhance users' privacy. Each building uses local data to train its local model and compute gradients, then the masked gradients are sent to a trusted third-party server, which in turn performs the aggregation (without capturing information from any participant), and the aggregated model is sent to the model owner (e.g. energy supplier or grid manager). The final model is finally sent back to building users, allowing them to update their local models.

4.3. *Possible attacks*

The scientific community has analysed and showcased several attacks in controlled or laboratory environments, exploiting known BACS vulnerabilities and security issues. In this subsection we identify some of the most relevant works in this specific line of work, which we complement in the next subsection with an overview of the more well-known attacks to real systems.

Ling et al. (2017) demonstrate four attacks to a popular smartplug model (the EDIMAX SP-2101W): device scanning; brute force attack; spoofing and a firmware attack.

The vulnerability of BACnet to amplification attacks has been assessed by Gasser et al. (2017). These denial-of-service attacks where the response payload is larger than the request payload (by the bandwidth amplification factor – BAF). An identification of the BACnet properties that provide responses larger than the requests (i.e., BAF>1) is presented, leading to the conclusion that around 90% of the BACnet requests lead to responses at least 5 times larger (i.e. BAF>5), in some cases up to 19.8 larger responses.

Potential attacks in wireless communications potentially used in BACS (near field communication (RFID), ZigBee and WiFi) are identified by Krishnan et al. (2017). Potential threats to these systems include eavesdropping, physical attacks, denial of service, spoofing, replay attacks, data manipulation or injection, man-in-the-middle and packet rerouting.

4.4. *Publicly known attacks in real systems*

In this subsection we overview 5 known attacks to real BACS systems: the attack to the St. Regis ShenZhen Hotel: the Mirai Malware; the attack to the Google Australia Office; the attack to the Target Corporation; and the attack to the Fragrance Hotel Singapore.

The **St. Regis ShenZhen Hotel**, that occupies the top 28 floors of a 100 story skyscraper, allows guests to use an iPad to control all the facilities of their room: music, blinds, lights, TV, temperature, do-not-disturb lights, etc. The hotel BACS system had several flaws that allowed Molina (2015) to create a remote control that allowed access to all the hotel rooms. The attacker stated that he could even be located in another country.

The BACS system existing at this hotel uses devices with the KNX standard, and the KNX twisted-pair network was interconnected to the WiFi local network in order to communicate with the iPad app, using a KNX/IP router. By using a network sniffing such as Wireshark, and just pressing every button on the iPad, the researcher was able to create a dictionary of actions. The packed decoding provided the KNX Group Address of each action, and also disclosed each device's Individual Address.

First, the *eibd* open source tool (Kogler, 2011) was used to perform the handshake with the target IP and to keep the connection alive. Then, by using a simple write, the hacker could send any KNX command to the KNX network (e.g. *groupswrite local:/tmp/eib 2/0/3 80* will switch on the lights).

The performed network sniffing also showed the existence of "ghost" addresses, not used by the iPads – pointing to several other devices available at the KNX network, besides those from guests rooms.

The only possible solution to solve this vulnerability while maintaining the existing architecture, according to Molina (2015), would be to implement a secure tunnel between the iPad and a network device preceding the KNX/IP router. The tunnel should provide mutual authentication (such as SSL) to avoid the certificate steal from the iPad. Before each guest checks-in, the certificate should be reinstalled and the integrity of the app should also be verified.

The **Mirai Malware** is a very relevant example of an attack to real world systems. Even though it did not specifically target BACS platforms, the generic profile of the target devices is very similar to the profile of typical BACS devices.

In 2016 Dyn, a high-profile provider of Domain Name System (DNS) services, was the victim of a distributed denial-of-service (DDoS) attack that was clocked at 1.2 TBps Hallman et al. (2017). Less than a month before, the KrebsOnSecurity cyber security blog was also targeted with a similar attack, with about half the power (around 620 GBps). A detailed analysis of all the preparation and evolving steps of this attack, based on the now well-known Mirai botnet, is provided in Peterson (2019).

A bot network is composed of a Botmaster that controls the all system, a set of command and control servers, and finally an army of infected and conscripted bots. A botnet can be used either to perform a distributed task like distributed computation (e.g. mining) or to empower an action and concentrate efforts against a specific target (e.g. DDoS).

The Mirai botnet was conducted through internet-connected unsecure IoT devices (e.g. CCTV cameras, home routers). As stated by Elliot Peterson (Wright, 2019) the evolution of the Mirai army was the result of a "war" between competitors like Lizard Squad and others, that started back in August 2016. Both groups launched a botnet in an effort to gain advantage in the booter black market.

The first high-profile Mirai attack targeted the Krebs website (taking it down for several days and forcing Akamai Technologies to drop the site from its DDoS protection service). Following this attack, several other Mirai-based attacks took place against other targets, such as DYN – a large DNS service provider.

The building management system of **Google offices** located at Wharf 7, Sydney, was hacked by two security researchers in 2013. This system was built using the Tridium Niagara AX platform and Tridium SoftJACE controllers (basically Windows systems with a Java virtual machine and the Tridium client running on it).

After hacking the system, the security researchers opted for reporting the issue to Google (Zetter, 2013). Nevertheless, malicious hackers could have used the same vulnerabilities to gain full control of the building management system.

The accessed data included a control panel showing blueprints of the floor and roof plans, as well as a clear view of water pipes snaked throughout the building and notations indicating the temperature of water in the pipes and the location of a kitchen leak. Moreover, due to unpatched vulnerabilities, researchers were able to remotely access and get the config.bog file (which holds the system configuration data, usernames and passwords) by means of privilege escalation, also allowing to overwrite other files.

Tridium has meanwhile released a patch for the vulnerability that was exploited on this attack. The involved security researchers stated that a good fraction of the 25,000 other Tridium systems they have found connected to the internet are still unpatched and just as vulnerable as the Google's system they hacked. Such systems were in use, for instance, at a British Army training facility, at Boeing's manufacturing facilities in Renton, at the Changi airport in Singapore and at the Four Points Sheraton Hotel in Sydney.

The Target Corporation, a large retailer in United States, saw its network hacked and broke into in November 2013, by means of credentials stolen from a vendor of refrigeration, heating and air conditioning equipment (Fazio Mechanical Services), a subcontractor that worked at several Target locations (Krebs on Security, 2014).

An unidentified source stated that in order to monitor heating and energy management systems, access to outside suppliers to control systems and production costs was guaranteed. This created a gateway to the internal networks to which these systems were connected. First, the attackers uploaded their card-stealing malicious software to a small number of cash registers within Target stores, for testing all the functions. Then, before Black Friday, the intruders pushed their malware to a majority of Target point-of-sales. Finally, the stolen credit card data from Target's customers was uploaded to compromised computers in the United States and Brazil, accessed from the Eastern Europe and Russia.

This incident shows that outsourced BACS services may lead to the creation of external backdoors to the systems, either due to lack of security updates or improper use of access credentials. Similarly, the simple installation of IoT devices (such as basic DIY solutions) may support malicious actions without the owners' knowledge. Both legacy BACS systems and IoT devices are prone to exploitation by hackers outside their normal scope or purpose.

5. Proposals for improving BACS security

This section summarizes the most relevant proposals for improving security in BACS systems found in the literature. According to their scope, they are organized into five different groups: security monitoring; anomaly detection; intrusion detection systems; and contributions to the improvement of BACS.

5.1. *Security monitoring*

The works discussed in this subsection focus on improving the monitoring of BACS systems, namely with the addition of specialized devices (able to read and process the messages exchanged between the different BACS nodes) and/or with specialized analysis techniques able to detect potential attacks.

Jones et al. (2018) propose an automated device-level solution to monitor BACnet networks. Deployed in a single board computer (SBC), this device intercepts communications between BACS devices at field-level. It supports deep packet inspection and is able to produce a few simple active responses, by using unsupervised artificial neural networks. When an attack is detected, malicious traffic is blocked until the affected node is brought back to its normal working state. The open source time series database *influxDB* is used, with a retention time period of one hour. Data collection is performed using Phyton scripts (*pcapy* library in network sensors and VOLTTRON Katipamula et al. (2016) for physical censoring system). Artificial Neural Networks (ANN) based on the unsupervised Adaptative Resonance Theory are used for the recognition of normal and abnormal behaviour.

Abdulmunem et al. (2016) analyse a scenario of cyber-attacks on a BACS testbed, as a case study of how they might affect the system performance, using Intervention Mode Effects and Criticality Analysis (IMECA) and Failure Mode Effects and Analysis (FMEA). Markov models are used to calculate BACS availability considering the possibility of recovery and different kinds of faults.

Chowdhury proposed a framework named Expat (Chowdhury, 2019), which aims at protecting smart-home platforms from malicious automation apps. For this purpose, a platform-agnostic formal specification language is used to encode the users' expectation of the building automation behaviour, thus defining a set of policies which are later used to verify actions and validate app behaviour. This proposal was tested on OpenHAB, a representative platform used in home automation, as stated by the authors.

A multi-agent system named JMonA was proposed in Vasyutynskyy et al. (2006). It spreads agents across the various nodes of the BACS system, for enlarged monitoring. This framework was first tested in a LONworks laboratory setup, later using a network simulator and several control systems as a mockup of larger BACS. Moreover, the authors also identified a set of fundamental requirements for monitoring BACS systems, such as: independence from specific low-level data formats; support for heterogeneous hardware and software; and ability to meet the different real-time requirements of different diagnosis tasks; ability to filter collected data.

Xu et al. proposed a bloom-filter based analytic framework (Xu et al., 2016), which they used for to an extended analysis (over 18 months) of real-world home network traffic.

Liu et al. analysed the impact of net metering technology on detection of cyberattacks targeting smart home energy pricing (Liu et al., 2015). More specifically, the authors developed a smart home energy pricing cyberattack detection framework which integrates the net metering technology with short/long term detection (based on support vector regression).

The approach proposed by Pedro and Silva (2007) enables the development of generic monitoring and generic command of home automation facilities, independently of the underlying BACS technologies. This approach is based on DomoBus technology (Nunes, 2016), which through its device abstraction model and communications service allows the development of easily configurable applications from XML files. This enables monitoring and controlling device networks based on heterogeneous technologies. The main tests and results presented by the author were obtained in a testbed based on standard KNX components.

5.2. *Anomaly detection*

Zheng and Reddy developed *The Driven*, an anomaly detector for BACnet (Zheng and Reddy, 2017) that is able to detect suspicious traffic in BACS networks with a small rate of false alarms. A dataset of BACnet traffic was also created, using Wireshark to capture traffic traces with detailed data: timestamp, source and destination IP, port number, packet length, and data payload. *The Driven* uses different mechanisms, according to three different types of traffic (data):

- Time-driven Traffic – used to determine if a flow-service stream presents time regularity behaviour at different time scales, and which regularity patterns it follows.
- Human-driven Traffic – generated by operators from the server or workstation. It constitutes around 5 percent of the total BACnet traffic and does not present time regularity.
- Event-driven Traffic – triggered by other service messages or changes in the system. Similarly to human-driven traffic, it also presents no regular/periodic behaviour, and represents a small volume of overall traffic.

Authors concluded, from their analysis, that (i) aggregated BACnet traffic does not exhibit diurnal patterns nor look strictly periodic because it consists of time-driven messages with different periodic behaviour as well as non-periodic streams; and (ii) the non-periodic traffic includes human-driven and event-driven traffic.

Pan et al. (2014) also presented an anomaly detection system for BACnet. This is a rule-based system which is trained with data flows that are dynamically captured from a Fire Alarm System testbed. Rules are generated by applying an inductive-rule learning algorithm (RIPPER Cohen (1995)). Authors tested their system with a number of well-known attacks, and concluded their platform can detect attacks against the BACnet protocol with a low rate of false positives, but the used testbed is rather simplistic and the injected attacks are also straightforward, making it difficult to extrapolate achieved results to larger buildings or more sophisticated attacks.

Pan et al. (2016) present an anomaly based intrusion detection system (IDS) that monitors BACnet traffic to extract its features (e.g. packet flow amount, header, payload) in order to describe the behavior of BACS assets. More specifically, collected features are modeled into two types of data structures. Behavior analysis methods including Discrete Wavelets Transform (DWT) and rule based anomaly behaviour analysis are implemented for detecting anomaly behaviors. Finally, a rule based attack classification is performed to trigger proper counter measures.

An autoencoder neural network was used by Legrand et al. (2018) for anomaly detection in BACS. The key point of an autoencoder is the dimension reduction taking place in it. Over training, an autoencoder neural network learns to approximate two functions: the encoding function that execute the dimension reduction and compresses the data; and the decoding function that recreates an approximation of the original input (the output). In this paper, autoencoders are used to measure the distance between a set of input and output vectors, establishing a threshold for anomaly classification. The authors used the REFIT dataset (Firth et al., 2017) of smart home measurements to test several recurrent and convolutional models, having concluded that recurrent autoencoders appear to be the best candidates in the field of neural networks applied to the detection of anomalies in connected buildings. While results are interesting in the scope of anomaly detection in general, the nature of the REFIT dataset makes it difficult to extrapolate conclusions to the scope of cybersecurity.

5.3. *Intrusion detection systems*

The authors of Fauri et al. (2018) present an intrusion detection system (IDS) for BACS that detects known and unknown attacks, as well as anomalous behaviour. It does so by leveraging BACnet protocol knowledge and semantics. A BACnet parser is used to extract the relevant message fields from each message, in order to create a white-box model of the nominal system behaviour. Additionally, a human domain expert manually refined a collection of known BACnet threats into attack patterns. Once an attack is detected, the system generates enriched alerts that include semantic information helpful to the operators.

The use of active model discrimination with application to fraud detection in BACS is proposed by Harirchi et al. (2017). The active model discrimination problem aims to find optimal separating inputs that guarantee that the outputs of all the affine models cannot be identical over a finite horizon. This will enable a system operator to detect and uniquely identify potential faults or attacks, despite the presence of process and measurement noise.

Context aware and anomaly behaviour analysis IDS for BACS were discussed and presented in Pan et al. (2019). This paper describes an implementation of such an IDS, for a BACnet system, that involves five phases:

- Feature acquisition;

- Context modelling, based on BAS Context Aware Data Structure;
- Behaviour analysis;
- Threat assessment;
- And actions management.

In the first phase, features are selected and acquired from various BACS sources. During the second phase, the collected features are grouped and mapped into a well-defined behaviour context model named Protocol Context-Aware Data Structure. In the third phase, the runtime models are generated and compared with those that are associated with normal BACS operations, in order to detect any malicious behaviours that might have been triggered by attacks against the BACS network and its services. The model comparison is performed with respect to both security and functionality. In the last phase, the detected attacks are classified according to their mechanisms and asset targets. In addition, a threat level is calculated in order to quantify the attack severity and, consequently, determine the appropriate defensive actions.

A fully automated approach to deploy specification-based IDS at network level was implemented for BACnet by Esquivel-vargas et al. (2017). The creation of specifications often require human intervention, but this works proposes an automated approach supported by BACnet protocol where properly certified devices are demanded to have technical documentation stating their capabilities. The authors leverage on those documents to create specifications that represent the expected behaviour of each device in the network.

Rehman and Gruhn (2018) proposed a solution that has a firewall between the net/LAN and the Internet Service Provider (ISP), for protecting smart home and IoT environments. That firewall acts like a filter between the home appliances' interfaces and the Internet.

5.4. *BACS Improvements*

Shuai et al. (2019) propose an efficient and anonymous authentication schema for smart home environments, using Elliptic Curve Cryptography (ECC). Computational costs, communication overhead and energy consumption costs are evaluated in this paper.

Still in the field of improved authentication solutions for Smart Home and IoT environments, Li et al. proposed SecHome (Li et al., 2018), a large-scale home system using the Hierarchical Identity Based Encryption protocol (HIBE). When a homeowner begins defining a smart home, he/she issues a secret key to house members based on the house hierarchy. Then, when any house member buys a smart device, he or she issues a private key to connect that device to the private network. This private network communicates with the public cloud using encryption, making data confidential, and allowing remote control. To enable users to control and access smart home devices, proper hierarchy and authentication are required in addition to said encryption. The root of the hierarchy can control all devices. The lower levels only see and control the ones below them and the devices on the leafs, corresponding to their branches of the hierarchy.

Werner et al. (2018) discuss suitable access control mechanisms specifically tailored to Web-connected smart home platforms. Then, they present their experiences from implementing access control solutions meeting the identified requirements in OpenHAB.

A lightweight symmetric keychain encryption and authentication for BACS, to distribute and manage session keys between Human Machine Interfaces (HMI) and Programmable Logic Controllers (PLC), is proposed in Ng and Keoh (2018). A prototype was implemented using the BACnet/IP communication protocol. The schema facilitates automatic renewal of session keys, periodically, based on the use of a reversed hash-chain.

A pen testing approach for the assessment of a distributed Modbus-based BACS is proposed in Tenkanen and Hamalainen (2017). This approach is applied to data flow recognition and environment analysis. Methods for risk mitigation are also suggested by the authors.

The creation of an additional level of security to control authentication violation cases, beyond the traditional authentication method and based on the user's behaviour, is proposed in Rath (2017).

The addition of hardware-based node authentication, over TLS connections, was proposed in Fischer et al. (2017b). The use of identity-based signcryption for smart homes was addressed in Ashibani and Mahmoud (2017).

An alternative approach to BACS security is presented by Bondarev and Prokhorov (2017). Instead of focusing on communication patterns or specific intrusion vectors, the proposed approach is concerned about the robustness of process-level data (e.g., sensor feeds). For this purpose, parameter filtering techniques are applied, in order to safeguard systems from taking wrong actions based on faulty or maliciously injected data.

6. Open issues and research directions

A single BACS may have hundreds or even thousands of devices to monitor. Most of the available research works focus on exploring and adapting the existing knowledge from ICT and IACS areas (cf. Table Table 3), often without addressing the specific requirements of BACS. In general, the proposals reviewed in this paper reveal that the approach to BACS security is still in its infancy, especially when compared to more generalist ICT applications fields.

In general, a suitable BACS monitoring solution should include devices capable of collecting data and performing Deep Packer Inspection (DPI) of the BACS messages, at local level. Eventually, the design of an encompassing security solution for BACS may cover aspects ranging from specialized probes, such as domain-specific honeypots or traffic analysis devices to the creation of Security Information and Event Management (SIEM) solutions to acquire, aggregate and process collected evidence. There is also space for forensic capabilities, in order to create knowledge and enable the analysis of past events.

Regarding the detection of anomalies, BACS have a particularity when compared to other automation systems: the need to distinguish between traffic resulting from automated actions and events and traffic resulting from asynchronous human actions (e.g. a user enters a room). This increases the

Table 3 – Mapping of referred research works.

	IoT	Security			Abunaser and Alkhatib (2019); Waqar et al. (2017); Dutta and Wang (2018); Fischer et al. (2017a); Santos (2018)
		Architectural Solutions			Asadullah and Raza (2016); Bajer (2018); Darabseh and Freris (2019); Jia et al. (2019); Lilis et al. (2017); Minoli et al. (2017); Mocrii et al. (2018); Qiu et al. (2018)Ilieva et al. (2016); Ray (2017)
		Standards			ANSI (2010); BACNet (2020); EN/ISO (2016); KNX Association (2020); MODICON (1996); Toschi et al. (2017); Usman et al. (2019); EEBUS-Initiative (2019), Hersent et al. (2012); Seifried and Kastner (2017); Wendzel et al. (2018); Zhibo et al. (2017)
		Energy			Groote et al. (2017); Komninos et al. (2014); Rathinavel et al. (2017); Serrenho and Bertoldi (2019); EEBUS-Initiative (2019)
		Architectural Solutions			Bugeja et al. (2018); Butzin et al. (2017); Fatehah (2018); Li (2018); Vanus (2018); Zhibo et al. (2017)
		Security Analysis	Vulnerabilities		Brauchli and Li (2015); Brooks et al. (2017); Gai et al. (2018); Lei et al. (2018); Meyer et al. (2017); Valli et al. (2017)
			Attacks	Management	Zetter (2013)
				Automation	
				Network	Deng (2018); Hallman et al. (2017); Krishnan et al. (2017); Ling et al. (2017); Peterson (2019); Wright (2019)
				Protocol	Peacock et al. (2018); Gasser et al. (2017); Krishnan et al. (2017)
Building automation				Field Level	Molina (2015); Mundt and Wickboldt (2016)
	BACS			Other	Gai et al. (2018); Krebs on Security (2014); Lei et al. (2018); Levy (2015); Macaulay and Singer (2011); Saxena et al. (2017)
			Taxonomies		Anwar et al. (2017); Graveto et al. (2019); Heartfield et al. (2018); Liu et al. (2018)
		Safety			Brooks et al. (2017); Chhetri and Motti (2019); Han et al. (2018); Nicklas et al. (2016); Sutherland et al. (2015)
			Users Feedback		Kaaz et al. (2017); Lin and Parkin (2020); Pathmabandu et al. (2020); Zeng et al. (2017)
			Use cases		Franke et al. (2016); Mundt et al. (2012)
		Privacy	Data Analysis		Alisic et al. (2020); Xu and Agung Julius (2019)
			IoT Implementations		Gao et al. (2020); Iqbal et al. (2021); Samarah et al. (2017); Santo et al. (2017)
			Energy		Dasari et al. (2021); Finster and Baumgart (2015); Pham and Mansson (2019); Sarbhai et al. (2019); Wu et al. (2016)
			Other		George et al. (2020); Hamberger Carl; Eastman Clifford (1964); Kraemer and Flechais (2018)
			Monitoring		Abdulmunem et al. (2016); Chowdhury (2019); Liu et al. (2015); Minoli et al. (2017); Pedro and Silva (2007); Vasyutynskyy et al. (2006); Xu et al. (2016)
			Anomaly Detection		Legrand et al. (2018); Pan et al. (2014, 2016); Zheng and Reddy (2017)
		Contributions	IDS		Fauri et al. (2018); Esquivel-vargas et al. (2017); Harirchi et al. (2017); Pan et al. (2019); Rehman and Gruhn (2018)
			BACS Improvements		Werner et al. (2018); Fischer et al. (2017b); Li et al. (2018); Ng and Keoh (2018); Rath (2017); Seifried and Kastner (2017); Shuai et al. (2019); Tenkanen and Hamalainen (2017)Ashibani and Mahmoud (2017); Bondarev and Prokhorov (2017)
			Other		Demeure et al. (2016); Handa et al. (2019); Wang et al. (2017, 2015)
		Market			Brooks et al. (2017); Groote et al. (2017); Khedekar et al. (2016)

complexity of anomaly detection, especially for approaches based on the establishment of nominal reference operation models, something which some authors tried to address by using systems based on rules, auto-encoders, support vector machines and/or discrete wavelet transforms.

The intrusion detection systems found in the literature are mostly based on rule-based approaches allowing for the identification of attacks or abnormal functioning, such as deviations from the expected operational behaviour. The majority of presented examples are mostly based on small testbeds, not representative of real world scenarios.

Many of the analysed proposals address BACS security mainly by means of evolving the BACS protocols, which is not an acceptable solution for legacy equipment already existing facilities. A noteworthy exception is the work developed in Bondarev and Prokhorov (2017), which proposes a different approach to the problem, based on data and not on protocols, as a possible methodology to increase the robustness, security and effectiveness of BACS.

Most studies focus on management and automation levels, thus creating space for new directions of research focused on the field level. Presented examples deal with IP communications, leaving direct messages between devices to be explored. Those communications use local and specific networks that may vary from protocol to protocol.

At field level, where the interaction with the physical systems takes place, it should be possible to identify threats and anomalies. From this perspective, Single Board Computers (SBC), connected to the field level for monitoring purposes could act as Network Intrusion Detection System (NIDS) devices. Additionally, these devices could also be used to sniff the IP network, where the Management and Automation actions take place, to enrich the obtained information and add value to the overall security system.

Another general gap in this field relates with the absence of useful datasets, based on real testbeds and capable of supporting validation work. This translates in two needs:

- Obtaining datasets and making them available to the scientific community. These must contain communication captures at the various levels, but especially at the field level (since at the management and automation level some of the already existing network capture datasets can be used).
- Documentation and characterization of real environments and on-site data collection, including the various existing devices and implemented home automation functions as well as labeled datasets.

The absence of these elements is hampering and limiting the scope of research in this area. In order to address these limitations, it makes sense to develop appropriate capture mechanisms to enable extraction of field-level datasets.

The amount of data obtained with a probe directly connected to the field bus, and the packets collected through the network port, represent a large amount of valuable data. This points to the potential of using low-cost SBCs connected to the field bus to act as specialized probes able to capture and analyse field network traffic, for security purposes. While this approach may sound interesting from a cost/practicality perspective, one must take into account the limited computing capabilities of the hardware platforms, which may impose some design choices and/or compromises, namely:

- The construction of analysis models should happen during an initial learning phase, or the information might be sent to an external processing unit, with more capacity, to build the model and then import it back in the SBC-based probe;
- Data stream processing should be handled with a throughput compatible with a buffer at the scale of the SBC;
- The data lifecycle should be handled using tight rules, concerning local storage of data (due to the limited capacity of the probes) and longer-term storage in central locations, for deeper analysis or forensics.

With the identified challenges, a non-restrictive list of available anomaly detection techniques includes, for instance:

- Classification-based techniques, such as static neural networks, some of the support vector machine variants or rule-based methodologies, used in two steps to create a model and test during the evaluation phase;
- Clustering-based techniques, with the assumption that the clusters are computed on the initial learning phase;
- Statistical-based techniques, on which the stochastic model is pre-processed;
- Also, the use of Finite State Automata and Markov chains could provide good results, keeping the model definition off-path of the testing process.

7. Conclusion

The scope of the present survey intends to provide a comprehensive perspective on the BACS security and privacy landscape. From this analysis, it becomes apparent that the majority of the published research works are focused on the automation and management level of the BACS architecture, often considering the use of IP-based protocols at such levels. For such reasons, existing knowledge from ICT systems is frequently adapted and enhanced to overcome the differences, between BACS and ICT.

Due to the aforementioned reasons, the specific nature of field-level protocols and technologies is often overlooked. For BACS this also means that datasets are scarce, especially the ones containing BACS-specific protocol traces – something that constitutes a crucial limitation when it comes to foster further research and developments regarding BACS security.

Local tampering is a reality and lots of threats exist at the field level. Thus, safety and security measures should encompass this level, which opens up a wide area of future research. In addition, all information collected at local level, at several points of the field network, can be sent to centralized and more robust systems for detecting anomalies or attacks, thus increasing the detection probability in complex BACS, using more powerful systems.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Vitor Graveto: Conceptualization, Methodology, Investigation, Data curation, Writing – original draft, Writing – review & editing. **Tiago Cruz:** Conceptualization, Methodology, Investigation, Writing – review & editing, Supervision, Funding acquisition. **Paulo Simões:** Conceptualization, Methodology, Investigation, Writing – review & editing, Supervision, Funding acquisition.

Acknowledgement

This work was co-funded by FEDER - Competitiveness and Internationalization Operational Program (COMPETE 2020), Portugal 2020 framework. Project Smart5Grid (POCI-01-0247-FEDER-047226).

REFERENCES

Abdulmunem A-sMQ, Al-khafaji AW, Kharchenko VS. THE METHOD OF IMECA-BASED SECURITY ASSESSMENT : Case study for buildind automation system. EU ERASMUS+ Project: Internet of Things: Emerging Curriculum for Industry and Human Applications (ALIOT) 2016;1(138). doi:10.11610/isij.3505.

Abunaser M, Alkhatib AAA. Advanced survey of blockchain for the internet of things smart home. 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT) 2019:58–62. doi:10.1109/JEEIT.2019.8717441.

Alisic R, Molinari M, Pare PE, Sandberg H. Ensuring privacy of occupancy changes in smart buildings. CCTA 2020 - 4th IEEE Conference on Control Technology and Applications 2020:871–6. doi:10.1109/CCTA41146.2020.9206317.

Amazon, 2014. Amazon Alexa.

ANSI, 2010. Smart Grid Standards Information Section I : Use and Application of the Standard Section I : Use and Application of the Standard.

ANSI/CEA. Smart grid standards information section i : use and application of the standard. Power Engineering 2010:1–12.

Anwar MN, Nazir M, Mustafa K. Security threats taxonomy : smart-Home perspective. 2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall) 2017. doi:10.1109/ICACCAF.2017.8344666.

Asadullah M, Raza A. An overview of home automation systems. 2016 2nd International Conference on Robotics and Artificial Intelligence (ICRAI) 2016:27–31. doi:10.1109/ICRAI.2016.7791223.

Ashibani Y, Mahmoud QH. An efficient and secure scheme for smart home communication using identity-Based signcryption. 2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC) 2017. doi:10.1109/PCCC.2017.8280497.

ASHRAE, 2016. ANSI/ASHRAE 135 - A Data Communication Protocol for Building Automation and Control Networks. https://www.ashrae.org/technical-resources/standards-and-guidelines/standards-addenda/standard-135-2016-bacnet-a-data-communication-protocol/-for-building-automation-and-control-networks.

BACNet, 2020. BACnet. http://www.bacnet.org.

Bajer M. IoT For smart buildings - long awaited revolution or lean evolution. 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud) 2018:149–54. doi:10.1109/FiCloud.2018.00029.

Bondarev SE, Prokhorov AS. Analysis of internal threats of the system " smart home " and assessment of ways to prevent them. 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) 2017:788–90. doi:10.1109/EIConRus.2017.7910676.

Brauchli A, Li D. A solution based analysis of attack vectors on smart home systems. 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC) 2015. doi:10.1109/SSIC.2015.7245682.

Brooks DJ, Coole M, Haskell-Dowland P, Griffiths M, Lockhart N. In: Technical Report. Building Automation & Control Systems: An Investigation into Vulnerabilities, Current Practice & Security Management Best Practice. ASIS Foundation; 2017. https://goo.gl/RM7ukP.

Bugeja J, Jacobsson A, Davidsson P. Smart Connected Homes. In: Internet ofThings A to Z: Technologies and Applications; 2018. p. 359–84.

Building Energy Management Open Source, 2019. BEMOSS FEATURES.

Butzin B, Golatowski F, Timmermann PD. A survey on information modeling and ontologies in building automation. IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society 2017. doi:10.1109/IECON.2017.8217514.

CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids, 2012. CEN-CENELEC-ETSI Smart Grid Coordination Group: Smart Grid Information Security(November),1–107, ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Security.pdf.

CENELEC, 2012a. EN 13321 - Open Data Communication in Building Automation, Controls and Building Management - Home and Building Electronic Systems solution. https://joinup.ec.europa.eu/solution/en-13321-12012-open-data-communication-building-//automation-controls-and-building-management-home-and/releases.

CENELEC, 2012b. EN50090 - Home and Building Electronic Systems (HBES). https://ec.europa.eu/eip/ageing/standards/home/domotics-and-home-automation/en-50090_en.

Chhetri C, Motti VG. Eliciting privacy concerns for smart home devices from a user centered perspective. Springer International Publishing; 2019. doi:10.1007/978-3-030-15742-5.

China Machinery Industry Federation,. GB/T 20965 - Control network HBES technical specification. Home and building control system. https://www.chinesestandard.net/PDF/English.aspx/GBT20965-2013.

Chowdhury O. Expat : expectation-based policy analysis and enforcement for appified smart-Home platforms. SACMAT '19 Proceedings of the 24th ACM Symposium on Access Control Models and Technologies 2019:61–72. doi:10.1145/3322431.3325107.

Ciholas P, Lennie A, Sadigova P, Such JM. The Security of Smart Buildings: A Systematic Literature Review; 2019. p. 1–50. http://arxiv.org/abs/1901.05837.

Cohen WH. Fast effective rule induction. Proceedings of the Twelfth International Conference on International Conference on Machine Learning (ICML'95) 1995:115–23. doi:10.5555/3091622.3091637.

Connectivity Standars Alliance, 2021. Zigbee. https://zigbeealliance.org/solution/zigbee/.

Coppolino L, Alessandro VD, Antonio SD, Lev L, Romano L. My smart home is under attack. 2015 IEEE 18th International Conference on Computational Science and Engineering 2015:145–51. doi:10.1109/CSE.2015.28.

Darabseh A, Freris NM. A software-defined architecture for control of IoT cyberphysical systems prominent applications enlist intelligent transportation. Cluster Comput 2019;8. doi:10.1007/s10586-018-02889-8. 10.1007/s10586-018-02889-8

Dasari SV, Mittal K, Sasirekha GV, Bapat J, Das D. Privacy enhanced energy prediction in smart building using federated learning. 2021 IEEE International IOT, Electronics and Mechatronics Conference, IEMTRONICS 2021 - Proceedings 2021:0–5. doi:10.1109/IEMTRONICS52119.2021.9422544.

Demeure A, Caffiau S, Elias E, Roux C, Demeure A, Caffiau S, Elias E, Building CR, Home U, Systems A, Study AF. Building and using home automation systems : A Field study. ISEUD 2015 2016.

Deng, I., 2018. Tencent engineer slapped with fine for hacking hotel Wi-fi in Singapore. https://www.scmp.com/tech/enterprises/article/2165855/tencent-engineer-slapped-fine-hacking-hotel-wi-fi-singapore.

digitalSTROM AG, 2019. Smart Home by digitalSTROM: A home of unlimited possibilities. https://www.digitalstrom.com/en/your-smart-home/#automation.

Domingues P, Carreira P, Vieira R, Kastner W. Computer standards & interfaces building automation systems : concepts and technology review. Computer Standards & Interfaces 2016;45:1–12. doi:10.1016/j.csi.2015.11.005.

Dutta J, Wang Y. ES3B : enhanced security system for smart building using IoT. 2018 IEEE International Conference on Smart Cloud (SmartCloud) 2018. doi:10.1109/SmartCloud.2018.00034.

EIBA, 2020. European installation Bus Association.

EN/ISO, 2016. EN ISO 16484 - Building Automation and Control Systems. https://ec.europa.eu/eip/ageing/standards/home/domotics-and-home-automation/en-iso-16484_en.

EnOcean GmbH, 2020. EnOcean. https://www.enocean.com/en/technology/.

Esquivel-vargas H, Caselli M, Peter A. Automatic deployment of specification-based intrusion detection in the BACnet protocol. CPS-SPC@CCS 2017:25–36. doi:10.1145/3140241.3140244.

Fatehah M. Design and process metamodels for modelling and verification of safety-Related software applications in smart building systems. ICIT 2018 Proceedings of the 6th International Conference on Information Technology: IoT and Smart City 2018:60–4. doi:10.1145/3301551.3301577.

Fauri D, Kapsalakis M, Ricardo D, Costante E, Hartog JD, Etalle S. Leveraging semantics for actionable intrusion detection in building automation systems. 13th International Conference on Critical Information Infrastructures Security (CRITIS) 2018;1(700665):113–25. doi:10.1007/978-3-030-05849-4.

Finster S, Baumgart I. Privacy-aware smart metering: a survey. IEEE Commun. Surv. Tutorials 2015;17(2):1088–101. doi:10.1109/COMST.2015.2425958.

Firth, S., Kane, T., Dimitriou, V., Hassan, T., Fouchal, F., Coleman, M., Webb, L., 2017. REFIT Smart Home dataset. https://figshare.com/articles/REFITSmartHomedataset/2070091.

Fischer R, Lamshöft K, Dittmann J, Vielhauer C. Advanced issues in wireless communication security: towards a security-Demonstrator for smart-Home environments. 2017 International Carnahan Conference on Security Technology (ICCST) 2017. doi:10.1109/CCST.2017.8167864.

Fischer T, Lesjak C, Hoeller A, Steger C. Security for building automation with hardware-Based node authentication. 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA) 2017. doi:10.1109/ETFA.2017.8247567.

Franke, S., Hermann, A., Junghans, S., Leonhardt, S., Neumann, T., Teich, T., Trommer, M., 2016. Event-Driven and District-Related Home Care. 10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.60

Gai A, Azam S, Shanmugam B, Jonkman M, Boer FD. Categorisation of security threats for smart home appliances. 2018 International Conference on Computer Communication and Informatics (ICCCI) 2018. doi:10.1109/ICCCI.2018.8441213.

Gao X, Li K, Chen W, Hu W, Zhang Z, Li Q. Efficient and privacy-Preserving speaker verification scheme for home automation devices. Proceedings - 3rd International Conference on Multimedia Information Processing and Retrieval, MIPR 2020 2020(1):237–40. doi:10.1109/MIPR49039.2020.00056.

Garg, P., Kohnfelder, L., 1999. STRIDE (security). https://en.wikipedia.org/wiki/STRIDE_(security).

Gasser O, Scheitle Q, Denis C, Schricker N, Carle G. Security implications of publicly reachable building automation systems. 2017 IEEE Security and Privacy Workshops (SPW) 2017. doi:10.1109/SPW.2017.13.

George CG, Tyranski DR, Simons DP, O'Quinn JD, York ER, Salman AA. Integrating social and technical solutions to address privacy in smart homes. 2020 Systems and Information Engineering Design Symposium, SIEDS 2020 2020. doi:10.1109/SIEDS49339.2020.9106585.

Google, 2016. Google Home Assistent. https://assistant.google.com.

Goossens, M., 1998. The EIB System for Home & Building Electronics.

Granjal J, Monteiro E, Sá Silva J. Security for the internet of things: A Survey of existing protocols and open research issues. IEEE Communications Surveys Tutorials 2015;17(3):1294–312. doi:10.1109/COMST.2015.2388550.

Granzer W, Praus F, Kastner W. Security in building automation systems. IEEE Trans. Ind. Electron. 2010;57(11):3622–30. doi:10.1109/TIE.2009.2036033.

Graveto V, Rosa L, Cruz T, Simes P. A stealth monitoring mechanism for cyber-physical systems. Int. J. Crit. Infrastruct. Prot. 2019;24:126–43. doi:10.1016/j.ijcip.2018.10.006. 10.1016/j.ijcip.2018.10.006

Groote MD, Volt J, Bean F. IS EUROPE READY FOR THE SMART BUILDINGS REVOLUTION ?. Buildings Performance Institute Europe; 2017.

Hallak G, Bumiller G. Power Line Communications: Principles, Standards and Applications from Multimedia to Smart Grid. In: Lampe L, Tonello AM, Swart TG, editors. PLC for Home and Indystry Automation. John Wiley & Sons, Ltd.; 2016.

Hallman R, Bryan J, Palavicini G, Divita J, Romero-mariona J. Ioddos the internet of distributed denial of service attacks : A Case study of the mirai malware and IoT-Based botnets. 2nd International Conference on Internet of Things, Big Data and Security 2017(November 2018). doi:10.5220/0006246600470058.

Hamberger Carl; Eastman Clifford, 1964. CARL H. HAMBERGER & a. v. CLIFFORD C. EASTMAN.https://law.justia.com/cases/new-hampshire/supreme-court/1964/5258-0.html.

Han SHI, Zhang D, Lin S, Li X. Systematically ensuring the confidence of real-Time home automation IoT systems. ACM Transactions on Cyber-Physical Systems 2018;2(3).

Handa A, Sharma A, Shukla SK. Machine learning in cybersecurity : a review. WIREs Data Min. Knowl. Discovery 2019(December 2018):1–7. doi:10.1002/widm.1306.

Harirchi F, Yong SZ, Arbor A, Royal KTH. Active model discrimination with active model applications to fraud detection in smart buildings. IFAC-PapersOnLine 2017;50(1):9527–34. doi:10.1016/j.ifacol.2017.08.1616. 10.1016/j.ifacol.2017.08.1616

Heartfield R, Loukas G, Budimir S, Bezemskij A, Fontaine JRJ, Filippoupolitis A, Roesch E. A taxonomy of cyber-physical

threats and impact in the smart home. Computers & Security 2018;78:398–428. doi:10.1016/j.cose.2018.07.011. 10.1016/j.cose.2018.07.011

Hersent O, Boswarthick D, Elloumi O. In: The Internet of Things: Key Applications and Protocols. Legacy M2M Protocols for Sensor Networks, Building Automation and Home Automation - the BACnet Protocol; 2012.

Hui TKL, Sherratt RS, Sánchez DD. Major requirements for building smart homes in smart cities based on internet of things technologies. Future Generation Computer Systems 2017;76:358–69. doi:10.1016/j.future.2016.10.026.

Ilieva S, Penchev A, Petrova-antonova D. Internet of things framework for smart home building. International Conference on Digital Transformation and Global Society 2016:450–62. doi:10.1007/978-3-319-49700-6.

ISO/IEC, 2006. ISO/IEC 14543 - technology - Home electronic system (HES) architecture. https://ec.europa.eu/eip/ageing/standards/home/domotics-and-home-automation/isoiec-14543_en.

Iqbal W, Abbas H, Rauf B, Abbas Y, Amjad F, Hemani A. PCSS: Privacy preserving communication scheme for SDN enabled smart homes. IEEE Sens J 2021(c):1–13. doi:10.1109/JSEN.2021.3087779.

Jia M, Komeily A, Wang Y, Srinivasan RS. Adopting internet of things for the development of smart buildings : a review of enabling technologies and applications. Autom. Constr. 2019;101(February):111–26. doi:10.1016/j.autcon.2019.01.023.

Jia X, Li X, Gao Y. A novel semi-Automatic vulnerability detection system for smart home. the International Conference 2017:195–9. doi:10.1145/3175684.3175718.

Jones CB, Carter C, Thomas Z. Intrusion detection & response using an unsupervised artificial neural network on a single board computer for building control resilience. 2018 Resilience Week (RWS) 2018(Section II):31–7. doi:10.1109/RWEEK.2018.8473533.

Kaaz KJ, Hoffer A, Saeidi M, Sarma A, Bobba RB. Understanding user perceptions of privacy, and configuration challenges in home automation. Proceedings of IEEE Symposium on Visual Languages and Human-Centric Computing, VL/HCC 2017;2017-October:297–301. doi:10.1109/VLHCC.2017.8103482.

Katipamula S, Haack J, Hernandez G, Akyol B, Hagerman J. Volttron: an open-source software platform of the future. IEEE Electrif. Mag. 2016;4:15–22. doi:10.1109/MELE.2016.2614178.

Khedekar, D. C., Oteyza, D. A., Truco, A. C., Huertas, G. F., 2016. Home Automation A Fast - Expanding Market. 10.1002/tie.21829

KNX Association, 2020. KNX. https://www.knx.org.

Kogler, M., 2011. BCU SDK - EIBD. https://www.auto.tuwien.ac.at/~mkoegler/index.php/eibd.

Komninos N, Philippou E, Pitsillides A, Member S. Survey in smart grid and smart home security : issues, challenges and countermeasures. IEEE Communications Surveys & Tutorials 2014;16(4):1933–54. doi:10.1109/COMST.2014.2320093.

Kraemer MJ, Flechais I. Researching privacy in smart homes: a roadmap of future directions and research methods. IET Conference Publications 2018;2018(CP740):1–10. doi:10.1049/cp.2018.0038.

Krebs on Security, 2014. Target Hackers Broke in Via HVAC Company.

Krishnan S, Anjana MS, Rao SN. Security considerations for IoT in smart buildings. 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC) 2017. doi:10.1109/ICCIC.2017.8524450.

Legrand A, Niepceron B, Cournier A, Trannois H. Study of autoencoder neural networks for anomaly detection in connected buildings. 2018 IEEE Global Conference on Internet of Things (GCIoT) 2018. doi:10.1109/GCIoT.2018.8620158.

Lei X, Tu G-h, Liu AX, Li C-y, Xie T. The insecurity of home digital voice assistants vulnerabilities, attacks and countermeasures. 2018 IEEE Conference on Communications and Network Security (CNS) 2018. doi:10.1109/CNS.2018.8433167.

Levy, H. P., 2015. Gartner Predicts Our Digital Future. http://goo.gl/3AyTvo.

Li Y. Design of smart home cloud server. 2018 IEEE International Conference of Safety Produce Informatization (IICSPI) 2018:200–3. doi:10.1109/IICSPI.2018.8690355.

Li Y, B YW, Zhang Y. Sechome : A Secure large-Scale smart home system using hierarchical identity. International Conference on Information and Communications Security 2018;1:339–51. doi:10.1007/978-3-319-89500-0.

Lilis G, Conus G, Asadi N, Kayal M. Towards the next generation of intelligent building : an assessment study of current automation and future IoT based systems with a proposal for transitional design. Sustainable Cities and Society 2017;28:473–81. doi:10.1016/j.scs.2016.08.019.

Lin VZ, Parkin S. Transferability of privacy-related behaviours to shared smart home assistant devices. 2020 7th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2020 2020. doi:10.1109/IOTSMS52051.2020.9340199.

Ling Z, Luo J, Xu Y, Gao C, Wu K, Member S, Fu X. Security vulnerabilities of internet of things : acase study of the smart plug system. IEEE Internet Things J. 2017;4(6):1899–909. doi:10.1109/JIOT.2017.2707465.

Liu Y, Hu S, Wu J, Shi Y, Jin Y, Hu Y, Li X. Impact assessment of net metering on smart home cyberattack detection. 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC) 2015. doi:10.1145/2744769.2747930.

Liu Y, Pang Z, Lan D, Gong S. A taxonomy for the security assessment of IP-Based building automation systems : the case of thread. IEEE Trans. Ind. Inf. 2018;14(9):4113–23. doi:10.1109/TII.2018.2844955.

Lobaccaro, G., Carlucci, S., Lofstrom, E., 2016. A Review of Systems and Technologies for Smart Homes and Smart Grids. 10.3390/en9050348

Macaulay T, Singer B. Cybersecurity for industrial control systems. CRC Press; 2011.

Meyer D, Haase J, Eckert M, Klauer B. New attack vectors for building automation and IoT. IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society 2017. doi:10.1109/IECON.2017.8217426.

Minoli D, Sohraby K, Occhiogrosso B. IoT Considerations, requirements, and architectures for smart buildings energy building management systems. IEEE Internet Things J. 2017;4(1):269–83. doi:10.1109/JIOT.2017.2647881.

Mocrii D, Chen Y, Musilek P. Internet of things IoT-based smart homes : a review of system architecture, software, communications, privacy and security. Internet of Things 2018;1–2:81–98. doi:10.1016/j.iot.2018.08.009. 10.1016/j.iot.2018.08.009

MODICON. In: Technical Report. Modicon Modbus Protocol Reference Guide. MODICON, Inc., Industrial Automation Systems; 1996. http://www.modbus.org/docs/PI_MBUS_300.pdf.

Molina, J., 2015. Learn how to control every room at a luxury hotel remotely. https://www.youtube.com/watch?v=RX-O4XuCW1Y.

Mundt T, Kruger F, Wollenberg T. Who refuses to wash hands? privacy issues in modern house installation networks. Proceedings - 2012 7th International Conference on Broadband, Wireless Computing, Communication and Applications, BWCCA 2012 2012:271–7. doi:10.1109/BWCCA.2012.51.

Mundt T, Wickboldt P. Security in building automation systems - A first analysis. 2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security) 2016:1–8. doi:10.1109/CyberSecPODS.2016.7502336.

Ng J, Keoh SL. SEABASS : Symmetric-keychain encryption and authentication for building automation systems. 2018 IEEE

4th World Forum on Internet of Things (WF-IoT) 2018:219–24. doi:10.1109/WF-IoT.2018.8355106.
Nicklas J-p, Mamrot M, Winzer P, Lichte D, Marchlewitz S, Wolf K-d. Use case based approach for an integrated consideration of safety and security aspects for smart home applications. 2016 11th System of Systems Engineering Conference (SoSE) 2016. doi:10.1109/SYSOSE.2016.7542908.
Novak T, Gerstinger A. Safety- and security-Critical services in building automation and control systems. IEEE Trans. Ind. Electron. 2010;57(11):3614–21. doi:10.1109/TIE.2009.2028364.
Nunes R. DomoBus. Technical University of Lisbon; 2016.
Pan Z, Hariri S, Hall K. Anomaly based intrusion detection for building automation and control networks youssif al-Nashif. 2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA) 2014:72–7. doi:10.1109/AICCSA.2014.7073181.
Pan Z, Hariri S, Pacheco J. Context aware intrusion detection for building automation systems. Computers & Security 2019;85:181–201. doi:10.1016/j.cose.2019.04.011. 10.1016/j.cose.2019.04.011
Pan Z, Pacheco J, Hariri S. Anomaly behavior analysis for building automation systems. 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA) 2016. doi:10.1109/AICCSA.2016.7945692.
Pathmabandu C, Grundy J, Chhetri MB, Baig Z. An informed consent model for managing the privacy paradox in smart buildings. Proceedings - 2020 35th IEEE/ACM International Conference on Automated Software Engineering Workshops, ASEW 2020 2020:19–26. doi:10.1145/3417113.3422180.
Peacock M, Johnstone MN, Valli C. An exploration of some security issues within the BACnet protocol. International Conference on Information Systems Security and Privacy 2018:252–72. doi:10.1007/978-3-319-93354-2.
Pedro J, Silva S. Aplicação de interface com sistema domótico EIB engenharia informática e de computadores. Master tesis 2007.
Peterson, E., 2019. Mirai Nikki: The Future of DDoS.
Pham CT, Mansson D. A study on realistic energy storage systems for the privacy of smart meter readings of residential users. IEEE Access 2019;7:150262–70. doi:10.1109/ACCESS.2019.2946027.
Praus F, Kastner W. Identifying unsecured building automation installations. Proceedings of the 2014 IEEE Emerging Technology and Factory Automation (ETFA) 2014:1–4. doi:10.1109/ETFA.2014.7005301.
Praus F, Kastner W, Palensky P. Software security requirements in building automation. 2010IEEE Transactions on Industrial Electronics 2016. doi:10.1109/TIE.2009.2036033.
Qiu T, Member S, Chen N, Li K, Member S, Atiquzzaman M, Member S, Zhao W, Member S. How can heterogeneous internet of things build our future : A Survey. IEEE Communications Surveys & Tutorials 2018;20(3):2011–27. doi:10.1109/COMST.2018.2803740.
Rath AT. Strengthening access control in case of compromised accounts in smart home. 2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) 2017:1–8. doi:10.1109/WiMOB.2017.8115827.
Rathinavel K, Pipattanasomporn M, Kuzlu M, Rahman S. Security concers and countermeasures in IoT-Integrated smart buildings. 2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT) 2017. doi:10.1109/ISGT.2017.8086057.
Ray AK. Study of smart home communication protocol ' s and security & privacy aspects. 2017 7th International Conference on Communication Systems and Network Technologies (CSNT) 2017. doi:10.1109/CSNT.2017.46.
Rehman S, Gruhn V. An approach to secure smart homes in cyber- Physical systems / internet-of-Things. 2018 Fifth International Conference on Software Defined Systems (SDS) 2018:126–9. doi:10.1109/SDS.2018.8370433.
Samarah S, Al Zamil MG, Aleroud AF, Rawashdeh M, Alhamid MF, Alamri A. An efficient activity recognition framework: toward privacy-Sensitive health data sensing. IEEE Access 2017;5:3848–59. doi:10.1109/ACCESS.2017.2685531.
Santo H, Maekawa T, Matsushita Y. Device-free and privacy preserving indoor positioning using infrared retro-reflection imaging. 2017 IEEE International Conference on Pervasive Computing and Communications, PerCom 2017 2017:141–52. doi:10.1109/PERCOM.2017.7917860.
Santos L. Intrusion detection systems in internet of things aliterature review. 2018 13th Iberian Conference on Information Systems and Technologies (CISTI) 2018. doi:10.23919/CISTI.2018.8399291.
Sarbhai A, Merwe JVD, Kasera S. Privacy-Aware peak load reduction in smart homes. 2019 11th International Conference on Communication Systems and Networks, COMSNETS 2019 2019;2061:312–19. doi:10.1109/COMSNETS.2019.8711168.
Saxena U, Sidhi JS, Singh Y. Analysis of security attacks in a smart home networks. 2017 7th International Conference on Cloud Computing, Data Science & Engineering - Confluence 2017:431–6. doi:10.1109/CONFLUENCE.2017.7943189.
Seifried S, Kastner W. KNX IPv6 : Design issues and proposed architecture. 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS) 2017. doi:10.1109/WFCS.2017.7991951.
Serrenho T, Bertoldi P. Smart home and appliances : State of the art. Luxembourg: Publications Office of the European Union; 2019. doi:10.2760/453301.
Shuai M, Yu N, Wang H, Xiong L. Anonymous authentication scheme for smart home environment with provable security. Computers & Security 2019;86:132–46. doi:10.1016/j.cose.2019.06.002. 10.1016/j.cose.2019.06.002
Sutherland I, Spyridopoulos T, Read H, Jones A. Applying the ACPO guidelines to building automation systems. Proceedings of the Third International Conference on Human Aspects of Information Security, Privacy, and Trust 2015;1:684–92. doi:10.1007/978-3-319-20376-8.
Tenkanen T, Hamalainen T. Security assessment of a distributed, modbus-based building automation system. 2017 IEEE International Conference on Computer and Information Technology (CIT) 2017. doi:10.1109/CIT.2017.38.
Thread Group, 2019. THREAD CERTIFIED PRODUCTS. https://www.threadgroup.org/what-Is-thread.
Toschi GM, Campos LB, Cugnasca CE. Home automation networks : a survey. Computer Standards & Interfaces 2017;50(September 2016):42–54. doi:10.1016/j.csi.2016.08.008.
Usman M, Ali I, Khan S, Khurram M. Journal of network and computer applications asurvey on software defined networking enabled smart buildings : architecture, challenges and use cases. Journal of Network and Computer Applications 2019;137(November 2018):62–77. doi:10.1016/j.jnca.2019.04.002. 10.1016/j.jnca.2019.04.002
Valli C, Johnstone MN, Peacock M, Jones A. BACnet - Bridging The cyber physical divide one HVAC at a time. 2017 9th IEEE-GCC Conference and Exhibition (GCCCE) 2017. doi:10.1109/IEEEGCC.2017.8448236.
Vanus J. Sciencedirect of home implementation design of home implementation design of home implementation design of home implementation within IoT with natural language within IoT with natural language design of home implementation within IoT with natural language. IFAC-PapersOnLine 2018;51(6):174–9. doi:10.1016/j.ifacol.2018.07.149. 10.1016/j.ifacol.2018.07.149
Vasyutynskyy V, Ploennigs J, Kabitzsch K. MULTI-AGENT SYSTEM FOR MONITORING OF BUILDING AUTOMATION SYSTEMS, Vol. 40. IFAC; 2006. doi:10.3182/20071107-3-FR-3907.00045.

Vikram N, Harish KS, Nihaal MS, Umesh R, Aashik S, Kumar A. A low cost home automation system using wi-Fi based wireless sensor network incorporating internet of things (IoT). 2017 IEEE 7th International Advance Computing Conference (IACC) 2017;100. doi:10.1109/IACC.2017.40.

Wang X, Habeeb R, Ou X, Amaravadi S, Hatcliff J, Mizuno M, Neilsen M, Rajagopalan SR, Varadarajan S. Enhanced security of building automation systems through microkernel-Based controller platforms. 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW) 2017:37–44. doi:10.1109/ICDCSW.2017.25.

Wang X, Neilsen M, Rajagopalan SR, Baldwin WG, Phillips B. Secure RTOS architecture for building automation categories and subject descriptors. CPS-SPC@CCS 2015:79–90. doi:10.1145/2808705.2808709.

Waqar A, Dustgeer G, Awais M, Shah MA. IoT Based smart home : security challenges, security requirements and solutions. 2017 23rd International Conference on Automation and Computing (ICAC) 2017(September):7–8. doi:10.23919/IConAC.2017.8082057.

Wendzel S, Tonejc J, Kaur J, Kobekova A. In: Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications. Cyber Security of Smart Buildings; 2018.

Wright, R., 2019. FBI: How we stopped the Mirai botnet attacks. https://searchsecurity.techtarget.com/news/252459016/FBI-How-we-stopped-the-Mirai-botnet-attacks.

Werner S, Pallas F, Bermbach D. Designing suitable acess control for web-Connected smart home platforms. International Conference on Service-Oriented Computing 2018:240–51. doi:10.1007/978-3-319-91764-1.

Wu J, Liu J, Hu XS, Shi Y. Privacy protection via appliance scheduling in smart homes. IEEE/ACM International Conference on Computer-Aided Design, Digest of Technical Papers, ICCAD 2016;07-10-November-2016. doi:10.1145/2966986.2980089.

Xu K, Wang F, Jia X. Secure the internet, one home at a time. Security and Communication Networks 2016(July):3821–32. doi:10.1002/sec.1569.

Xu Z, Agung Julius A. Robust temporal logic inference for provably correct fault detection and privacy preservation of switched systems. IEEE Syst. J. 2019;13(3):3010–21. doi:10.1109/JSYST.2019.2906160.

Zeng E, Mare S, Roesner F, Clara S, Zeng E, Mare S, Roesner F. End user security and privacy concerns with smart homes this paper is included in the proceedings of the end user security & privacy concerns with smart homes. Thirteenth Symposium on Usable Privacy and Security (SOUPS) 2017(Soups):65–80.

Zetter, K., 2013. Researchers Hack Building Control System at Google Australia Office.

Zheng Z, Reddy ALN. Safeguarding building automation networks : THE-Driven anomaly detector based on traffic analysis. 2017 26th International Conference on Computer Communication and Networks (ICCCN) 2017. doi:10.1109/ICCCN.2017.8038393.

Zhibo P, Bag G, Ngai E, Leung V. [Invited Paper] Native IP connectivity for sensors and actuators in home area network. Smart Grid Inspired Future Technologies 2017;2:222–31. doi:10.1007/978-3-319-47729-9.

EEBUS-Initiative, 2019. EEBUS. https://www.eebus.org/en/.

Vitor Graveto is a Ph.D. student at the department of informatics engineering of the University of Coimbra (Coimbra, Portugal). Previously, he completed his BSc (1989) and Master's degree in Civil Engineering (1999), as well as a BSc in Informatics Engineering (2013), in the same University. His main research interests include areas such as building automation and control systems, building management systems, cyber-physical systems security and cybersecurity for critical infrastructures.

Tiago Cruz received his Ph.D. degree in informatics engineering from the University of Coimbra (Coimbra, Portugal), in 2012. He has been an Assistant Professor in the Department of Informatics Engineering, University of Coimbra, since December 2013. His research interests include areas such as management systems for communications infrastructures and services, critical infrastructure security, broadband access network device and service management, Internet of Things, software-defined networking, and network function virtualization (among others). He is the author of more than 80 publications, including chapters in books, journal articles, and conference papers. Dr. Cruz is a senior member of the IEEE Communications Society.

Paulo Simões Paulo Simões received the Doctoral degree in informatics engineering from the University of Coimbra (Coimbra, Portugal), in 2002. He is an Associate Professor in the Department of Informatics Engineering, Univer- sity of Coimbra, where he regularly leads technology transfer projects for industry partners such as telecommunications operators and energy utilities. His research interests include network and infrastructure management, security, critical infrastructure protection, and virtualization of networking and computing resources. He has more than 150 publications in refereed journals and conferences. Dr. Simões is a senior member of the IEEE Communications Society.