

Article

Standards for Cyber-Physical Energy Systems—Two Case Studies from Sensor Technology

Michael C. Krutwig ^{1,*} , Bernhard Kölmel ², Adrian D. Tantau ¹ and Kejo Starosta ¹

¹ Department of Business Administration, The Bucharest Academy of Economic Studies (ASE), Romană Square No. 6, 010371 Bucharest, Romania; adriantantau@fabiz.ase.ro (A.D.T.); k@ksfx.de (K.S.)

² Institute of Smart Systems and Services, Pforzheim University of Applied Sciences, 75175 Pforzheim, Germany, bernhard.koelmel@hs-pforzheim.de

* Correspondence: michael@krutwig.com; Tel.: +49-721-9426970

Received: 30 December 2018; Accepted: 24 January 2019; Published: 28 January 2019



Abstract: Cyber-physical energy systems (CPES) describe a specialization of the cyber-physical system concept, in which energy systems are transformed into intelligent energy networks. These systems provide the basis for the realization of smart microgrids and smart grids. In the last decade, numerous research projects have intensively explored the fundamentals and modeling of CPES and validated them in pilot projects. In the meantime, more and more CPES solutions have been appearing on the market and the battle for the most suitable standards has begun. This paper gives an overview of the currently available standards for CPES sensor technologies and assesses the suitability for implementation. In two case studies in the application area of operational energy management in German companies, a sensor retrofitting is described—once with proprietary technology and once using the standards Long Range (LoRa) Wide Area Network and OPC Unified Architecture (OPC UA). As a result, the shortcomings of the standards for their use in CPES are shown and discussed. OPC UA, which was originally developed for the manufacturing industry, turns out to be a suitable standard for a wide range of CPES implementations.

Keywords: cyber-physical energy systems; standards; low power wide area networks; long range wide area network; OPC unified architecture; energy management systems; sensors

1. Introduction

While existing electricity grids work unidirectionally from producer to consumer, intelligent electricity grids, otherwise known as smart grids [1], offer new possibilities for energy use, particularly in integrating decentralized energy generation facilities. Smart grids scale through networking among each other and are subject to constant dynamics. For example, electric and hybrid vehicles can be included in grids as consumers or storage devices to avoid peak loads and reduce carbon emissions [2]. The smallest unit of smart grids, which comprises unidirectional energy flow from power generators to consumers and networked intelligence, is referred to as a smart microgrid [1]. Smart microgrids offer a communication interface for data and services and a virtual representation of the energy components they contain. This follows the general concept of cyber-physical systems (CPS) [3] and is grouped under cyber-physical energy systems (CPES) in the energy context. The survey in [4] highlights the concepts and challenges surrounding CPES. The high dynamics and intense networking between smart grids require standards in practical implementation to make numerous heterogeneous infrastructures interoperable. These standards must meet CPES requirements, which include reliability, security, robustness against unexpected states, and adaptability, should there be subsystem failure.

The emergence of smart grids from the networking of several microgrids is inhibited by two factors. The first is the legal framework and charges in some countries, which reduces the economic

attractiveness of decentralized electricity supply. In Germany, for example, reduced grid fees and the introduction of net metering [5] could make the use of public electricity grids more appealing for smart grids. The second challenge is insufficient standardization. Without CPES standards, smart microgrids will remain isolated solutions. The significance of standards is clear when considering the forecast of 50 billion devices in the Internet of Things (IoT) by 2020 [6], while being cognizant that CPS and CPES also make up these “things”.

The addition of CPS functionality to existing systems and devices is also known as retrofit. These procedures are often used to turn buildings into so-called smart buildings, which are less energy-intensive, with the ideal goal of realizing zero-energy buildings [7]. Improved energy efficiency is achieved by saving, redistributing, and storing energy, as well as by intelligent building use; for example, by occupancy detection using CPES sensors [8] or Wi-Fi probe-based detection [9]. The components of a smart building are [10] sensors, actuators, controllers, a central unit, an interface network, and a smart meter for communicating with the utility company. If the smart building also has components for generating and storing energy, the result will be a smart microgrid.

According to [4], the four main research areas surrounding CPES are modeling energy systems, energy efficiency, energy resource management, and energy control. The use cases of this work relate to energy efficiency. An energy management system (EMS) helps organizations reduce energy costs, act more sustainably, reduce carbon emissions, and implement a well-structured energy policy [11]. In addition, non-energy benefits, such as better working conditions and lower costs of raw materials, maintenance, and repairs can be gained [12]. An EMS often includes energy monitoring software, which acquires energy data from meters, sensors, and other sources, and presents it in a visualization software system. Realized as CPES, these sensors and meters can also be used for other purposes and non-energy benefits in smart grids. Our work deals with such networked energy sensors. By examining CPES standards, we aim to contribute to overcoming a common challenge in planning submetering: the more measuring points the submetering includes and the shorter the measuring intervals, the more information can be obtained from the data. However, the problem lies in the uncertain economic profitability of submetering. Measuring equipment is costly and the possible useful value becomes visible only after purchase—or not at all. In addition, new networked measurement equipment also brings new potential safety challenges. Though there are technical methods for identifying the best submetering [13], one strategy that is never wrong is minimizing the cost of sensors. In light of this, radio networked sensors can easily be used at different locations for temporary measurements.

In the search for suitable CPES standards, simulation methods are only of limited use, as the reduction of complexity is usually not a requirement for simulations. In recent years, numerous studies on CPES modeling [14,15] have been conducted. These describe approaches to simulations and mathematical calculation models concerning merging the physical world of the energy industry with the cyber world into a CPES. In this context, [15] provides the challenges for models, which must also apply analogously to the required standards. A comprehensive overview of models and methods can be found in [16]. Our case studies highlight that standards must not hinder efficient application in practice, because the most sophisticated technologies cannot be substituted for usability. In this paper, currently available standards are examined for their suitability to CPES and some are then subjected to practical application. The first case provides a retrofit without standards for comparison purposes, while the second case uses several standards with high suitability for CPES, generating a high level of interoperability at the price of higher system complexity.

2. Scope and Structure

The research begins with a review of currently available standards suitable for wireless networking in CPES. These are analyzed in the third section, which describes wireless sensor networks (WSN) and the class of low power wide area networks (LPWANs), both aimed at networking in smart microgrids. The Long Range (LoRa) standard, which is practically analyzed in one proposed research case, is

presented in more detail. This critical review of the standards helped refine the initial research ideas and build the context for the standards currently available for wireless networking in CPES.

The fourth section discusses standards that can be considered for the cyber representation of CPES. The OPC Unified Architecture (OPC UA) framework analyzed here is a particularly promising candidate and is more closely aligned with CPES requirements.

The hands-on work of this research is presented in the fifth section, where we discuss the two representative case studies we are conducting in companies in Germany. We compare a retrofit using a non-standard product with a setup based on the LoRa and OPC UA standards. The first company is a retailer with low energy consumption that receives a retrofit of its utility energy meter through a glued-on optical character recognition (OCR) camera solution. In the second company, an automobile manufacturer, we measure energy consumption in three phases of a process plant using current transformers. In both case studies, the sensors for measuring energy consumption are connected to a universal EMS. The observation focuses on the complexity and effort of integrating CPES sensors into a universal EMS in a real-life context. A comparison shows the cost differences of implementation, configuration, and hardware costs.

The discussion in the sixth section compares the two approaches and shortcomings of the standards applied for their use in CPES.

3. Standards for Cyber-Physical Energy Systems (CPES) Wireless Networking

While Ethernet is the key to wired networks for CPES, there are numerous proprietary and standardized technologies for wireless technologies. The wireless networking of CPES requires machine-to-machine (m2m) radio technologies with a low data rate; the requirements for reliability, real-time capability, and range depend on the specific application. In the "last mile" of wireless sensor networks (WSN) applications [17], there are numerous available standards and a growing market of "smart" wireless components. Many of these products possess proprietary technologies for radio transmission, whereby the term "proprietary" is also valid if the protocols are known, but the provider has authority over a transmission medium or cloud storage.

IoT radio networks, known as low-power wide area networks (LPWAN) [18], exist for ranges of several kilometers in combined indoor and outdoor use. This class of networks is specially designed for M2M and CPES communications. Instead of a high data rate, the requirements for such LPWANs are in other areas:

- *Coverage*: a single radio base station must cover a smart microgrid. As its maximum radius is not definable, one may assume several kilometers. Public LPWAN infrastructures cover entire countries or continents.
- *Sensor energy consumption*: battery-powered sensor nodes should be able to work with one battery for several years.
- *Capacity*: a base station must be able to supply several thousand IoT devices.
- *Adaptively*: An LPWAN standard should consider multiple user profiles for different deployment scenarios. For instance, [19] contains four different categories with application examples that describe different requirements for hardware complexity and use of radio channels.
- *Reliability*: the radio link must also function within buildings through numerous walls and floors. The protocols should detect transmission errors and then be able to take appropriate action.
- *Security*: the network protocols must provide security mechanisms at all protocol levels to ensure privacy, authenticity, and integrity.
- *Economic efficiency*: the hardware required for networking must be cost-effective in order to make use of a large number of sensors or even disposable objects economically feasible.

With LPWANs, we distinguish between commercial providers for network as a service (NaaS) and infrastructures that can be set up independently. For the latter, the Long Range (LoRa) Wide Area

Network (WAN) technology is currently without an alternative. Furthermore, NaaS has no relevance for short-range WSN.

3.1. Short-Range Communication Standards

In the field of home automation, radio networks are used to connect sensors at close range, which operate in star topologies or as mesh networks [20]. These networks can also be used for CPES, for instance [21] is investigating the use of IEEE 802.15.4 in electric power system environments. With the exception of Wi-Fi, all the technologies mentioned here are optimized for low power consumption of sensors. Table 1 gives an overview of standards for local sensor networks.

Table 1. Common Standards for local sensor networks.

	Wi-Fi	Z-Wave	ZigBee	Bluetooth Version 5	Bluetooth LE	6LoWPAN
Standard	IEEE 802.11 (a/b/g/n/ac)	(proprietary)	IEEE 802.15.4	IEEE 802.15.1	IEEE 802.15.1	IETF RFC 4944
Frequency band (EUR)	2.4 GHz	868 MHz	868 MHz, 2.4 GHz	2.4 GHz	2.4 GHz	868 MHz, 2.4 GHz
data rate	>3 MBit/s	100 kbit/s	250 kbit/s	>10 MBit/s	1 MBit/s	250 kbit/s
Indoor range	100 m	30 m	10–75 m	10 m		200 m
References	[22,23]	[24]	[25]	[26]	[27,28]	[25]

Another WSN for IoT applications is Wi-SUN [29], which is based on IEEE 802.15.4g. This standard can be characterized between WSN and LPWAN. The technology modulates with FSK in the free ISM 800–900 MHz, offers a data rate up to 150 kbit/s, and reaches nodes up to 5 km away [30]. For the sake of completeness, the Weightless [31] LPWAN technologies should also be mentioned.

3.2. Low Power Wide Area Networks (LPWANs) as a Service

For wireless networking, CPES can use several LPWAN providers that offer NaaS nationwide in one or more countries. The best-known competing technologies in Europe are LoRaWAN [32], SigFox [33], NB-IoT (Release 13) [19], and LTE-M [34], which differ in technical parameters and marketing concepts. The SaaS Sigfox of the French company Sigfox S.A. is available in 53 countries (December 2018), but without seamless coverage. Sensors with Sigfox modules are available for applications in smart homes, smart cities, agriculture, environment, health and assisted living, industry, and fleet management. The network works in the ISM band at 868 MHz and supports half-duplex communication, which can only be invoked by the node. For modulation, the differential binary phase shift keying (DBPSK) method is used for the uplink and the gaussian frequency shift keying (GFSK) method for the downlink [35]. To further reduce energy consumption, Sigfox can also be used in an operating mode with a unidirectional uplink so the nodes act exclusively as transmitters. The elimination of the receiver also reduces hardware costs. The payload is 12 bytes small. Technical parameters, restrictions, and rules for competing access are country-specific. In Europe, up to 140 messages can be uplinked daily at a rate of 100 bit/s and the network usage ratio must not exceed 1%. This amount of data restricts the usability of Sigfox to sensors with transmission of single values at an interval of not less than five minutes. The transmission range of a base station can be up to 50 km in flat rural areas, but only 3 to 10 km in an urban environment [35]. In the United States, Ingenu [36] offers another commercial NaaS of the same name for IoT applications and smart grids operating in the 2.4 GHz band with random phase multiple access (RPMA) modulation.

As a part of the Long Term Evolution (LTE) [37] standard family, Narrowband IoT (NB-IoT) (also: LTE Cat-NB1) [19], and LTE for Machines (LTE-M) (also: LTE Cat-M1 or eMTC) [34] are standards for cellular LPWANs maintained by the Third-Generation Partnership Project (3GPP). Both are based on GSM/LTE networks and operate in licensed frequency bands. Providers are large mobile operators who can expand their existing LTE radio systems with extensions for IoT services. Using the existing

LTE system design for media access, channel coding, interleaving, rate matching, and more gives providers a significant time and cost advantage. In LTE-M, a software update of the existing LTE systems is sufficient [34], while Narrowband IoT (NB-IoT) requires a hardware upgrade of the base stations to perform the required modulation. Unlike LTE-M, which only works for LTE in-band, NB-IoT can be operated in three different modes: standalone as a carrier in the GSM band, LTE in-band, or within an LTE guard band. To fulfill the additional need of 20 dB maximum coupling loss (MCL), NB-IoT uses techniques to increase coverage, such as power boosting in the downlink or subframe repetition in the uplink and downlink [38].

Both standards use the single carrier frequency division multiplex access (SC-FDMA) method for uplink modulation and the orthogonal frequency-division multiple access (OFDMA) method for downlink modulation. With its 180 kHz wide channels, NB-IoT achieves a data rate in the uplink of about 200–250 kbit/s and can handle up to 50,000 devices per cell. With LTE-M, an upload rate of up to 1 MBit/s is possible, and the capacity of a cell is about 10,000 devices. Compared to regular LTE, 3GPP has introduced some simplifications for NB-IoT: a single antenna is sufficient for receivers and transmission hardware just implements a half-duplex mode, resulting in a less complex hardware design and cheaper radio modules. LTE-M provides full duplex communication.

As the providers of this network as a service (NaaS) promise complete network coverage, we do not have to worry about the size of the smart microgrids or the range of a base station, only the actual coverage in the desired region is of relevance here. However, one must be aware that not every sensor is always accessible in areas that are considered to be supplied. Studies like [35,39] report 99.9% indoor and outdoor accessibility at LTE-M in a rural area. For deep indoor usages, NB-IoT is required and the coverage remains at about 95% of all devices. A summary of the technological details and architecture of NB-IoT can be found at [38,40,41].

LoRaWAN is also offered as NaaS by several commercial network providers. Moreover, with The Things Network (TTN) [42], there is also a free crowd-funded LoRaWAN NaaS. In this growing network, everyone can make their LoRaWAN gateway available to all participants worldwide. According to the project website [43], in December 2018 there were 658 participating gateways listed in Germany, organized in 66 regional communities.

3.3. LoRaWAN

The only LPWAN technology currently available on the market for setting up own radio infrastructures in the free ISM band is long range wide area (LoRa) [32]. LoRa is a wireless infrastructure for LPWAN developed by Semtech Corporation. The system architecture consists of three components: the end devices, gateways, and a network server (Figure 1). The end devices are integrated into the LoRaWAN by a LoRa radio chip. A gateway forms the radio base station for all nodes and forwards their data packets to the network server (NS) connected via IP. As the gateways are transparent for the connected nodes, the NS filters receive duplicate messages of a node via more than one gateway and decide which gateway is responsible for the downlink. The NS also provides the API for one or more application servers [32].

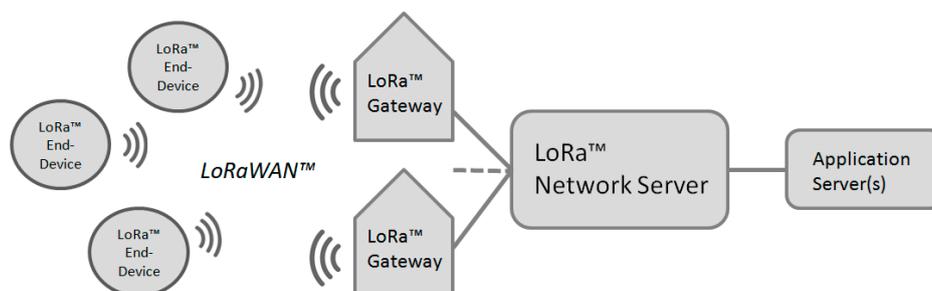


Figure 1. Long Range (LoRa) system components.

LoRa defines a modulation technique [44] for radio data transmission on the license-free ISM band 169 MHz, 433 MHz, 868 MHz (Europe), and 915 MHz (North America); the radio module is also referred to as “concentrator”. LoRa meets the above requirement for adaptivity in LPWANs with the patented chirp spread spectrum [45,46] modulation. This enables control of the data rate and signal level for each connected device via an individually selectable spreading factor (SF) in a value range from 7 to 12. This allows the energy consumption to be controlled specifically according to the usage profile and the distance of the node from the base station. More intensive use of the radio network with a modulation frequency (BW) and an improved error correction can be obtained with LoRa by setting a lower data rate. In Europe, typical BW values are 125 kHz, 250 kHz, and 500 kHz. The error correction is controlled by a code rate (CR, value range 1–4). The relationship of these influencing factors to the data rate (R_b) is calculated as follows:

$$R_b = \frac{SF \times BW \times 4}{2^{SF} \times (4 + CR)} \text{ Bit/s} \quad (1)$$

Without taking CR into account, a raw data rate of 22 Bit/s to 27 kbit/s is, therefore, possible in Europe. As another limitation, the regulation of shared access for the frequency band used must also be taken into account. In the European ISM band, the duty cycle transmission may not exceed 1% of the time [47].

The LoRa specification distinguishes three device classes—A, B, and C—for end devices [32] in order to meet different requirements for power consumption. The most economical class A devices use the ALOHA method in the uplink, where a downlink is only possible in a short time window immediately after the uplink. This class is suitable for sensors that transmit regularly and only need to receive an acknowledgment of receipt. Class B devices can also receive data independently of uplink. For this purpose, fixed time windows are defined with the network server, in which the nodes are woken up and supplied via a beacon packet broadcasted by the gateway. This device class is required when actuators have to be switched or other information has to be supplied to the node. Class C devices are permanently in receiving mode. Therefore, battery operation is not possible. This allows fast feedback to the node. All three classes can be mixed within a LoRa network.

There are numerous case studies that investigate the reliability, range, and achievable data rate of LoRa. Owing to the different conditions and parameters, these results vary significantly. In a suburban area, coverage of 3km could be achieved [48]. Another study [41] inside buildings confirms an achievable range of more than 300 m through several walls, but none of the SF could achieve a 100% loss-free transmission. TTN [43] reports a LoRa packet transmission that was achieved over a distance of 702 km with a transmission power of 25 mW (measured in August 2017), transmitted by a helium-filled balloon from an altitude of 38,772 km under perfect weather conditions.

4. Standards Enabling CPES

In addition to a communication interface, a CPES requires data and methods of physical energy systems—the cyber component. This represents a model of the physical system with services offered to retrieve relevant data and methods. By looking at the cyber-physical production systems (CPPS) [49], we find suitable standards for such a modeling at the CPS of the industry. As the close integration is a characterizing element of CPES [4], centralized control models and all standards for pure simulation are omitted. In contrast, technologies from automation are a good approach.

4.1. OPC UA (IEC 62541)

OLE for Process Control (OPC) [50] is the successor of OPC Unified Architecture (OPC UA) [51]. This framework was created for data exchange in automation technology and has since become widely used in industry. OPC UA is maintained by the OPC Foundation [52]. The standards IEC 62541-3 describe the object-based address space model of OPC UA. This framework follows a service-oriented, internet-enabled approach that is available across platforms. It provides a communication model

and a uniform data model for processing data, alarms, and historical data, which can be used on a system-wide basis.

Objects, properties, relationships, and methods can be used to create an information model of the physical application. A basic set of nodes is already defined in the standard system [53,54]. This basic scaffold can be extended to specific information models of any application domain, such as CPES. Standardized, cross-manufacturer information models are referred to as Companion Specifications (CS). The uniform semantics of this CS enables interoperability between type-like devices of different brands. A client-server model via TCP/HTTPS, as well as a connectionless publisher-subscriber model using existing standards, such as the User Datagram Protocol (UDP), Advanced Message Queuing Protocol (AMQP), and Message Queue Telemetry Transport Protocol (MQTT), are supported for data exchange [55]. The scalability in larger infrastructures is given by the possibility to use multiple OPC UA servers and clients.

In addition to the information models and transport mechanisms, OPC UA offers an integrated security architecture to protect data and access. Different security policies and selectable mechanisms for authentication and authorization make the protocol flexible. [56]. In order to further reduce complexity, OPC UA has several server profiles with different, interdependent functional ranges [57]. These profiles gradually build on each other:

- *Nano Embedded Device Server*: the smallest possible profile includes the core server, binary message encoding, and TCP support.
- *Micro Embedded Device Server*: additionally includes at least two simultaneous sessions and a simple subscription protocol.
- *Embedded UA Server*: in this profile, additional messages can be signed and encrypted. The number of possible subscriptions is also increased.
- *Standard UA Server*: this full-featured profile allows server configuration customization, allows the use of X509 certificates, and further increases subscription capacity.

For the mapping of the CPES system topology, the authors of [15] recommend an object-oriented representation of the numerous, heterogeneous components. OPC UA meets this requirement because the objects in its information model allow states, methods, values, and hierarchy-free relationships via links. Moreover, variable structural dynamics are mentioned as a challenge, which is given in OPC UA over the extendable address space. OPC UA clients with the appropriate authorization can add any other objects to the address space. After all, the extensible markup language (XML) meets the demand for a model language that can be read by humans, as well as machines.

The most important must-have properties of CPES are summarized in [4]. Table 2 examines the OPC UA standard for coverage of these criteria.

Table 2. Cyber-physical energy systems (CPES) features and their coverage by OPC Unified Architecture (OPC UA).

CPES Requirements according to [4]	OPC UA Features
(i) Reliability	Robustness and reliability against system failures and changes in the environment are offered by OPC UA by the possibility of a distributed infrastructure of any number of OPC UA server clients. The standard ensures change security by using unique namespaces.
(ii) Autonomics	OPC UA can continue to operate even in the event of a subsystem failure; the possibility of self-adjustment has to be implemented individually. A message broker can also be used instead of the client-server mechanism to decouple communication.
(iii) CPES is closely integrated	The different server profiles and security policies allow an implementation close to the device even with limited hardware resources. The connection to the physical component is always system-dependent and is realized, e.g., via bridges to fieldbuses.

Table 2. Cont.

CPES Requirements according to [4]	OPC UA Features
(iv) CPS-property of every component	The concept of OPC UA considers a migration, so not every component in the overall system has to be a CPES from the beginning, but it can be.
(v) Networked at multiple and large scale	As OPC UA is basically based on IP-based networks, it can adopt the scalability of this technology. The architecture provides unrestricted horizontal and vertical integration.
(vi) Complexity at multiple temporal and spatial scales	OPC UA cannot yet be used in time-sensitive networks (TSN), an extension of the standard is still in preparation. A spatial scaling is, however, problem-free. In addition, OPC UA also offers scalability of functionality owing to its flexible address space.

The high suitability of OPC UA for smart grids is also attested by works such as [58,59], in which the standard is combined with semantic web services or information models for energy management. Existing implementations in limited field devices [60] and at chip level [61] show the applicability for CPES at the sensor level.

4.2. Other Standards

The IEC 61850 [62] standard was originally defined for the automation of legacy substations and distributed generators. The aim of IEC 61850 is the interoperability of electrical systems in substations of all types and brands [63]. By now, IEC 61850 (in combination with other standards, such as IEC 61499) has gained considerable importance for the implementation of smart grids [64,65]. With an abstract, tree-like data model, as well as an abstract data interface, the standard enables the virtualization of physical components in the sense of CPES. To describe all objects, the XML-based Substation Configuration Language (SCL) is used. SCL is often found in electrical substation devices to perform an offline exchange of the configuration between tools. An OPC UA IEC 61850 Companion Specification [49] exists for mapping the data and object model into the address space of OPC UA without loss of semantics.

The Common Information Model (CIM), standardized in IEC 61970/61968, is an energy-specific information model for objects and their relations in the context of energy supply [66]. The model considers numerous aspects, such as generation, transmission, maintenance, and asset management in its objects. Therefore, CIM can also be considered as large domain ontology, and is often used for simulation purposes. The exchange of messages is XML-based. For the exchange of the topology itself, CIM provides a serialization with the Resource Description Framework (RDF) [50]. CIM can be integrated into an OPC UA server by translating the UML descriptions into the OPC UA address space [67]. This combination is suitable for the description of complex CPES.

AutomationML is a data format for the exchange of technical data between heterogeneous production systems. AutomationML enables the modeling of physical and logical plant components as a hierarchical structure of data objects. The description language thus follows an object-oriented paradigm. These objects contain information about plants and plant components, such as topology, interfaces, geometry, kinematics, logic, and behavior. AutomationML is standardized in IEC 62714 [68] and is based on IEC 62424 [69] (CAEX), and the open description language XML. These standards can be combined with OPC UA by applying the AutomationML Companion Specification for OPC UA [70], so the AutomationML data models can make use of the OPC UA functionality for data exchange, communication, and security. In addition, the data model can be used to specify the configuration of an OPC UA server in a standardized way and to make it exchangeable [71]. Other standards more related to smart grids can be found in the review studies [72,73].

5. Case Studies

We conducted our case studies in two different companies in Germany. The first installation was done at a retailer and the second at an automobile manufacturer. Both case studies were based on universal EMS software, in which numerous other data sources, measuring instruments, and data loggers are connected. In this case, the term "universal" refers to the EMS integrating its energy meters across manufacturers and connectors for common communication standards, such as Modbus TCP, being already available in the software.

In both cases, the energy sensor must be implemented as part of a CPES. This provides us with networked sensors, which are necessary for forming smart microgrids and with which we can realize further added value, for example for smart building functions. For non-standardized systems, such as manufacturer-specific data loggers, gateways, or IoT clouds, additional connectors must be developed in the EMS if required.

5.1. Case 1: A Proprietary Retrofit

In this case, we use a radio networked device with a camera and optical character recognition (OCR) to retrofit an electromechanical induction type energy meter with a communication interface, transmitting these values to an energy management system every five minutes. The cyber representation of the counter takes place in an IoT cloud of the camera manufacturer. OCR is a relatively mature and well-researched technology [74] for the digital retrofitting of analog devices, whereby feature extraction and detection without the use of handwriting, while the narrowly defined context and the small character set is not a big challenge. Further work on OCR of energy meters can be followed in [75–77].

Despite the advantageous conditions for text recognition with an energy meter, a good result depends on the initial configuration of the software. The following parameters must be set: differentiation between analog and digital meters, the background color, placement of the meter reading in the image, as well as information about possible partially visible digits owing to the rotary movement. We were able to do this configuration with Windows-based software after gluing the camera module to the counter (Figure 2). The power consumption of the camera module is supplied by a 3.6 V 1600 mAh AA lithium-ion battery from an external box. Alternatively, a power supply via USB cable would be possible.



Figure 2. Mounted camera module on the analog energy meter.

The camera module uses a proprietary, undocumented radio protocol in the 868 MHz ISM band with a transmission rate of 50 kbit/s and AES 128 encryption according to the manufacturer’s specifications. The receiving IP gateway is located in the same IP gateway building, four floors below. The gateway then transmits the measured values to the IoT manufacturer’s cloud service, where the data can be retrieved via a documented application programming interface (API) from the energy management system in JavaScript Object Notation (JSON).

Up to this point, the setup was still easy because we had only moved into the well-documented manufacturer’s world. The effort of the non-standardized system becomes clear in the connection to the universal EMS. As access to the IoT cloud is proprietary, a connector had to be implemented in the EMS software first. This connector offers the user sufficient configuration parameters, such as the entry of API access data and interactive selection from the sensors available in the IoT cloud, so that the implementation can be used for all sensors in this cloud. This multiple-use capability relativizes the extra effort required for non-standard interfaces.

From the link via the connector, the user now generates a measuring point in the EMS and can use it to include the data received from the sensor in the overall energy monitoring. The data transmitted by the sensor are meter readings. The conversion into consumption and costs takes place automatically by the EnM software. Figure 3 shows the result, where the user has created an exemplary dashboard for this sensor.

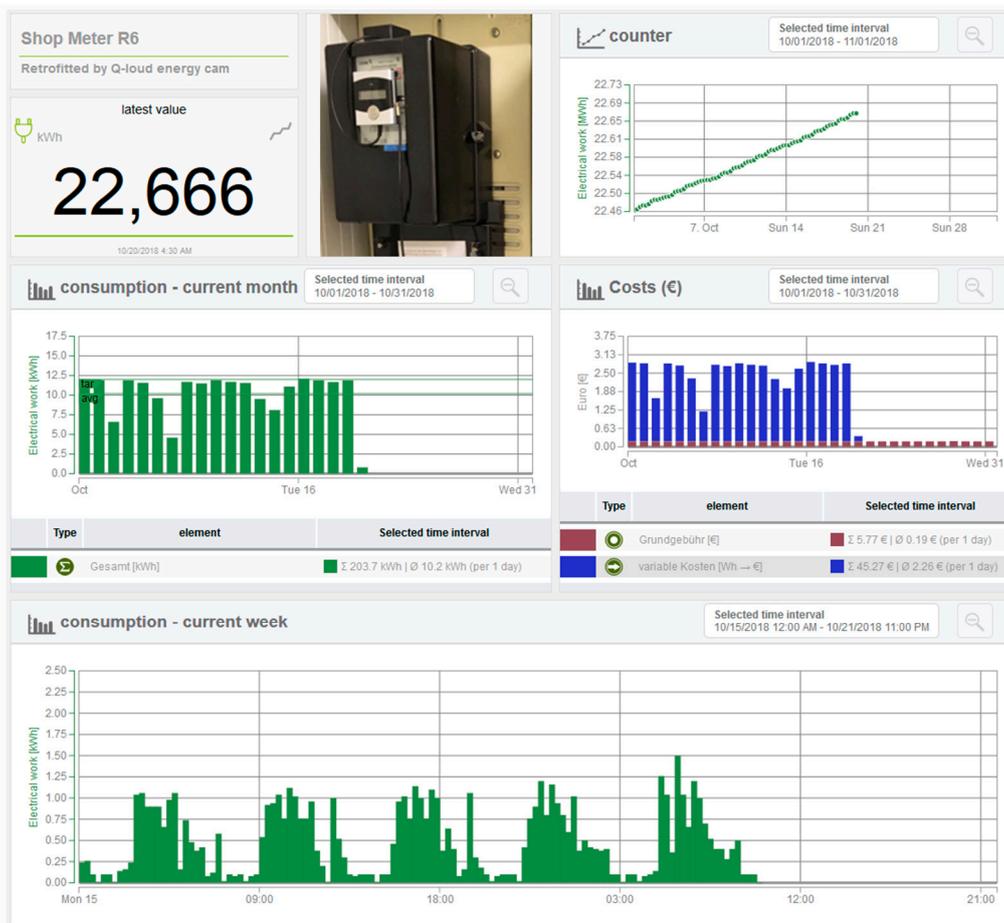


Figure 3. Screenshot of the resulting dashboard.

5.2. Case 2: A Setup Using Standards

In the second use case, we created a setup based on LoRaWAN for transmission using an OPC UA server as a local IoT cloud for the cyber component of the sensor. The goal is a three-phase power

measurement and transmission to the EMS in at least 15-minute intervals. The setup consists of three folding current transformers (CT) with each 63A at 50Hz, shown in Figure 4a, which are connected to the prototypes of a CT bridge (Figure 4b) The measurements of a CT are performed continuously and are recorded in the bridge as counter values. The bridge makes these values available via the LoRaWAN. The power supply of the bridge is done by energy harvesting from the CT. Therefore, it will be operated as LoRa class C device, although the sensor operation does not necessitate this receive mode.



Figure 4. The setup with the CT (a), the CT bridge (b), and the base server (c).

The CT bridge can connect up to 6 CT with maximum 250 A each. The configuration is done by transferring a static XML file via USB. The following parameters are specified: the transformer ratio of each CT and the type of measurement as true root mean square (RMS) or 50 Hz component. As we were interested in the power consumption and not in the real current, we chose the 50 Hz component. The consumption P equals:

$$P = U \times I_{50Hz} \times \cos(\varphi) \tag{2}$$

The factory voltage U is known in most cases or must be measured separately; the power factor $\cos(\varphi)$ is indicated on the label of the machine. The other parameters of the configuration apply to the LoRaWAN transmission: a send interval in seconds, the network key, the application session key, the spread factor (SF), and the receive port in the base station. Owing to the short distance to the base station and the limited power supply by energy harvesting, we chose SF = 10 and an interval of 900.

The LoRa data frame has 26 bytes and contains the values of the six currents in ampere-seconds, as well as two values for temperature in degrees Celsius and humidity in percent (Figure 5). The semantics of this data is described via the JavaScript object notation (JSON) [78]. Figure 6 shows an abbreviated copy of this description.

CT1 [32 bit]	CT2 [32 bit]	CT3 [32 bit]	CT4 [32 bit]	CT5 [32 bit]	CT6 [32 bit]	TEMP [8 bit]	HUM [8 bit]
-----------------	-----------------	-----------------	-----------------	-----------------	-----------------	-----------------	----------------

Figure 5. Our LoRa data frame.

```

{
  "name": "CT-Bridge",
  "portconfigs": [
    {
      "direction": "uplink",
      "port": 3,
      "values": [
        {
          "byteorder": 1,
          "multiplier": 1,
          "name": "AC1_counter",
          "type": 13,
          "unit": "As",
          "valuetype": "value"
        },
        {
          "byteorder": 1,
          "multiplier": 1,
          "name": "AC2_counter",
          "type": 13,
          "unit": "As",
          "valuetype": "value"
        },
        // SHORTENED: same for AC3 ... AC6
        {
          "byteorder": 1,
          "multiplier": 1,
          "name": "Temperature",
          "type": 1,
          "unit": "°C",
          "valuetype": "value"
        },
        // SHORTENED: humidity analogue to temp
      ]
    }
  ]
}

```

Figure 6. LoRa payload description in JavaScript Object Notation (JSON).

The radio counterpart provides a LoRaWAN base server, which is installed in an IT switch cabinet in the same production hall about 30 m away (Figure 4c). This is a commercially available device with a built-in LoRaWAN concentrator and network server, which operates in the ISM frequency band 863–870 MHz. The hardware platform with a TI AM33x chip is based on a Yocto embedded linux system. The LoRa application server, network server, and the gateway are implemented in C++ and the JavaScript based environment NodeJS. The base server supports two operating modes for packet forwarding: either as a pure LoRaWAN concentrator for use with an external commercial network server (a LoRa NaaS) or with internal packet relay to a built-in network server and a built-in OPC UA application server. We use the latter one. In this mode, the received data is interpreted and written into the address space of the OPC UA server. The JSON description of the payload is also entered and the values are connected to the OPC UA address space. The measured counter readings are now available on the OPC UA server.

The connection between the OPC UA server and the EMS is established via a virtual private network (VPN). The EMS has a built-in OPC UA client that can be configured by the user via a wizard-guided user interface. After selecting the server address, the security profile, and the authentication (via login or certificate), the address space of the OPC UA server can be browsed, and the desired value of the node can be assigned to a measurement point in EMS (Figure 7). A visualization of the measurements of all three CTs is shown in (Figure 8). In this analysis, the conversion from Ah to A was performed by the EMS.

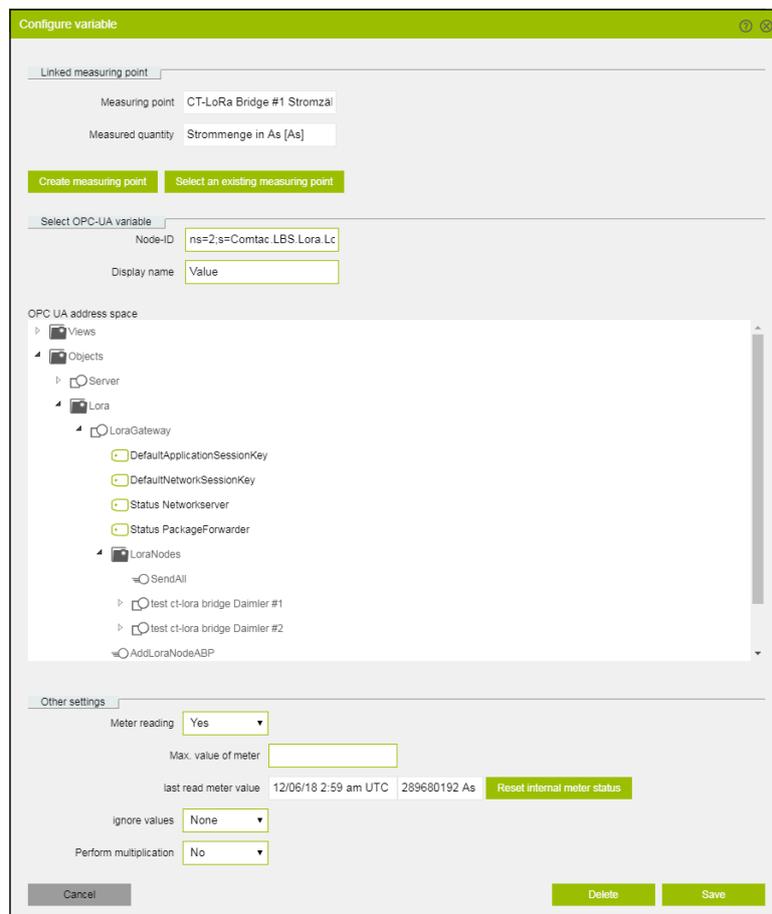


Figure 7. OPC UA client setup in the energy management system (EMS).

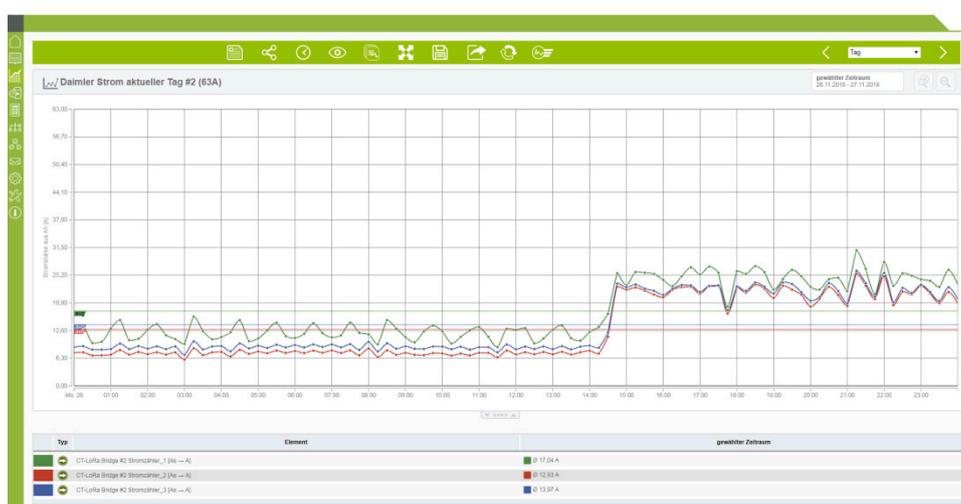


Figure 8. EMS chart of the measured current transformers (CT).

The numerous steps for installation and configuration of the CT bridge, the LoRa base server, and the EMS result mainly from the prototypical character of the devices. The CT bridge is still a hardware prototype, in which configuration and software updates are carried out via manually imported files without any user interface.

5.3. Cost Comparison

A comparison of the costs for implementation, configuration, and hardware support between the two approaches is shown in Table 3. It must be highlighted that direct comparability is limited because of the different procedures and cost types. In the first case, it took approximately one hour of work to mount the camera and configure the vendor's IoT cloud. This same amount of effort would be required for each additional camera sensor. In the second case, the LoRa base server, the LoRaWAN infrastructure, and the LoRa payload had to be configured and tested, which took about three hours. Each CT bridge was then integrated into the LoRaWAN infrastructure, which took a few minutes.

Table 3. Cost comparison (h = working hours).

	Case 1 (without Standards)	Case 2 (with Standards)
Sensor configuration (per sensor)	1.5 h	< 0.25 h
Sensor configuration (once per setup)	0 h	3 h
Energy Management System (EMS) implementation (once)	128 h	720 h
EMS configuration (once per setup)	0.5 h	0.5 h
EMS configuration (per sensor)	<0.25 h	<0.25 h
Hardware fix cost per setup	0 €	900 € (market price)
Hardware variable costs per sensor	210 € (market price)	60 € (estimated w/o cu. transform)

In the EMS, the respective data source's interface had to be implemented as a device driver with a graphical user interface. The representational state transfer (REST) API for the IoT cloud required 16 days of effort, including a simple, interactive configuration of the data source and mapping to measurement points. For the second case, it took 90 days to implement a universal OPC UA client, including security profiles and browsing through the offered OPC UA address space. The main effort in both cases was implementing the user interfaces. The configuration per setup and per sensor in the EMS was similar in both cases; the configuration of the data source (IoT cloud or OPC UA server) only occurred once per setup.

While our costs for the OCR camera were known in the first case, at €210 net without a quantity discount, we could only quote the invoice for the LoRa base server at €900 in the second case. For the CT bridge, which is not yet available on the market, a price of about €60 was estimated.

Beyond cost, it must also be considered that no IoT cloud of a third-party provider was involved in the second case. The data, thus, remains in the company's sphere of sovereignty at all times.

6. Discussion

The typical smart microgrid, consisting of consumers, a power generator, power storage, and a control unit, can already be delivered, but in most cases, all from a single source. Without appropriate standards, however, this CPES will remain an island in a multi-stakeholder smart grid. The example of energy management shows that more complex CPES will only be possible using a mix of several standards for different tasks. For the time-critical communication processes in CPES, such as switching operations in power grids, other advanced technologies are needed. The standards presented here are not—or are only partially—suitable for this purpose.

Comparing our two presented use cases, we can state that the non-standardized solution in the first case was easily installed because the product and IoT cloud came from the same manufacturer and worked well together. The usability of this solution was subjectively perceived as being good. For simple monitoring, one can stop at this point, leave the meter data in the manufacturer's IoT

cloud, and be satisfied with the rudimentary visualization offered. For application in heterogeneous Smart Grids, this solution would be possible, in principle, through an API. However, for every other manufacturer, new API connectors would have to be programmed, which would mean disproportionately high development expenditure. Therefore, we do not consider this approach suitable for Smart Grids. In applying our EMS, the development of an API connector containing a user interface for configuration took 128 h of effort, which is only worthwhile if a larger number of sensors from the same manufacturer's IoT have to be connected.

If, however, the data are to be processed in a heterogeneous CPES and combined with data from other sources, the need for standards becomes clear. Our second setup showed the use of open standards. LoRaWAN was applied for the radio connection. As this is the only LPWAN technology available on the market for self-operation, using NaaS was not considered in this application. The LoRa deployment showed it is particularly suitable for CPES. The radio coverage of a base station of several kilometers should be sufficient for most smart microgrids; the good building penetration offers reliability and the various device classes allow for battery-powered sensors with a service life of up to 10 years. The need for strong security mechanisms is also met by the LoRa architecture, as the data is transmitted with AES-128 encryption and operator and application data can be separated using a network key and an application key. In summary, LoRa can be certified as being highly suitable for use in smart grids, at least if the application does not require time-critical transmissions or large amounts of data.

Regarding standardization, LoRa's Achilles' heel is the freely configurable user data package, so cross-manufacturer radio components, in particular, cannot be combined or can only be combined with a certain amount of effort. In the example shown, vendor-independent standardization has only become possible by exposing a non-standardized LoRa data frame in the standard notation. This step meant great impairment of usability. A transfer of this JSON description into the configuration of the base station provides the semantics of the sensor data. This solves the technical problem, but user-friendly implementation would only be achieved if the payload semantics were already provided in the form of existing, selectable device drivers. For this purpose, the LoRa standard would have to be extended by a uniform payload description notation, which could be inspired by the JSON implementation presented here.

The OPC UA framework can make a major contribution to the interoperability of smart grids far beyond industrial production environments, as it already fulfills numerous requirements for CPES, as shown in Table 2. OPC UA's address space provides an ideal location for the cyber components of Smart Grids and CPES. Reduced server profiles allow OPC UA to be easily integrated into embedded systems, such as sensors, while the flexible address space and the CS support also allow for large-scale smart grids. Only the missing integration of time-sensitive networks (TSN) reduces the application scope. Although the implementation effort for the more complex OPC UA client in the EMS was high at 720 h, this can now integrate any OPC UA sensor from any manufacturer, so it appears this effort is a profitable investment. The client's user interface offers high usability for sensor integration. The connection of the OPC UA server to the EMS requires only a few mouse clicks and the sensor data is available to any other OPC UA client in the grid. The employed base server should be extended by the OPC UA functionality of historical data access (HDA), so it can also fulfill the function of a data logger for an EMS. As, in our case, meter readings are transferred, the loss of a value is not critical. It would also be desirable to have a CS for energy sensors in the special field of application EMS, similar to [79] but less extensive.

7. Conclusions

Numerous research projects on modeling CPES show the networking of smart (micro)grids places high demands on interoperability between many heterogeneous components. In practice, this can only be achieved by having suitable, open standards. This work provides an overview of suitable candidates for CPES standards, particularly for implementing sensors in smart microgrids, as promising standards,

such as OPC UA and LoRa, already exist. A use case shows the practical application of these standards and compares the implementation with a second setup in a different context using non-standardized technologies. Proprietary technologies are easy to integrate but leave behind isolated systems. The greater complexity of using standards offers significantly greater flexibility in integrating sensors into the overall CPES concept of smart microgrids. The paper indicates the need for further research for CPES standardization. Future work concerning real-time communication between smart grids and the semantic definition of protocol payloads in existing standards is necessary to achieve sufficient interoperability between components. For LoRa, we propose an extension of the standard by a common description notation for the data frame. The concept of JSON notation presented in this article could provide a basis for the standard's future extension.

Author Contributions: Conceptualization and methodology, M.C.K. and A.D.T.; setup case 1, K.S.; setup case 2, M.C.K., K.S., and B.K., writing, review, and editing, M.C.K.; supervision and paper revision, A.D.T.

Funding: This research received no external funding.

Acknowledgments: The authors thank Dieter Braun and Holger Heidenblut for their technical support.

Conflicts of Interest: The authors declare no conflict of interest.

References

- Farhangi, H. The path of the smart grid. *IEEE Power Energy Mag.* **2010**, *8*, 18–28. [[CrossRef](#)]
- Saber, A.Y.; Venayagamoorthy, G.K. Efficient Utilization of Renewable Energy Sources by Gridable Vehicles in Cyber-Physical Energy Systems. *IEEE Syst. J.* **2010**, *4*, 285–294. [[CrossRef](#)]
- Wolf, W.H. Cyber-physical systems. *IEEE Comput.* **2009**, *42*, 88–89. [[CrossRef](#)]
- Macana, C.A.; Quijano, N.; Mojica-Nava, E. A survey on Cyber Physical Energy Systems and their applications on smart grids. In Proceedings of the 2011 IEEE PES Conference on Innovative Smart Grid Technologies Latin America (ISGT LA), Medellin, DC, USA, 19–21 October 2011. [[CrossRef](#)]
- Yamamoto, Y. Pricing electricity from residential photovoltaic systems: A comparison of feed-in tariffs, net metering, and net purchase and sale. *Sol. Energy* **2012**, *86*, 2678–2685. [[CrossRef](#)]
- Evans, D. The internet of things: How the next evolution of the internet is changing everything. *Cisco White Pap.* **2011**, *1*, 1–11.
- Kleissl, J.; Agarwal, Y. Cyber-physical energy systems. In Proceedings of the 47th Design Automation Conference on DAC Textquotesingle10, Anaheim, CA, USA, 13–18 June 2010. [[CrossRef](#)]
- Agarwal, Y.; Balaji, B.; Gupta, R.; Lyles, J.; Wei, M.; Weng, T. Occupancy-driven energy management for smart building automation. In Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building—BuildSys Textquotesingle10, Zurich, Switzerland, 2 November 2010. [[CrossRef](#)]
- Wang, W.; Hong, T.; Li, N.; Wang, R.Q.; Chen, J. Linking energy-cyber-physical systems with occupancy prediction and interpretation through WiFi probe-based ensemble classification. *Appl. Energy* **2019**, *236*, 55–69. [[CrossRef](#)]
- Morvaj, B.; Lugaric, L.; Krajcar, S. Demonstrating smart buildings and smart grid features in a smart energy city. In Proceedings of the 2011 3rd International Youth Conference on Energetics (IYCE), Leiria, Portugal, 7–9 July 2011; pp. 1–8.
- Ranky, P.G. Sustainable energy management and quality process models based on ISO 50001:2011 the International Energy Management Standard. In Proceedings of the 2012 IEEE International Symposium on Sustainable Systems and Technology (ISSST), Boston, MA, USA, 16–18 May 2012. [[CrossRef](#)]
- Krutwig, M.; Starosta, K. Characterization, Classification and Assessment of Non-Energy Benefits of Energy Efficiency Measures. In Proceedings of the 30th IBIMA Conference, Madrid, Spain, 8–9 November 2017.
- Rao, P.; Muller, M.R.; Gunn, G. Conducting a metering assessment to identify submetering needs at a manufacturing facility. *Cirp J. Manuf. Sci. Technol.* **2017**, *18*, 107–114. [[CrossRef](#)]
- Ilic, M.D.; Xie, L.; Khan, U.A.; Moura, J.M. Modeling of future cyber-physical energy systems for distributed sensing and control. *IEEE Trans. Syst. Man and Cybern. Part A: Syst. Hum.* **2010**, *40*, 825–838. [[CrossRef](#)]

15. Palensky, P.; Widl, E.; Elsheikh, A. Simulating Cyber-Physical Energy Systems: Challenges, Tools and Methods. *IEEE Trans. Syst. Man and Cybern. Syst.* **2014**, *44*, 318–326. [[CrossRef](#)]
16. Shi, L.; Dai, Q.; Ni, Y. Cyber-physical interactions in power systems: A review of models, methods, and applications. *Electr. Power Syst. Res.* **2018**, *163*, 396–412. [[CrossRef](#)]
17. Potdar, V.; Sharif, A.; Chang, E. Wireless Sensor Networks: A Survey. In Proceedings of the 2009 International Conference on Advanced Information Networking and Applications Workshops, Bradford, UK, 26–29 May 2009. [[CrossRef](#)]
18. Bardyn, J.-P.; Melly, T.; Seller, O.; Sornin, N. IoT: The era of LPWAN is starting now. In Proceedings of the 42nd European Solid-State Circuits Conference, Lausanne, Switzerland, 12–15 September 2016; pp. 25–30. [[CrossRef](#)]
19. 3GPP. TR 45.820, *Cellular System Support for Ultra-Low Complexity and Low Throughput Internet of Things (CIoT)*, Rel. 13; 3GPP: Nice, France, 2016.
20. Akyildiz, I.F.; Wang, X. A survey on wireless mesh networks. *IEEE Commun. Mag.* **2005**, *43*, S23–S30. [[CrossRef](#)]
21. Gungor, V.C.; Lu, B.; Hancke, G.P. Opportunities and Challenges of Wireless Sensor Networks in Smart Grid. *IEEE Trans. Ind. Electron.* **2010**, *57*, 3557–3564. [[CrossRef](#)]
22. Yaqoob, I.; Hashem, I.A.T.; Mehmood, Y.; Gani, A.; Mokhtar, S.; Guizani, S. Enabling Communication Technologies for Smart Cities. *IEEE Commun. Mag.* **2017**, *55*, 112–120. [[CrossRef](#)]
23. Verma, L.; Fakharzadeh, M.; Choi, S. Wifi on steroids: 802.11AC and 802.11AD. *IEEE Wirel. Commun.* **2013**, *20*, 30–35. [[CrossRef](#)]
24. Gomez, C.; Paradells, J. Wireless home automation networks: A survey of architectures and technologies. *IEEE Commun. Mag.* **2010**, *48*, 92–101. [[CrossRef](#)]
25. Mahmood, A.; Javaid, N.; Razzaq, S. A review of wireless communications for smart grid. *Renew. Sustain. Energy Rev.* **2015**, *41*, 248–260. [[CrossRef](#)]
26. Bocker, S.; Arendt, C.; Wietfeld, C. On the suitability of Bluetooth 5 for the Internet of Things: Performance and scalability analysis. In Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017. [[CrossRef](#)]
27. Gomez, C.; Oller, J.; Paradells, J. Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology. *Sensors* **2012**, *12*, 11734–11753. [[CrossRef](#)]
28. Darroudi, S.; Gomez, C. Bluetooth Low Energy Mesh Networks: A Survey. *Sensors* **2017**, *17*, 1467. [[CrossRef](#)] [[PubMed](#)]
29. Wi-SUN Alliance Website. Available online: <https://www.wi-sun.org/> (accessed on 4 December 2018).
30. Harada, H.; Mizutani, K.; Jujiwara, J.; Mochizuki, K.; Obata, K.; Okumura, R. IEEE 802.15.4g Based Wi-SUN Communication Systems. *IEICE Trans. Commun.* **2017**, *E100.B*, 1032–1043. [[CrossRef](#)]
31. Weightless SIG Website. Available online: <http://www.weightless.org/> (accessed on 4 December 2018).
32. Sornin, N.; Luis, M.; Eirich, T.; Kramp, T.; Hersent, O. *LoRaWAN Specification*, Available from the LoRa Alliance; LoRa Alliance: Fremont, CA, USA, 2015.
33. Sigfox Website. Available online: <https://www.sixfox.com> (accessed on 2 September 2018).
34. Ratasuk, R.; Mangalvedhe, N.; Ghosh, A.; Vejlgaard, B. Narrowband LTE-M System for M2M Communication. In Proceedings of the 2014 IEEE 80th Vehicular Technology Conference (VTC2014-Fall), Vancouver, BC, Canada, 14–17 September 2014. [[CrossRef](#)]
35. Vejlgaard, B.; Lauridsen, M.; Nguyen, H.; Kovács, I.Z.; Mogensen, P.; Sorensen, M. Coverage and capacity analysis of sigfox, lora, gprs, and nb-iot. In Proceedings of the 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), Sydney, Australia, 4–7 June 2017; pp. 4–7.
36. Ingenu Inc. Website. Available online: <https://www.ingenu.com/> (accessed on 6 December 2018).
37. Astely, D.; Dahlman, E.; Furuskar, A.; Jading, Y.; Lindstrom, M.; Parkvall, S. LTE: The evolution of mobile broadband. *IEEE Commun. Mag.* **2009**, *47*, 44–51. [[CrossRef](#)]
38. Wang, Y.-P.E.; Lin, X.; Adhikary, A.; Grovlen, A.; Sui, Y.; Blankenship, Y.; Bergman, J.; Razaghi, H.S. A Primer on 3GPP Narrowband Internet of Things. *IEEE Commun. Mag.* **2017**, *55*, 117–123. [[CrossRef](#)]
39. Lauridsen, M.; Kovacs, I.Z.; Mogensen, P.; Sorensen, M.; Holst, S. Coverage and Capacity Analysis of LTE-M and NB-IoT in a Rural Area. In Proceedings of the 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall), Montreal, QC, Canada, 18–21 September 2016. [[CrossRef](#)]

40. Ratasuk, R.; Vejlgard, B.; Mangalvedhe, N.; Ghosh, A. NB-IoT system for M2M communication. In Proceedings of the Wireless Communications and Networking Conference (WCNC), Doha, Qatar, 3–6 April 2016; pp. 1–5. [CrossRef]
41. Zayas, A.D.; Merino, P. The 3GPP NB-IoT system architecture for the Internet of Things. In Proceedings of the 2017 IEEE International Conference on Communications Workshops (ICC Workshops), Paris, France, 21–25 May 2017. [CrossRef]
42. Blenn, N.; Kuipers, F. LoRaWAN in the wild: Measurements from the things network. *arXiv* **2017**, arXiv:1706.03086.
43. TTN the Things Network. Available online: <https://www.thethingsnetwork.org> (accessed on 11 December 2018).
44. SemtechCorp. *LoRa™ Modulation Basics, AN1200.22*; Semtech Corporation: Camarillo CA, USA, 2015.
45. Reynders, B.; Pollin, S. Chirp spread spectrum as a modulation technique for long range communication. In Proceedings of the 2016 Symposium on Communications and Vehicular Technologies (SCVT), Mons, Belgium, 22–22 November 2016; pp. 1–5. [CrossRef]
46. Goursaud, C.; Gorce, J.M. Dedicated networks for IoT: PHY/MAC state of the art and challenges. *Eai Endorsed Trans. Internet Things* **2015**, *1*, 150597. [CrossRef]
47. ETSI. *Short Range Devices (SRD); Radio Equipment to Be Used in the 25 MHz to 1000 MHz Frequency Range With Power Levels Ranging up to 500 mW*; ETSI: Nice, France, 2012; Volume 330, pp. 220–221.
48. Augustin, A.; Yi, J.; Clausen, T.; Townsley, W. A Study of LoRa: Long Range & Low Power Networks for the Internet of Things. *Sensors* **2016**, *16*, 1466. [CrossRef]
49. Monostori, L.; Kádár, B.; Bauernhansl, T.; Kondoh, S.; Kumara, S.; Reinhart, G.; Sauer, O.; Schuh, G.; Sihm, W.; Ueda, K. Cyber-physical systems in manufacturing. *Cirp Ann.* **2016**, *65*, 621–641. [CrossRef]
50. Rehbein, D.A.; Pederson, A. Impact of the OLE for Process Control (OPC) standard on the process industry. In Proceedings of the Industrial Computing Conference, Chicago, IL, USA, 6–11 October 1996; Research Triangle Park, NC, USA; Volume 6, pp. 285–293.
51. OPCFoundation. *OPC UA Specification: Part 1—Concepts, Core Specification Parts, Version 1.04*; OPC Foundation: Scottsdale, AZ, USA, 2017.
52. Website OPCFoundation. Available online: <https://opcfoundation.org/> (accessed on 2 December 2018).
53. OPCFoundation. *OPC UA Specification: Part 3—Address Space Model, Core Specification Parts, Version 1.04*; OPC Foundation: Scottsdale, AZ, USA, 2017.
54. OPCFoundation. *OPC UA Specification: Part 5—Information Model, Core Specification Parts, Version 1.04*; OPC Foundation: Scottsdale, AZ, USA, 2017.
55. OPCFoundation. *OPC UA Specification: Part 14—Pub Sub, Version 1.04*; OPC Foundation: Scottsdale, AZ, USA, 2018.
56. OPCFoundation. *OPC UA Specification: Part 2—Security Model, Core Specification Parts, Version 1.04*; OPC Foundation: Scottsdale, AZ, USA, 2018.
57. OPCFoundation. *OPC UA Specification: Part 7—Profiles, Core Specification Parts, Version 1.04*; OPC Foundation: Scottsdale, AZ, USA, 2017.
58. Matzler, S.; Wollschlaeger, M.; Fernbach, A.; Kastner, W.; Huschke, M. An OPC UA cross-domain information model for energy management in automation systems. In Proceedings of the IECON 2013-39th Annual Conference of the IEEE Industrial Electronics Society, Vienna, Austria, 10–13 November; pp. 7513–7518.
59. Rohjans, S.; Fensel, D.; Fensel, A. OPC UA goes semantics: Integrated communications in smart grids. In *ETFA2011*; IEEE: New York, NY, USA, 2011.
60. Veichtlbauer, A.; Ortmayer, M.; Heistracher, T. OPC UA integration for field devices. In Proceedings of the 2017 IEEE 15th International Conference on Industrial Informatics (INDIN), Emden, Germany, 24–26 July 2017. [CrossRef]
61. Imtiaz, J.; Jasperneite, J. Scalability of OPC-UA down to the chip level enables Internet of Things. In Proceedings of the 2013 11th IEEE International Conference on Industrial Informatics (INDIN), Bochum, Germany, 29–31 July 2013. [CrossRef]
62. IEC. *IEC TR 61850-1:2013 Communication Networks and Systems for Power Utility Automation—Part 1: Introduction and Overview (Edition 2.0)*; IEC: Geneva, Switzerland, 2013.
63. Mackiewicz, R.E. Overview of IEC 61850 and Benefits. In *2005/2006 PES TD*; IEEE: New York, NY, USA, 2006. [CrossRef]

64. Zhabelova, G.; Vyatkin, V. Multiagent Smart Grid Automation Architecture Based on IEC 61850/61499 Intelligent Logical Nodes. *IEEE Trans. Ind. Electron.* **2012**, *59*, 2351–2362. [[CrossRef](#)]
65. Higgins, N.; Vyatkin, V.; Nair, N.-K.C.; Schwarz, K. Distributed Power System Automation with IEC 61850, IEC 61499, and Intelligent Control. *IEEE Trans. Syst. Man and Cybern. Part C (Appl. Rev.)* **2011**, *41*, 81–92. [[CrossRef](#)]
66. McMorran, A.W. An introduction to iec 61970-301 & 61968-11: The common information model. *Univ. Strathclyde* **2007**, *93*, 124.
67. Rohjans, S.; Uslar, M.; Appelrath, H.J. OPC UA and CIM: Semantics for the smart grid. In *IEEE PES T&D 2010*; IEEE: New York, NY, USA, 2010. [[CrossRef](#)]
68. IEC. *IEC 62714-1: 2014 Engineering Data Exchange Format for Use in Industrial Automation Systems Engineering—Automation Markup Language—Part 1*; IEC: Geneva, Switzerland, 2014; Volume 1, pp. 62714–62722.
69. IEC. *IEC 62424 Representation of Process Control Engineering-Requests in P&I Diagrams and Data Exchange between P&ID Tools and PCE-CAE Tools*; IEC: Geneva, Switzerland, 2008.
70. OPC Foundation. *OPC UA OPC UA Information Model for AutomationML, Release 1.00.00, February 22th, 2016*; OPC Foundation: Scottsdale, AZ, USA, 2016.
71. Henßen, R.; Schleipen, M. Interoperability between OPC UA and AutomationML. *Procedia Cirp* **2014**, *25*, 297–304. [[CrossRef](#)]
72. Rohjans, S.; Uslar, M.; Bleiker, R.; González, J.; Specht, M.; Suding, T.; Weidelt, T. Survey of smart grid standardization studies and recommendations. In *Proceedings of the 2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Gaithersburg, MD, USA, 4–8 October 2010; pp. 583–588.
73. Gungor, V.C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G.P. Smart Grid Technologies: Communication Technologies and Standards. *IEEE Trans. Ind. Inform.* **2011**, *7*, 529–539. [[CrossRef](#)]
74. Mori, S.; Suen, C.Y.; Yamamoto, K. Historical review of OCR research and development. *Proc. IEEE* **1992**, *80*, 1029–1058. [[CrossRef](#)]
75. Cortez, P.; Felix, J.; Girão, A.; Frota, J.; Bessa, J. An OCR system for numerals applied to energy meters. *IEEE Lat. Am. Trans.* **2014**, *12*, 957–964. [[CrossRef](#)]
76. Elrefaei, L.A.; Bajaber, A.; Natheir, S.; AbuSanab, N.; Bazi, M. Automatic electricity meter reading based on image processing. In *Proceedings of the 2015 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT)*, Amman, Jordan, 3–5 November 2015; pp. 1–5. [[CrossRef](#)]
77. Castells-Rufas, D.; Carrabina, J. Camera-based Digit Recognition System. In *Proceedings of the 2006 13th IEEE International Conference on Electronics, Circuits and Systems*, Nice, France, 10–13 December 2006. [[CrossRef](#)]
78. Crockford, D. *The Application/Json Media Type for Javascript Object Notation (Json)*; Request for Comments (RFC), July 2006.
79. OPC Foundation. *OPC UA IEC 61850 Companion Specification, Release Candidate Version 1.0, February 5th, 2018*; OPC Foundation: Scottsdale, AZ, USA, 2016.

