Cybersecurity Perspectives for Smart Building Automation Systems

Grigore Stamatescu
Department of Automation and Industrial Informatics
University Politehnica of Bucharest
Bucharest, Romania
grigore.stamatescu@upb.ro

Iulia Stamatescu
Department of Automation and Industrial Informatics
University Politehnica of Bucharest
Bucharest, Romania
iulia.stamatescu@upb.ro

Nicoleta Arghira
Department of Automation and Industrial Informatics
University Politehnica of Bucharest
Bucharest, Romania
nicoleta.arghira@upb.ro

Ioana Făgărășan
Department of Automation and Industrial Informatics
University Politehnica of Bucharest
Bucharest, Romania
ioana.fagarasan@upb.ro

Abstract— **As the built environment becomes the hallmark of urbanisation tendencies worldwide, people have come to rely on buildings for a large majority of their daily activities. Modern buildings are equipped with new sensor technologies and advanced controllers, integrated through communication interfaces and application software to handle various required functions through automation. This is partially extended to legacy buildings through retrofitting. Integration of these new technologies opens up the automation system of the building to internal and external attackers. The challenges related to cybersecurity identified are partially similar to the industrial control system domain while adding specific constraints for the built environment as compared to a production/manufacturing environment, which relate to human safety, security and privacy aspects. We provide a critical overview of cybersecurity challenges for smart building automation systems by focusing on key areas of development at the device, system and communication and interoperability levels. A representative example for BACnet protocol features and tools is provided.**

Keywords—smart building, automation, cybersecurity, intrusion detection systems, BACnet

I. Introduction

Cyber-physical energy systems (CPES) mark the integration of computing, communication, control and cognition in the energy domain. These assume the growing role of the new technologies for efficient and environmentally friendly operation. Buildings are considered a key part of CPES for the role they play as large, individual or aggregated, consumers, local distributed energy resources and grid integration for demand response and peak shaving functions [1]. As buildings become increasingly connected, both internally and externally, the role of cybersecurity increases as multiple components and services become exposed and vulnerable to attackers. Potential risks can lead to devastating outcomes for human lives and economic consequences e.g. altering program control logic impeding the release valve of a steam boiler which results in an explosion.

A typical architecture of a smart building automation system has been described in [2] and it identifies the main components of a building control network: sensors, actuators, communication buses, controllers, human machine interfaces, databases, application servers and cloud components. These components are grouped either spatially, for handling specific functions in a certain area of the buildings, especially in large commercial buildings: offices, malls, public halls, or functionally, in accordance to the subsystem or function to which they belong. The main subsystems in a modern building may include the Heating, Ventilation, and Air Conditioning (HVAC) subsystem, lighting, access control and safety, elevators, networking and electrical infrastructure.

Once the required infrastructure and equipment is put in place, local databases and more advanced internet of things (IoT) platforms are able to collect, store and present rich data traces resulting from the daily building operation and in accordance to the various operational and economic criteria. This has allowed multiple developments in statistical learning algorithms that aim to optimize various aspects of the building and closing the loop through predictive control approaches. Representative for this higher level data processing for the HVAC subsystem an application example is given by [3]. A data-driven model based on support vector machines (SVM) is developed to characterize the operation modi of various air handling units (AHU) in a large academic building. Given the large social and economic impact of buildings, various local legislation pieces which are aligned to regional strategies for decarbonization and energy efficiency, such as the energy performance of buildings directive (EPBD), further mandate improvements in building operation which become feasible only though increased automation with learning and big data components for online optimization. Moreover, data needs to be shared across multiple stakeholders in standardized formats.

A differentiating factor when comparing to cybersecurity of industrial control systems is that multiple restrictions have to be considered when handling building data as various slices of these data can reveal sensitive personal information. These can relate to data protection, ownership, cybersecurity and are covered in various EU directives such as the security of network and information systems (NIS), electronic identification and trust services for electronic transactions (eIDAS) and the general data protection regulation (GDPR). One example for this can be that in residential buildings, individual energy consumption patterns are tightly correlated to occupancy and particular activities. Unhindered access to such data by an unauthorized entity or person can breach multiple privacy rules and can become a security issue for the residents. In commercial buildings, correlating access control logs, with CO2 levels and energy readings can also reveal occupancy patterns that are both useful for scheduling

978-1-7281-6843-2/20/$31.00 ©2020 IEEE

purposes and control energy use and at the same time a rich source of information to an external malicious entity.

In this article we present several aspects of smart building automation system security at the individual device and at the system levels. A special focus is put on standardized communication protocols that enable the interoperability of various devices and subsystems e.g. BACnet and mining resulting network patterns using state-of-the-art techniques in new intrusion detection systems (IDS).

II. Device and System Level Security Considerations

We identify several cybersecurity challenges at the device level and system level in smart building automation.

Building automation devices:

- New, IoT-type, devices using one or more communication interfaces become exposed to the outside world without proper configuration;
- Limited on-board resources with low-end processors and little memory, unable to support complex security and encryption schemes;
- Iterative design process in which cybersecurity is seen as an add-on feature, not a core one;
- Trade-off between specialized and multi-function devices;
- Exposed to physical tampering.

Building automation systems:

- Heterogeneous mix of device networks for distributed monitoring and control can become vulnerable in their weakest links e.g. high jacking of basic light switches can allow access to temperature set-points at the room level;
- Need to support devices which are several decades old and obsolete communication standards given long upgrade cycles of classical automation technology;
- Integration of equipment from different manufacturers given different standard interpretations can lead to a relaxation of security policies;
- Prioritization of critical functions over non-critical functions can open breaches during high network congestion;
- Human factors which can potentially expose sensitive information to external malicious entities.

III. Communication Protocols and BACnet Development Tools

A. Communication Protocols

Similar to industrial communication protocols, smart building automation communication is organized in an hierarchical fashion from simple function-specific interfaces to rich multifunctional protocols that support a wider range of applications, across subsystems. At the lower levels, protocols such as LonWorks and KNX are used to interface basic equipment such as temperature and contact sensors and switches up to room level controllers. Several types of controller, including equipment ported from industrial automation to the building domain use ModBus [4], in both RTU and TCP implementation. According to the network and Building Management System (BMS) design, several gateways can be implemented to allow interoperability between various components handling different protocols. In parallel, wireless protocols cover specific areas for ambient monitoring and video surveillance e.g. ZigBee and WiFi. LoRa stations have been implemented to integrate the building in smart city networks for low-rate wide-area data collection and monitoring e.g. utilities automated meter reading.

As a reference widely used standard, BACnet is a networking standard for building automation and control developed by the American Society of Heating, Refrigeration and Air Conditioning Engineers (ASHRAE), adopted by a large number of manufacturers of equipment and systems. It operates in client-server or peer to peer topologies across building functions and allows exchange of information between heterogeneous devices. Currently the BACnet/IP implementation is growing in popularity with the availability of local Ethernet networks. It can be implemented over typical CAT-5e media at 10/100 Mbps communication rates with 32-bit addresses and over 1000 devices supported in the network. Various other datalink layers are supported by the standard, which include ARCNET, MS/TP (serial RS485), PTP (serial RS232), and LonTalk. The BACnet standard layers, according to the OSI stack are illustrated in Figure 1.

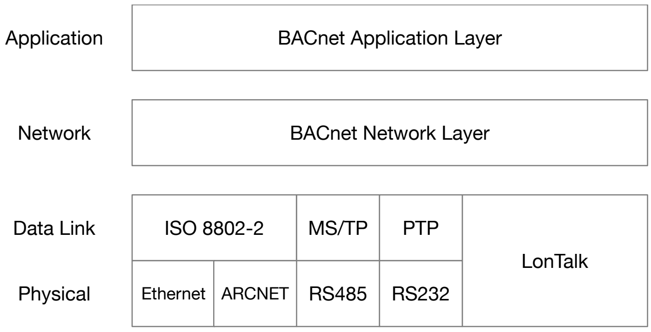


Fig. 1. BACnet layers

The BACnet/IP data frame, uses UDP over the standard port 47808 (0xBAC0) and is encapsulated into an Ethernet packet [5]. The BACnet Virtual Link Layer (BVLL) that includes the Network Layer Protocol Data Unit (NPDU) and Application Layer Protocol Data Unit (APDU) is presented in Figure 2.

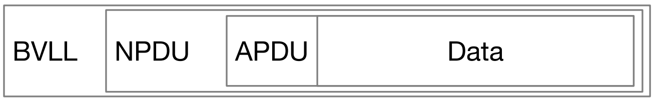


Fig. 2. BACnet packet

In [6] BACnet challenges are identified which stem from the fact that the initial design of the protocol considered isolated and trusted network architectures, a paradigm that is quickly changing within new Industry 4.0 deployments. The usage of peer to peer structures is also seen as a vulnerability where each node can issue commands and alter points in the network. This requires significant engineering and standardization efforts to tag on additional security features and profiles order to support a wide range of equipment over multiple data link layers and instruction sets. Given that some devices can be difficult to update, this represents a significant security challenge.

With regard to BACnet security features, the standard message wrapper structure is listed in Table 1, for secure-enabled communication [7].

TABLE I. SECURITY MESSAGE WRAPPER

Field name	***Size***
Control	1 Byte
Key revision	1 Byte
Key Id	1 Byte
Source Device Instance	3 Bytes
Message Id	3 Bytes
Timestamp	4 Bytes
DNET	2 Bytes
DLEN	1 Byte
DADR	Variable
SNET	2 Bytes
SLEN	1 Byte
SADR	Variable
Authentication Mechanism	1 Byte
Authentication Data Service	Variable
Data	Variable
Padding	Variable
Signature	16 Bytes

The authors of [8] present an approach to encrypt the communication using several approaches: MD5, SHA256, MD5-AES, SHA256-AES. The experimental set-up includes a connection between a desktop pc and an embedded development board (Raspberry Pi 3), using an open source implementation of the standard, over Ethernet with both devices acting, in turns, as client and as server. The most widely used services are tested through multiple requests such as: ReadProperty, WriteProperty, WhoIs and WhoHas. A statistical analysis of the network performance metrics is carried out. It is shown how adding encryption significantly increases the network latency, almost doubling in some cases, over the no security case, while more complex encryption has only an incremental effect on performance degradation. BACnet Secured Connect (BACnet/SC) [9] is the latest feature update to the standard that acknowledges the growing need to secure building automation networks and mitigate cybersecurity risks. It operates as a virtual data link at the application layer and adopts Transport Layer Security (TLS) through Secure WebSockets over TCP. A hub-spoke topology is deployed with hub and node devices, with support for redundant hubs and failover mechanisms.

Logging and online analytic tools for network traffic allow intrusion detection systems to be developed for various types of scenarios in relation to snooping, tampering, spoofing, denial of service (DoS), man in the middle or other types of attacks. An IDS algorithm based on clustering processed network data is presented in [10]. The unsupervised approach focuses on both ModBus and BACNet traffic using publicly available datasets. Typical accuracy, precision and recall metrics are reported in conjunction with dynamic adjustment of cluster boundaries of anomalous/non-anomalous data. In this context, advanced data mining techniques can also be applied for network security [11]. This can include distance and similarity search measures across the data traces and new recurrent neural network structures for learning anomaly patterns and alerting. Events are classified as malicious or non-malicious based on the deviations of the new samples from expected probability distributions, built in the training phase. An alternative can be considered by using an analogy derived from control charts to establish a suitable interval around usual variation of network metrics. The Exponentially Weighted Moving Average (EWMA) is a stable running average of the monitored parameters for a continuous process and can be computed as follows:

$$\mathrm{z}_i = \lambda\, \bar{\mathrm{x}}_i + (1-\lambda)\, \mathrm{z}_{i-1} \tag{1}$$

where λ is a weighting parameter with $0 < \lambda \leq 1$. When σ is the standard deviation of the EWMA, we can compute the upper limit (UL) and the lower limit (LL) for the variations as follows:

$$\mathrm{UL} = +\mathrm{L}\sigma_{\mathrm{z}}\sqrt{\frac{\lambda}{2-\lambda}} \tag{2}$$

$$\mathrm{LL} = -\mathrm{L}\sigma_{\mathrm{z}}\sqrt{\frac{\lambda}{2-\lambda}} \tag{3}$$

where L is a parameter controlling the width of the acceptable interval, usually set as $L = 3$. Persistent deviations outside of the dynamic interval defined by [LL; UL] can signal an anomaly in the automation network behavior caused by an attacker. The potential improvement from added context e.g. building-specific information into the models is underlined to increase classifier performance.

For building-specific IDS semantics are exploited in [12], given the observation that in general building protocols are more expressive. The developed system combines both an automated system to build white-box models based on captured network traffic and a knowledge based system with the support of a human domain expert. It operates online on live traffic to issue alerts for statistically significant deviations from expected values. Value ranges based on known sources and the number of messages according to source-specific frequencies are the main parameters for the thresholding. Results analyze false positive (FP) alerts under varying parametrisation and tolerance levels on a laboratory test-bed of commercial devices.

B. Tools

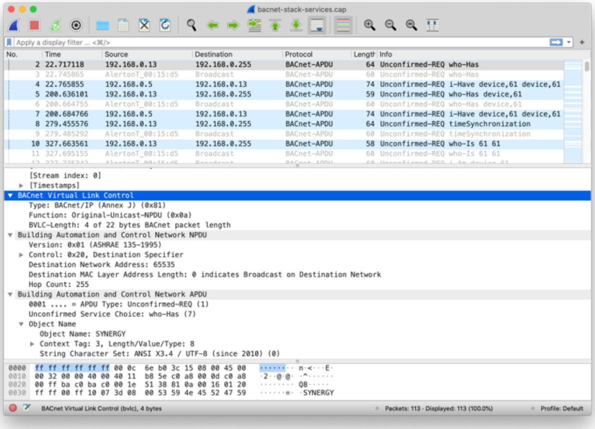
Several open-source tools are available to design, implement and test the behavior of smart building automation networks using BACnet. Various vendors also provide commercial solutions aimed at equipment developers and for certification purposes. Cross-protocol developments have been investigated to simplify heterogeneous network deployment with KNX, LonWorks, ZigBee integration [13].

The BACnet protocol stack (https://sourceforge.net/projects/bacnet/) is a salient open-source implementation of the standard that provides all the required layers to implement BACnet on embedded hardware. Several demonstrative applications are provided to test various con- figurations, functions and parameters for particular use cases. Many research developments use this implementation as a starting point for investigating various security aspects of the protocol in custom deployments. One example [14] presents the development using a customized ARM9 and embedded Linux system as an IP network controller using the stack.

The Visual Test Shell (https://sourceforge.net/projects/vts/) is a Windows GUI-based application to test BACnet devices which has been developed by the National Institute of Standards and Technology (NIST) and released to the public domain. It provides a practical way to interact with devices before commissioning and verifying expected behaviour within the network.

BACpypes (https://github.com/JoelBender/bacpypes) is a Python library for the application and network layers of the standard. Given the emergence of this programming language for various data processing and optimization tasks, it can be used for developing complex applications in smart building automation.

Using the popular Wireshark network traffic analyser and the BACnet profile (https://wiki.wireshark.org/Protocols/bacnet) supplied with it we show a sample packet which adheres to the standard in Figure 3.



```
No.  Time        Source               Destination     Protocol     Length Info
   2 22.717118   192.168.0.13         192.168.0.255   BACnet-APDU  64 Unconfirmed-REQ who-Has
   3 22.745865   AlertonT_00:15:d5    Broadcast       BACnet-APDU  60 Unconfirmed-REQ who-Has
   4 22.765855   192.168.0.5          192.168.0.13    BACnet-APDU  74 Unconfirmed-REQ i-Have device,61 device,61
   5 200.636101  192.168.0.13         192.168.0.255   BACnet-APDU  59 Unconfirmed-REQ who-Has device,61
   6 200.664755  AlertonT_00:15:d5    Broadcast       BACnet-APDU  60 Unconfirmed-REQ who-Has device,61
   7 200.684766  192.168.0.5          192.168.0.13    BACnet-APDU  74 Unconfirmed-REQ i-Have device,61 device,61
   8 279.455576  192.168.0.13         192.168.0.255   BACnet-APDU  64 Unconfirmed-REQ timeSynchronization
   9 279.485292  AlertonT_00:15:d5    Broadcast       BACnet-APDU  60 Unconfirmed-REQ timeSynchronization
  10 327.663561  192.168.0.13         192.168.0.255   BACnet-APDU  58 Unconfirmed-REQ who-Is 61 61
  11 327.695155  AlertonT_00:15:d5    Broadcast       BACnet-APDU  60 Unconfirmed-REQ who-Is 61 61
```

```
    [Stream index: 0]
  ▶ [Timestamps]
▼ BACnet Virtual Link Control
    Type: BACnet/IP (Annex J) (0x81)
    Function: Original-Unicast-NPDU (0x0a)
    BVLC-Length: 4 of 22 bytes BACnet packet length
▼ Building Automation and Control Network NPDU
    Version: 0x01 (ASHRAE 135-1995)
  ▶ Control: 0x20, Destination Specifier
    Destination Network Address: 65535
    Destination MAC Layer Address Length: 0 indicates Broadcast on Destination Network
    Hop Count: 255
▼ Building Automation and Control Network APDU
    0001 .... = APDU Type: Unconfirmed-REQ (1)
    Unconfirmed Service Choice: who-Has (7)
  ▼ Object Name
      Object Name: SYNERGY
    ▶ Context Tag: 3, Length/Value/Type: 8
      String Character Set: ANSI X3.4 / UTF-8 (since 2010) (0)
```

```
0000  ff ff ff ff ff ff 00 0c  6e b0 3c 15 08 00 45 00   ········ n·<···E·
0010  00 32 00 00 40 00 40 11  b8 5e c0 a8 00 0d c0 a8   ·2··@·@· ·^······
0020  00 ff ba c0 ba c0 00 1e  51 38 81 0a 00 16 01 20   ········ Q8······
0030  ff ff 00 ff 10 07 3d 08  00 53 59 4e 45 52 47 59   ······=· ·SYNERGY
```

```
BACnet Virtual Link Control (bvlc), 4 bytes     Packets: 113 · Displayed: 113 (100.0%)     Profile: Default
```

Fig. 3. Wireshark BACnet capture example

It lists a WhoHas service unconfirmed request used in device and object discovery. APDU type is automatically identified along with the object name/manufacturer. The object identifier according to the standard is a unique 22-bit value for each compatible device, in the range 0-4194303 Broadcast requests are also possible within a given subnet as well as confirmed requests e.g. in the case of writing specific properties to adjust set-points. These can be either acknowledged by the destination device or a suitable error message is provided for failures.

Further objects, properties and services can be identified with the goal of improving network operation, identifying unusual behaviour and learning data-driven models in various operation regimes. Flagging suspicious network traffic can be implemented in real-time as a service at a local or centralized level. Communication protocols for smart building automation systems represent a key area of development as well as vulnerability along with a considerably increasing need for training of specialists that can handle all the complexities and implication of misconfigurations and deficient operation from a cybersecurity perspective. This considers also the role of the smart building as a prosumer in local microgrids with distributed energy generation from renewable energy sources [15], where localized attacks can exhibit a spill-over effect to other parts of the (smart) grid with potentially damaging consequences. The aim to deploy is to avoid that the building automation system becomes a vulnerable entry point that enables unauthorized access to other critical infrastructure components with far reaching negative impact. Decision support systems can integrate cybersecurity risks into the control algorithm.

C. *System resilience*

As a generic term, system resilience is concerned with how an (information, in our case) system behaves in the face of adversity (cybersecurity breaches and attacks, in our case) and its ability to maintain delivering the intended functionality. Resilience is not quantified in binary terms but rather on a continuous scale, based on a detailed analysis of the system functions, weighted by their criticality. For cyber-physical systems which include a computing layer and a physical layer, interlinked through a communication layer, resilience can be evaluated at the individual system layer level, cross-layer verticals associated to specific system functions or at a global level. The speed and the degree to which the system recovers from a disturbance is also a factor for evaluating resilience. A recovery timeline starts from normal operation to faulty or degraded operation, operation in degraded mode whilst a recovery/contingency plan is activated and finally back. In the case of building automation, resilience can be evaluated first by identifying the critical functions that the system performs. These can relate to the safety and life preserving subsystems such as fire protection, ventilation, emergency automation functions. Several instruments such as cybersecurity audits and drills can be implemented on a periodic basis to yield contingency plans for the building administrators and control authorities. Adding software or hardware-based components such as firewalls, trust certification modules and additional authentication layers around these components can increase resilience [16]. One particular example for active measures can be the deployment of honeypots [17] that can bring valuable insights regarding the types of vulnerabilities and attack patterns that intruders use and their specific targets. The lessons learned can be used in a systematic manner to improve building automation system resilience. The types of security attacks can be classified at both the device and network levels [18]. Means to avoid tampering and breaches include static code analysis for the automation devices while higher level systems implement IDS methods and continuous monitoring of target parameters through both thresholds based and machine learning based methods. Hardware-based methods involve physical network partitioning and function specific modules that assure the integrity of network communication and of the authentication mechanisms. The human layer sits at the top of methods to assure resilience of the building automation by means of periodic inspection and (re)certification.

IV. Conclusions

The paper discussed several current aspects of smart building automation cybersecurity, as critical task in the development of modern urbanised communities. Automation devices and systems have to be designed with cybersecurity features in mind while upgrading of legacy equipment remains a challenge given high costs, mainly related to the purchase and installation, in existing buildings. We presented several BACnet features - an interoperable widely used building automation communication standard, limitation and ongoing developments with regard to security and several tools that can be used for further analysis and development. It can be established that while many issues are common to industrial control systems, some are different and cybersecurity policies new to account for the specific building automation context. New devices, systems and protocols have to be robustly assessed given the human-facing context of building automation: safety, security, comfort and quality of life, in an energy efficient and environmentally friendly context.

References

[1] G. Stamatescu, I. Stamatescu, N. Arghira, V. Calofir, and I. Fagarasan, “Building Cyber-Physical Energy Systems,” arXiv e-prints, p. arXiv:1605.06903, May 2016.

[2] G.Stamatescu, I.Stamatescu, N.Arghira, and I. Fagarasan,“Pervasive system architecture for optimal hvac control in smart buildings,” in 2017 12th IEEE Conference on Industrial Electronics and Applications (ICIEA), 2017, pp. 59–63.

[3] G. Stamatescu, I. Stamatescu, N. Arghira, and I. Fagarasan, “Data-driven modelling of smart building ventilation subsystem,” Journal of Sensors, vol. 2019, 2019.

[4] E. Pricop, J. Fattahi, N. Paraschiv, F. Zamfir, and E. Ghayoula,“Method for authentication of sensors connected on modbus tcp,” in 2017 4th International Conference on Control, Decision and Information Technologies (CoDIT), 2017, pp. 0679–0683.

[5] J. Tonejc, J. Kaur, A. Karsten, and S. Wendzel, “Visualizing BACnet data to facilitate humans in building-security decision-making,” arXiv e-prints, p. arXiv:1502.06460, Feb. 2015.

[6] C. Valli, M. N. Johnstone, M. Peacock, and A. Jones, “Bacnet - bridging the cyber physical divide one hvac at a time,” in 2017 9th IEEE-GCC Conference and Exhibition (GCCCE), 2017, pp. 1–6.

[7] ASHRAE, “First public review draft of bsr/ashrae addendum g to ansi/ashrae standard 135-2004, bacnet — a data communication protocol for building automation and control networks.”

[8] M. Nast, B. Butzin, F. Golatowski, and D. Timmermann,“Performance analysis of a secured bacnet/ip network,” in 2019 15th IEEE International Workshop on Factory Communication Systems (WFCS), 2019, pp. 1–8.

[9] D. Fisher, B. Isler, and M. Osborne,“Bacnet secure connect:A secure infrastructure for building automation,” ASHRAE, Tech. Rep., 2018.

[10] T. Yu, J. Huang, I. Liao, and K. Kao, “Mining anomaly communication patterns for industrial control systems,” in 2018 Australasian Universities Power Engineering Conference (AUPEC), 2018, pp. 1–6.

[11] S. Duque Anton, L. Ahrens, D. Fraunholz, and H. D. Schotten, “Time is of the essence: Machine learning-based intrusion detection in industrial time series data,” in 2018 IEEE International Conference on Data Mining Workshops (ICDMW), Nov 2018, pp. 1–6.

[12] D. Fauri, M. Kapsalakis, D. R. dos Santos, E. Costante, J. den Hartog, and S. Etalle, “Leveraging semantics for actionable intrusion detection in building automation systems,” in Critical Information Infrastructures Security, E. Luiijf, I. Zutautaite, and B. M. Hammerli, Eds. Cham: Springer International Publishing, 2019, pp. 113–125.

[13] S. H. Hong, “Development of a bacnet-zigbee gateway for demand response in buildings,” in 2013 Pan African International Conference on Information Science, Computing and Telecommunications (PACT), 2013, pp. 19–23.

[14] H. Jian-Cang, “Research on bacnet building controller based on arm9 and embedded linux,” in 2018 Chinese Control And Decision Conference (CCDC), 2018, pp. 2318–2324.

[15] Stamatescu, I.; Arghira, N.; Făgărăşan, I.; Stamatescu, G.; Iliescu, S.S.; Calofir, V. Decision Support System for a Low Voltage Renewable Energy System. Energies 2017, 10, 118.

[16] A. Antonini, A. Barenghi, G. Pelosi and S. Zonouz, "Security challenges in building automation and SCADA," 2014 International Carnahan Conference on Security Technology (ICCST), Rome, 2014, pp. 1-6, doi: 10.1109/CCST.2014.6986996.

[17] J. Bauer, J. Goltz, T. Mundt and S. Wiedenmann, "Honeypots for Threat Intelligence in Building Automation Systems," 2019 Computing, Communications and IoT Applications (ComComAp), Shenzhen, China, 2019, pp. 242-246, doi: 10.1109/ComComAp46287.2019.9018776.

[18] W. Granzer, F. Praus and W. Kastner, "Security in Building Automation Systems," in IEEE Transactions on Industrial Electronics, vol. 57, no. 11, pp. 3622-3630, Nov. 2010, doi: 10.1109/TIE.2009.2036033.