Cloud, wireless technology, internet of things: the next generation of building automation systems?

To cite this article: Gerrit Bode et al 2019 J. Phys.: Conf. Ser. 1343 012059

View the article online for updates and enhancements.
Cloud, wireless technology, internet of things: the next generation of building automation systems?

Gerrit Bode¹, Marc Baranski¹, Markus Schraven¹, Alexander Kümpel¹, Thomas Storek¹, Markus Nürenberg¹, Dirk Müller¹, Andreas Rothe², Jan Henrik Ziegeldorf², Johannes Fütterer² and Bernd Scheuffele³

¹RWTH Aachen University, E.ON Energy Research Center, Institute for Energy Efficient Buildings and Indoor Climate, Mathieustraße 10, 52072 Aachen, Germany
²aedifon GmbH, Hohenzollererring 72, 50672 Köln, Germany AutomationOne GmbH,
³Wiesweg 32, 82409 Wildsteig, Germany

E-mail: gbode@eonerc.rwth-aachen.de

Abstract. Building automation and control systems (BAS) have become a common part of non-residential buildings in the past decades. However, many automation systems rely on severely outdated technology that render it challenging, if not impossible, to implement recently developed, advanced building control approaches. By contrast, recent developments in cloud computing and wireless technology could support solutions to these challenges. However, many stakeholders require a suitable methodology to determine the potentials and the requirements of future, possibly next generation BAS. In this paper, we thus present and apply a method to answer the open questions and define minimum requirements. For that end, we investigate available communication technologies, protocols, and interfaces. Moreover, we present a simple test bench layout that could serve as a blueprint for future, more comprehensive test benches. It is a model a ventilation circuit consisting of a CO₂ sensor for the supply air and an electronic damper. We turned these conventional components with analogue interfaces into IoT devices using a previously developed WiFi gateway. An exemplary test is the control of the CO₂ concentration using a feedback controller implemented on an external machine. We aim to extend our initial prototype to a real-life building demonstration for dynamically scalable automation systems using wireless communication and develop our set-up into a platform enabling arbitrarily complex automation strategies and artificial intelligence applications.

1. Introduction and related work

In recent decades, buildings have become highly monitored data sources, often comprising thousands of sensors, actuators and configuration information [1]. As of now, most of the data sources such as single sensor elements are wired to larger automation stations, often in a strictly hierarchical way. The format of the data is governed by a multitude of different protocols and standards [2]. The set-up of such a system is a mayor task in construction, and altering the system in later stages of the buildings life-cycle is often an expensive and difficult task. The implementation of new automation applications is often hindered significantly by vendor-locked systems that are not fully interoperable with other suppliers [3].

With the rise of the Internet of Things (IoT) and Cloud computing, low-cost and often wireless devices have attracted more attention from researchers in automation and subsequently, the building automation industry [4]. The promises of IoT include easy installation, reduced
configuration effort, high availability and direct cloud integration. The deployment of IoT sensors can also be used to enhance existing building management systems [5]. Cloud computing in turn promises the access to unlimited computing power, to be used in artificial intelligence, model predictive control and more.

IoT includes stakeholders and actors from many different fields, each viewing the problem under the notions and concepts of their field. As a result, IoT represents a synergy of three different visions[6, 7]:

- **the thing oriented vision**, focusing on the single sensor or component, that is now considered as an individual object rather than part of a major device,
- **the internet-oriented vision**, where the network and interconnectivity, and subsequently the middleware, of things are the starting point for design, and
- **the semantic-oriented vision**, considering the problem of identifying, representing, storing and exchanging unique information.

IoT architectures can be utilized to develop and deploy advanced control algorithms for devices like HVAC units and, ultimately, whole building energy systems [8]. Despite the high research interest of the recent years, many problems still remain to be studied [7]. Experiences from field test show that the development of IoT devices is a challenge that needs to be addressed by the whole industry to create common standards and provide interoperability [9].

Among the major concerns is the architecture of the system and the development of security among all layers of the system [10, 11, 12]. Therefore, we propose a methodology that could be the basis for future in-depth analyses of the above-mentioned research questions and the development of future IoT-based building automation systems (IoT-BAS).

In this paper, we propose specifications that we consider the minimum requirements of IoT-BAS. Based on these specifications, we deduct questions that, in our opinion, any future researcher or developer of IoT-BAS should answer before the actual development. After these theoretical considerations, we present a low-cost test bench setup that allows practical evaluation of IoT control loops. A summary of the methodology and its application to the presented test bench concludes the paper. The activities outlined in this paper are part of the research project Next Generation of Building Automation Technology (NextGenBAT).

2. Methodology

In order to support the development of future IoT-BAS, we propose the following minimum requirements and a non-exhaustive list of questions that can provide guidelines for researchers and developers.

2.1. Minimum requirements

As the terms IoT has various definitions, we define the following for the considerations in this paper. An IoT-BAS contains, although not exclusively, devices that can communicate via the internet with servers located outside of the building. This communication is not typical for contemporary BAS and has a series of interesting implications, which are summarized in Figure 1 and described in the following.

Each field device, i.e. sensors and actuators, in the BAS should either be Internet Protocol (IP)-enabled or connected to a gateway that is. Multiple field devices can be connected to one gateway. However, we consider one major advantage of IoT-BAS that they avoid the aggregation of a large number of devices on central stations and therefore provide more flexibility. The gateways can be installed in close proximity to the field devices, thus reducing the wiring effort or the damping in case of wireless communication. Moreover, the nearby installation also facilitates the future operators’ orientation in the BAS, which, traditionally, are complex and often confusing systems.
Each component supports Internet Protocol (IP), either Ethernet or wireless. Each component has a unique ID (e.g. the MAC address). Data points are linked according to the physical topology.

Time series and meta data is stored in (separated) data bases. Flexible availability of computing power. Support of established field bus protocols to support application in existing BAS. Flexible implementation of control functions or automatic commissioning tests.

Small buffer of time series data. Devices that do not support IP are connected using gateways.

Remote configuration is possible worldwide. The user can select pre-fabricated models for grouping data points.

Figure 1. The proposed architecture for IoT BAS

The IP-enabled devices have a fixed identifier such as the MAC address. Additional information such as a string containing the position and the function of the device can be stored on the device. It is imaginable that pre-configured devices are delivered to the construction site. However, we consider it important that the configuration can be altered remotely and any time to increase flexibility.

The devices communicate with some kind of cloud platform via a light-weight protocol such as MQTT [7]. The cloud platform should allow for basic modelling of the physical and functional relations of the data points provided by the devices. The user should have access to basic templates, such as a heat pump model that consists of four temperature measurements and electrical power. There are many ontologies available such as SAREF [13] or BRICK [14].

Time series data and meta data provided by the devices should be stored in separate data bases, for example a time series data base and a PostgresSQL data base, respectively. The cloud platform should also allow the user to implement various types of control algorithms such as rule-based and model-predictive control (MPC). We consider it a major advantage of cloud-based control that data can be used for training data-driven model that can, in turn, be used for MPC, load predictions and error detection. It should be possible to send control decisions back to the devices. Thus the communication should be bi-directional.

The IT security is one of the major concerns in IoT-BAS. The requirements to Internet connected devices are very complex and secure systems are hard to design even for domain expert. The topic of security will therefore be analysed in separate work later in the project.

2.2. Open questions
Based on the definition of the minimum requirement, we list the open questions in the following to provide guidelines for the future development of IoT-BAS.

What should be included in the pre-configuration of the devices? These configurations include anything relevant for the secure communication via the internet, e.g. firewall settings of the devices in the local network, IP addresses of the external server and certificates.

What meta-data should be stored on the device? The meta-data can include information on the device type and data point types. It can be comparable to the information in the BACnet standard.
What message format should be used? The messages, e.g. sent from a field device to an external broker via the MQTT protocol, should have a pre-defined format such as data point name, measurement value, time stamp.

What is the ideal message size? In case of measurements, multiple observations could be gathered in one message. Alternatively, each observation can be sent in a dedicated message. There is a trade-off between latency and message count.

What part of the control logic should remain locally? There may be reasons for and against controlling certain control loops from the cloud, depending on the individual situation.

What is the minimal required measurement accuracy? Especially if low-cost sensors are used, the accuracy of the measurements may be an issue. The minimum accuracy required for a certain application should be defined.

What are the highest allowable delays and latencies? IoT environments may reduce time delays via slow field buses such as BACnet MS/TP or slow translations on gateways but require the user to consider the latency of the communication between, for example, an MQTT publisher and a subscriber. Depending on the control task, the user must determine the maximum admissible sample rate.

What is stored on the device temporarily? Each device could store a certain amount of time series data to buffer temporary communication breakdowns or delays or to allow e.g. multiple observations to be gathered in one message.

Is there a need for fall-back control logics? How can the system remain functional in case of connection loss to the cloud system?

2.3. Transition steps
As described in the introduction, the IoT concept consists of multiple parts. It is not necessary for a system to fully support all visions of IoT at once to leverage the positive effects. It is, for example, possible to consider also wired sensors and actuators as semantic objects by individually handling their addressing and data. In such a system, new devices can be integrated following the same semantic convention.

Since many buildings are already fitted with BAS systems, a transition strategy should be present to quickly achieve the amount of users necessary for economically operation of cloud platforms. For current wired systems, the use of IoT Gateways is a comparably cost efficient method to continue using installed wired devices and connect them to a cloud platform. The gateway itself can be either wired or connected wireless.

3. Prototype test bench
In order to provide an example of how future test benches for IoT-BAS could be designed, we built a test stand as small representation of a ventilated and conditioned room. This test bench shall show how common devices can obtain IoT capabilities and demonstrate how the communication between the devices and the cloud-platform can be established. Besides that, we implemented a controller within the cloud-platform, which additionally provides services for data visualization.

The test bench comprises a small box as a representative room, which is occupied by two heating and CO₂ sources in form of candles and a room control unit measuring the temperature and CO₂ concentration within the box. Fresh air is provided by a computer fan. A damper, which is controlled by an electric valve actuator, allows for reducing or increasing the supply air flow.

All the sensors and the actuators use common analogue interfaces for transferring and receiving signals. They are connected to a gateway device we developed in previous works,
Converting analogue signals into the digital representation and transferring the data via WiFi [15].

The data is sent using MQTT. Hence, sensors publish values to a defined topic, while actuators subscribe to a topic and listen for messages published by the broker.

A schematic overview of the bench stand with its components and connections is presented in Figure 2.

On the notebook, data is incorporated into a FIWARE deployment [16] as our demo cloud platform. FIWARE provides message broker and IoT device management components as well as functionality for database storing, visualization and a Python container we use to host the control process. Within the container, we implement a basic PID controller controlling the CO\textsubscript{2} concentration in the test chamber, thus increasing or decreasing the ventilation rate.

Figure 3 shows the result of an experiment conducted on the test bench. The two peaks mark intentional disturbances of the system. The controller is able to keep the CO\textsubscript{2} concentration at the desired level for both tested set points despite the highly fluctuating burning rate of the candles and the two disturbing reboots of the controller.

4. Conclusion and Outlook
In this paper, we presented minimum requirements for the transition from classical to IoT-based BAS. We described an architecture with which these requirements can be met. The architecture was partly set up and demonstrated in a laboratory test set-up using prototype hardware and a minimal control-loop example. In this small-scale scenario, we showed that IoT devices enable cloud-based controls to perform basic BAS functionalities and that both the test bench and the method in general are suitable for further analysis of new technology in BACS.

As a next step in the project, we will retrofit an HVAC unit within the E.ON ERC main building in Aachen to become a fully IoT-enabled component, transferring not only monitoring,
but all control functions into the cloud. This comprehensive test bench will allow to research possible answers to the questions raised in this paper, especially the fall-back time, latency and control quality of IoT systems.

Working together with renowned security specialists, we will run penetration tests on the system, identifying weaknesses in both the architecture design and the implementation, to ensure from the start that IoT is not a greater safety risk than common BAS systems.

To ensure the penetration of IoT into the German construction market, the project aims to create a interest community of stakeholders from the entire building life-cycle, including planers, building owners, building operators, manufacturers of sensors and actuators, manufacturers of wireless communication technology and network and cloud providers. Cooperating with the project team, the committee of this community will ensure that requirements are met and stakeholders are introduced to the new concepts and technologies.

Acknowledgments
We gratefully acknowledge the financial support provided by the BMWi (Federal Ministry for Economic Affairs and Energy), promotional reference 03ET1657A.

References
[1] Stimmel C L 2015 Big data analytics strategies for the smart grid (Boca Raton, FL: CRC Press) ISBN 9781482218282 URL http://proquest.tech.safaribooksonline.de/9781482218282
[2] Domingues P, Carreira P, Vieira R and Kastner W 2016 Computer Standards & Interfaces 45 1–12 ISSN 09205489
[3] Veichtlbauer A, Pfeiffenberger T and Schrittesser U 2012 Generic Control Architecture for Heterogeneous Building Automation Applications 6th International Conference on Sensor Technologies and Applications (SensorComm 2012)
[4] Lilis G, Conus G, Asadi N and Kayal M 2017 Sustainable Cities and Society 28 473–481 ISSN 22106707
[5] Zhang X, Adhikari R, Pipattanasomporn M, Kuzu M and Rahman S 2016 Deploying IoT devices to make buildings smart: Performance evaluation and deployment experience 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT) (IEEE) pp 530–535 ISBN 978-1-5090-4130-5
[6] Atzori L, Iera A and Morabito G 2010 Computer Networks 54 2787–2805 ISSN 13891286
[7] Jia M, Komeily A, Wang Y and Srinivasan R S 2019 Automation in Construction 101 111–126 ISSN 09265805
[8] Png E, Srinivasan S, Bekiroglu K, Chaooyang J, Su R and Poolla K 2019 Applied Energy 259 408–424 ISSN 03062619
[9] Coates A, Hammoudeh M and Holmes K G 2017 Internet of Things for Buildings Monitoring Proceedings of the International Conference on Future Networks and Distributed Systems - ICFNDS '17 ed Unknown (New York, New York, USA: ACM Press) p 38 ISBN 9781450348447
[10] Weyrich M and Ebert C 2016 IEEE Software 33 112–116 ISSN 0740-7459
[11] Minoli D, Sohraby K and Kouns J 2017 IoT security (IoTSec) considerations, requirements, and architectures 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC) (IEEE) pp 1006–1007 ISBN 978-1-5090-6196-9
[12] Minoli D, Sohraby K and Occhiogrosso B 2017 IEEE Internet of Things Journal 1
[13] Daniele L, den Hartog F and Roes J 2015 Created in Close Interaction with the Industry: The Smart Appliances REference (SAREF) Ontology Formal Ontologies Meet Industry (Lecture Notes in Business Information Processing vol 225) ed Cuel R and Young R (Cham: Springer International Publishing) pp 100–112 ISBN 978-3-319-21544-0
[14] Balaji B et al. 2016 Brick Proceedings of the 3rd ACM International Conference on Systems for Energy-Efficient Built Environments - BuildSys '16 (New York, New York, USA: ACM Press) pp 41–50 ISBN 978-1-4503-4264-3
[15] Schraven M H, Carducci C G C, Baranski M A, Müller D and Monti A 2019 Designing a Development Board for Research on IoT Applications in Building Automation Systems 36th International Symposium on Automation and Robotics in Construction (ISARC 2019)
[16] Zahariadis T et al. 2014 FIWARE Lab: Managing Resources and Services in a Cloud Federation Supporting Future Internet Applications 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing (IEEE) pp 792–799 ISBN 978-1-4799-7881-6

1 See http://www.nextgenbat.de/ for details