Energy Informatics

RESEARCH Open Access

Cybersecurity in smart local energy systems: requirements, challenges, and standards

Siyuan Dong[1*], Jun Cao[2], David Flynn[3] and Zhong Fan[1*]

*Correspondence: michaelsec9103@gmail.com; Z.Fan@keele.ac.uk

[1] School of Computing and Mathematics, Keele University, Keele, Newcastle-under-Lyme ST5 5BG, UK
[2] Environmental Research and Innovation Department, Luxembourg Institute of Science and Technology, 4362 Belval, Luxembourg
[3] James Watt School of Engineering, University of Glasgow, Glasgow G12 8QQ, UK

Abstract

Smart local energy system (SLES) can support tailored regional solutions through the orchestration of cyber physical architectures, coordinating distributed technologies, with operational and forecasting models across all energy actors. Unprecedented access to new information, data streams and remotely accessible control can substantially benefit the multi-objective optimisation of multiple performance metrics. Given the expansion of this internet of things (IoT) and cyber-physical system (CPS), it is important to not only design effective detection and management of potential cybersecurity issues, but also to address the challenges in having affective and adaptive governance—built on standards to ensure the security of the IoT to minimise risks and harms to all users. This study conducts an extensive and critical investigation into the existing standards and identifies areas to focus on as to support the expansive adoption of cyber physical networks. Although existing standards and protocols are highly fragmented, our findings suggest that many of them can meet the requirements of the applications and infrastructures of SLES. Additionally, many standards have been introduced to protect information security and personal privacy due to their increasing importance. The research also suggests that the industry needs to produce more affordable and cyber-secured devices and services. For the government and regulators, relevant guidelines on the minimum function and security requirements for applications should be provided. Additionally, compliance testing and certifications should be in place and carried out by an independent third party to ensure the components of SLES ecosystem with a satisfied security level by design.

Keywords: Cybersecurity, Standards, Smart local energy system, Distributed energy resource

Introduction

In the past few years, the global investment into net zero future has been focusing on distributed energy resources (DERs). This encompasses both top-down critical infrastructure investments such as offshore wind farms, as well as community level investments, such as community energy system. They emerged as a promising solution to reduce the carbon emissions and help the transmission of existing energy industry towards a cleaner and more decentralised manner. The proportion of the renewables has significantly increased in the total energy production mix in the UK in the recent years (Elliott 2004), such as offshore wind. Similar to most countries, the UK's energy system

is based upon the "supplier hub model" (Ofgem 2017), which means the electricity is generated from energy suppliers, transmitted via transmission and distribution networks, and finally consumed by end-users. The newly built large-scale DER sites are usually far away from the consumer end. Together with increasing energy demand, they pose new challenges to the existing energy system, which may require additional expensive generation assets and network reinforcement and expansion. However, there is an alternative approach, solving the problem at the near-consumer side.

The demand for more active energy management and more affordable energy supply have contributed to the rapid growth in DER deployments at the near-user end (Office of Gas and Electricity Markets 2017). Customers therefore will access to more complex and blended energy products, empowered by smart technologies and algorithms to manage their energy demand remotely and autonomously. Generators will need to optimise the operation of their assets to develop different business models and unlock the value (Energy Digitalisation Taskforce 2022). Additionally, they also need to make the best use of the enormous flexibility that potentially benefits the whole system, while maintaining the stability throughout the system at all levels. The network operators therefore must seek for new solutions to the problems and challenges. For the better integration, some potential solutions have been proposed to embrace the idea of localising energy supply and provide additional flexibility and resilience, such as virtual power plants (Rodríguez-Molina et al. 2014), local energy market (Mengelkamp et al. 2018), aggregators (Burger et al. 2017), and community energy system.

Amongst all potential solutions, SLES is considered as a promising pathway for fast-track decarbonisation through "green" tech integration. It can also facilitate a more effective and localised operation (Ford et al. 2021) with enhanced energy equity and justice. The extraordinary scalability and replicability enable SLES to have more flexible implementations. It can be as small as a community energy system and can be scaled up to be as a part of the main grid. Previous study (Ford et al. 2021) identified the benefits of SLES, including effective provision of energy service, enabling flexibility within and across energy vectors, improved resilience, and ability to cope with failure, etc. SLES substantially benefits from its complex information and communication technology (ICT) infrastructures that can provide enhanced observability and distributed control on DERs. The smart elements include both physical smart devices and digital functionality (Mokhtar et al. 2021; Kirli et al. 2022). The physical smart devices, consisted of various IoT technologies, have enhanced the interoperation of the grid system by providing multi-directional information flow with adequate data from users, substations, transmission, and generation sides. More recently, there is increasing focus on the digital functionalities such as artificial intelligence (AI) and analytics. These smart elements contribute to the provision of a real-time balance, monitoring, and control at high granularity and accuracy. Stakeholders in the SLES can benefit from such system setup and operation, therefore an autonomous and locally self-sufficient energy system can be achieved.

However, the substantial information exchanged between the smart elements, can lead to an outstanding concern regarding the security, because of the competing interests of different parties or stakeholders, high level of interdependence, and social complexity (Jurcut et al. 2020). In general, there are two categories of threats, operation threats and

information threats. There are mainly three types of operation threats, including data manipulation, impersonation, and denial of service (DoS) (Gunduz and Das 2020). The second category of threats is the privacy and information threat. The smart elements will inevitably increase significant data exchanges, elevating the security of privacy and information to an extremely important level. Although more attention has been distributed to this area, there is still a lack of understanding in the digital transition of the energy system and big data. The SLES is essentially reliant upon the accurate measurements and digitalised and interactive management through the smart elements. The data-driven analysis is supporting and on occasion leading operational and planning decisions across all services in the energy sector. In this way, its integrity is paramount to how we live now, and in the future.

Apart from the threats, the SLES will require many advanced devices to participate in the process, and it therefore is necessary to consider the compatibility for low-end devices. Previous studies suggested that existing standards and guidelines have not provided any clear definition of roles that different parties play, and a common understanding of key security requirements is yet to be shared (Labib et al. 2019). Additionally, the inherent vulnerabilities may potentially expose the system to potential attacks (Sha et al. 2018), because the controlling and monitoring is undertaken based on internet-protocols and off-the-shelf solutions. Similar to smart grid, the nature of SLES can be considered as part of critical infrastructures, which will likely draw unwanted attention and become the target of cyber-attack. It therefore is vital to undertake thorough examination on the components and identify existing vulnerabilities to ensure the main security objectives are met. To protect the IoT from the potential external cyberattacks, it requires not only effective threat detection and management, but also a considerable number of well-designed standards are necessary to ensure the security of the IoT system to minimise the risks. It is therefore worth investigating the currently existing standards and identify the area to focus on in the future.

The rest of the paper is structured as follows: in "Background of SLES" section, the background of SLES is described, including its key components, features and benefits, and potential challenges and risks; "Cybersecurity of smart local energy systems" section introduces general cybersecurity objectives and requirements for SLES and general energy system, and also cross compare the existing standards related to cybersecurity; "Discussion and suggestion" section discusses and explains the main findings and proposes several suggestions for SLES planning and development; and conclusions and future works are summarised in "Conclusion".

Background of SLES

In general, there are many key components comprising an energy system, including production, conversion, transmission, distribution and consumption (Alanne and Saari 2006). This structure also works for a small energy system at a local level, such as a community or a building, and SLES. SLES can transmit electric and information flow during the operation. The electric flow starts from energy producers and finish at end users in the traditional system. To some extent, the SLES operates in a similar way to the virtual power plants that can monitor and operate embedded DER assets to trade the generated power based on different market environments. Additionally, different

shareholders and components communicate through a bi-directional communication flow, with the assistance of substantial number of sensors, actuators other smart objects (Antonopoulos et al. 2021). However, unlike the VPPs, the SLES can provide required service to protect grid stability and can even operate in island mode. Although there has not been any clear definitions or explicit frameworks for SLES, some key elements and functions have been identified in previous studies (Ford et al. 2021).

Key components of SLES

To deliver these features, a localised and highly automated system infrastructure is required. Many components are connected to the SLES for operating, monitoring, and controlling electricity flow and measurements. The SLES requires involvement of different stakeholders comprising of various domains, such as service provider domain, communication network, grid domain, advanced metering infrastructure and customer domains, which are similar to the smart grid structure defined in NIST (2014). The SLES is a desired solution to deliver more interactive operation and localised energy supply and control, which will be increasingly challenging for the existing system setup. The existing cybersecurity techniques and standards may no longer serve the purpose of SLESs. Therefore, a SLES has different objectives and features to provide reliable communication architecture and power supply. Here are the key components of a SLES:

Grid domain is a critical part of the SLES, managing the bulk energy generation and distribution. In the grid domain, Supervisory Control and Data Acquisition (SCADA) system plays an important role, which is a type of industrial control system that can monitor and control assets over large geographical areas with the help of control equipment. The decentralised automation management and remote control are helpful to ensure the reliability of power supply and lower the maintenance costs of the network. There are four main parts in a typical SCADA system (Akhtar et al. 2018) (a) data interface appliance like remote terminal units (RTUs) and programmable logic controllers (PLCs); (b) communication network; (c) central master terminal unit (MTU); and (d) human–machine interfaces (HMIs). RTUs and PLCs are extremely important in SCADA system. They are connected to many sensors and metres, which are responsible for collecting and translating information for the operators and proceed with commands sent from central MTU. RTUs and PLCs can communicate MTUs with a secured network and receive signals from other parts of the system to facilitate control function. Such setups would enable the SLES to coordinate with the grid operators and operate as a part of the existing power grid. Additionally, a SLES is also able to operate off-grid when it cannot access to the utility grid. Hence, the whole SLES working in the island mode still has similar components tailored to serve the local network (Electronics Projects Focus 2020).

Advanced metering infrastructure (AMI) plays a vital role in the SLES, acting as the connection between control centre and metres. It consists of home-area and wide-area communication network, smart meter and data concentrators, and metre data management system (Bayliss and Hardy 2012). The bi-directional communication between the central system and smart metres becomes easier due to the increasing penetration of IoT based technologies. The increasing installation of smart metre technologies enables the distribution networks to capture consumers' electricity usage

along more precisely with other information. In this way, smart metres can collect and transmit data back to utility operators for better understanding of the energy consumption pattens. Smart metres can action upon request or in response to some events to the utility. On the other hand, smart metres can also benefit consumers through helping them understand and improve their energy consumption (Manbachi 2018).

IoT-based communication network is considered one of the fundamental elements in the SLES. It enables the interaction between service provide domain and customer domain. The development of SLES is substantially contributed by IoT technologies that enable data flowing through the networks. Within the communication network, the utilisation of standard communication protocol enables each device or object to be individually addressed, and the communication between them can be near-real time. Therefore, different devices can be sensed and controlled remotely via a scalable communication network, enabling further integration of physical grid devices and computer-based control system. As the result, the IoT-based network can make system control and operation more efficient and accurate (Mocrii et al. 2018). On the other hand, the increasing adoption of IoT devices also poses a challenge on the system with regards to the physical and cyber security of the infrastructure, which requires more complicated regulatory and technical measures.

Customer domain includes smart appliances, premises networks and distributed energy resources. DERs are becoming increasingly popular in recent years, as they can efficiently provide end users more localised and cost-effective energy supply with technologies such as PV, wind turbine in tandem with energy storage. The consumers can manage the operation of DERs and smart appliances through the premise's networks, either HAN or WAN. However, the introduction of DERs results in two-way electricity flow, which creates some issue for the distribution network operators. The problem can be solved in an active approach by modifying the SCADA system to reconfigure distribution network based on changes in power flow. It requires a substantial amount of data from installed sensors that monitor system conditions such as faults and status of switches, which is significantly facilitated by the IoT-based network. Such an integration with the power grid can enhance the active energy management from the consumer end and add greater reliability and resilience to the system (Norbu et al. 2021; Couraud et al. 2022).

Service provider domain includes markets, operators, and service providers. It uses the communication network to coordinates the functions of energy generators, distribution and transmission network operators and consumers. The market creates a platform for all actors to participate and maintain the energy balance between the supply and demand. The operators ensure the delivery of service through the energy network provided by service providers. In the SLES, there may be more diversified actors in the service provider domain, as the results of localised governance and regulatory. Local authorities can take more responsibilities to govern the operation and the consumers may more actively participate in local energy market, where the local energy network operator will play a more transformative roles as a local system operator (Andoni et al. 2021).

Key features and benefits of SLES

A SLES aims to achieve local balancing from both demand and supply sides. For energy supply, the SLES can maximise the utilisation of energy produced locally from DERs to reduce the consumers' energy import (Menniti et al. 2018). It can also perform demand response to adjust energy demand across many sectors, such as heating and transport, based on the availability of power supply. The smart technologies are the fundamental attributes to realising these functions. For example, smart elements can contribute to more accurate measurements and more digitalised and interactive management through bi-directional information and electricity networks across different levels in the system. The high-resolution data enables consumers and system operators to have a better insight on the system operation and status. The smart elements together with emerging technologies, such as artificial intelligent and machine learning, can help with better decision-making (Ding et al. 2011) and therefore result in a more efficient and effective operation (Koolen et al. 2017; Rajasekaran et al. 2017; Keerthisinghe et al. 2019; Sunny et al. 2020).

The other important feature is the localness as the result of the extraordinary scalability. As mentioned previously, a SLES can scale up and operate as a part of the wider power grid and can also scale down as a local energy network. From a technical aspect, this is particularly important in the event of system failure. It still can ensure the consumers to have secure and continuous power supply with local DERs, resulting in a more resilient network. More importantly, SLESs would also bring other social-economic benefits. Different from the traditional system, the ownership of a SLES can be more flexible and diverse, which may encourage more active participation and engagement of the local authorities, network operators and consumers. Therefore, the SLES is very helpful to deliver more affordable energy and a fairer energy system (Ford et al. 2021). Additionally, local decision-making process will also make the service providers put more focus on consumers and quality of service, which can provide local customers an easy access to the system and address the desire to tackle the climate change locally (Ford et al. 2021). In this way, the locality of the SLES can not only help us exploit the value of system better, but also provide a location-specific solution to the energy transition.

Although the SLESs have some different characteristics compared to the traditional power grid shown in Table 1, the integration of SLES with existing power grid will benefits mutually. On one hand, the implementation of SLES can equip the existing grid with more flexibility and resilience, and therefore contributes to more autonomous operation and optimise the utilisation of connected resources. For example, the DERs within the SLES, such as wind turbines and energy storage, can provide the traditional power grid with more flexible and low-carbon generation and demand side management to mitigate the energy fluctuation in the grid and facilitate the renewable energy transition. Additionally, the SLES can increase the energy self-sufficiency at the local level, which can defer and even avoid the reinforcement and expansion of the network. On the other hand, the connection to the grid can enhance the reliability of power supply to the SLES. Especially when there is insufficient local generation, the connection to power network ensures the consumers can always have reliable and secure energy supply.

Challenges and potential risks

As mentioned previously, the lack of understanding in SLES and its operation, hinder the development of SLES. However, it has some similarities to smart cities. For example, both are part of the key public infrastructure and both heavily reliant upon the participation of private companies and consumers. In traditional system, the utility companies usually have the ownership of the entire infrastructure or utilise a managed service, which may prioritise the cybersecurity during system acquisitions and ensures the correct security measures in place. The emerging technologies, especially built upon IoT, are usually designed for the easy adoption so that the consumers can operate the devices through HAN or WAN. The number of consumer-owned smart devices can therefore easily outnumber those owned and operated by the utility. However, most consumers may not have the technical expertise or incentives to prioritise or maintain the infrastructure security. The divided administration makes the utility or system operators hard to monitor and manage devices, leading to a disparity in security protection. Therefore, administrative boundaries must be broken by interconnecting different networks to ensure the utility companies can operate smart devices and DERs together with consumers in a collaborative manner.

Most IoT-based devices adopted in the SLES are manufactured by third parties or private companies. Lu et al. (2013) acknowledged that the secure operation of the power system is based on a stable ICT supply chain, and any disruption on its components can lead to catastrophic impacts on the whole system. Boysen (2014) also identified that many security concerns and incidents usually can trace back to the inadequate management and risk of manufacturers and suppliers. In most of the real-life deployments, third parties or private companies are given access to key infrastructure assets and critical information without thorough reviews. Although it may contribute to faster service delivery and easier integration, it may lead to catastrophic impacts if without proper management.

In addition, the utilisation of HAN and WAN provide an easy and flexible access to the system management. It enables users and utility companies to obtain more accurate consumer demand and status of DER production in higher resolution and participate in more complex system operation, such as demand side response. However, exposing the system to the external WAN may also increase the attack surfaces, leading to private data breach, device compromise, and even instability of the whole system. The substantial growth in smart appliances and DERs in the SLES will essentially increase the cyber-physical interdependencies.

The operation therefore will no longer merely depend upon the secure physical status of the infrastructure, bringing the importance of cybersecurity to an unprecedented level.

Cybersecurity of smart local energy systems

According to the data provided by Scopus, the cybersecurity has been an increasingly popular topic in the past two decades, especially since 2016 shown in Fig. 1. Additionally, the Fig. 2 shows the most publications mainly focus on several areas, including Computer Sciences (33.5%), Engineering (26%), Mathematics (7.9%) and Energy (6.2%).

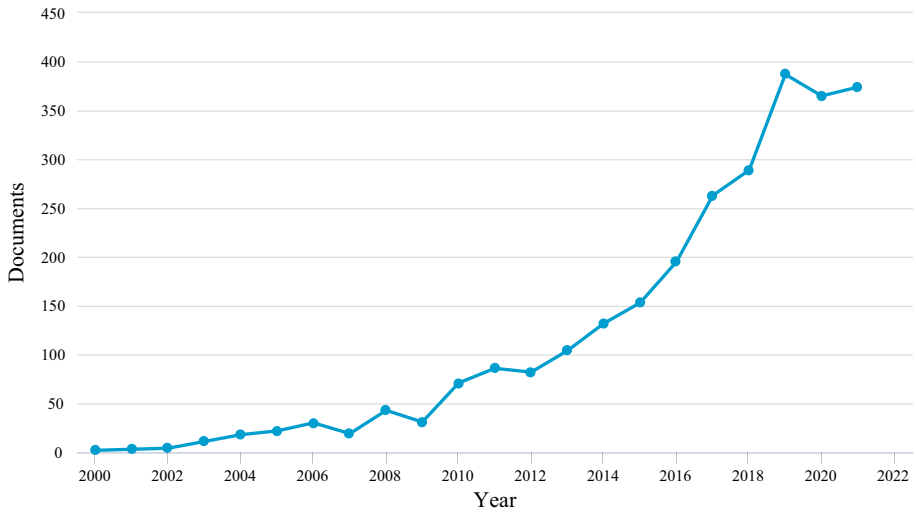

Fig. 1 The number of publication on cybersecurity since 2000

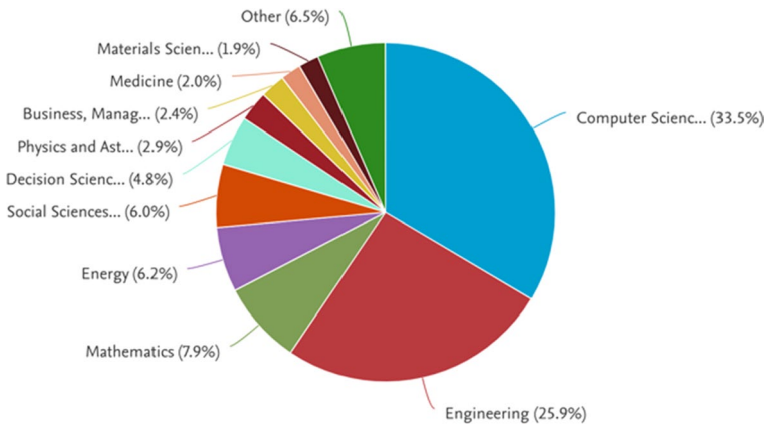

Fig. 2 The proportion of publication on cybersecurity by area since 2000

Amongst all the publications, the majority of publications are conducted by researchers from the US and the EU and the leading affiliations are shown in the Fig. 3.

The added ICT dimension to the classical power grid, introduced new security issues and challenges that were not or rarely present on the traditional power grid. These security issues and challenges could hinder the rapid deployment and adoption by end-users of the IoT-based smart grid and future SLES.

Cybersecurity objectives and requirements

According to National Institute of Standards and Technologies (NIST), there are three cybersecurity objectives to protect information being stolen, compromised, or attacked. The objectives include confidentiality, integrity and availability, also known as the CIA triads (Brooks et al. 2017). In most IT systems, confidentiality has been considered being of the greatest importance. However, in SLES, the priority is to ensure the availability of

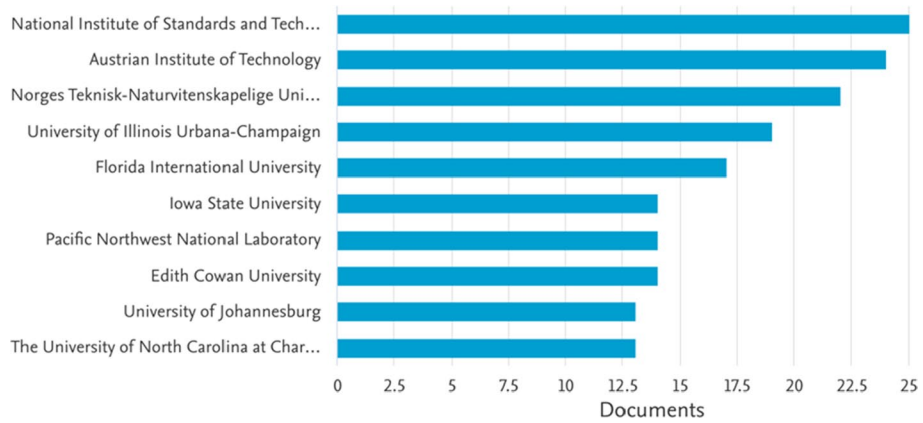

Fig. 3 The number of publication on cybersecurity by affiliation since 2000

Table 1 Comparison between traditional grid and SLES (Ford et al. 2021; Alotaibi et al. 2020)

Parameters	Existing grid	SLES
Generation	Centralised	Decentralised
Communication	None/one way	Two-way, real-time
Customer interaction	Limited	Extensive
Metering	Electro-mechanical meters	Digital meters
Operation	Manual equipment checks and maintenance	Remote monitoring, predictive, time-based maintenance
Maintenance	Network operated by centralised network operators	Local authorities actively manage the SLES operation
Power flow control	Limited	Comprehensive and automated
Reliability	Prone to failures and cascading outages	Automated, prevents outages before they start
Restoration following disturbance	Manual	Self-healing
System topology	Radial. Power flows one-way	Network. Power flows multiple paths
Distributed generation	Limited grid accessibility	Full and efficient grid accessibility

system and secure energy supply and integrity is the next important security objective followed by confidentiality.

Availability is to ensure the information is available when authorised users need to access it. In traditional power gird, utilities use limited information to estimate meter readings and hence the data availability is unlikely to cause serious impact on the grid. However, in the SLES, the safe operation of systems is heavily reliant upon the real-time and near real-time data from the sensors across the SLES, AMI and control signals exchanged between multiple entities. The application of AMI not only provides consumer's data with higher resolution, but also transmits outage alarms and manage critical functions, such as distribution automation. Availability is therefore the primary security objective in the SLES to ensure the timely transmission of data, even when the network is under attack and flooded traffic (Cleveland 2008). The availability of data in the SLES needs a secure collection of network layers, including application layer, transport layer, network layer and physical layer (Pishva 2017). Any threats and attacks on single or multiple layers in the network may keep the system from secure and safe

operation. The most common threat is denial of service attack (Liu et al. 2013; Berthier et al. 2010; Grochocki et al. 2012; Hong et al. 2014) where some malicious activities are designed to disrupt the accessibility of services to legitimate users and hence disrupt normal system operation (Huseinović et al. 2020; Islam et al. 2019).

Integrity aims to protect data and keep it in a correct state from any accidental or malicious modification of data. The data must not be changed in an unauthorised or undetectable manner (Mohammadpourfard et al. 2020). It involves maintaining the consistency, accuracy, and trustworthiness of data during storage, transmission, and usage. In the context of SLES, the data integrity is usually targeted by attackers who attempt to alternate critical data such as metre reading, billing information and control demand. Therefore, authentication, certification and attestation are commonly adopted as protection measures (Li et al. 2018). The components in the SLES needs to authenticate each other so that impersonation can be detected and avoided (Zhang et al. 2019). Then the data certificate keeps the message exchanges from any alternation and changes during the data transmission. With the increasing IoT devices, the system has become more vulnerable to complex data integrity attacks, such as false data injection (Lin et al. 2016; Yang et al. 2014; Xie et al. 2011), bypassing data detection (Zhang et al. 2018) etc.

Confidentiality refers to protecting personal privacy and proprietary information from unauthorised access. It emphasises the need for information protection, requiring relevant measures to ensure only authorised people being allowed to obtain the information. Attacks targeting confidentiality do not necessarily cause substantial impacts on the system operation but can be a preparatory step to a more damaging attack. The smart metre has raised some concerns regarding the consumers' privacy in recent years. Customers fear that the data leakage may potentially be used by unauthorised people or marketing firms. In the future, a SLES will involve with significantly frequent interaction between consumers, network operators and local authorities comparing to the traditional energy system. Counter measures against confidentiality issues such as eavesdropping and privacy breach, will becoming increasingly important (Bao and Lu 2015; Karampour et al. 2019; Chaudhry et al. 2021).

The development of cybersecurity standards

As previously discussed, due to the growth in distributed and integrated technologies into CPS with unprecedented reach and interdependencies, we provide an analysis of current best practices in cybersecurity within the energy sector concerned with SLES. Cybersecurity in the energy sector is not as mature as other markets, therefore, it's important to have a detailed understanding of current best practice in infrastructure security standards and protocols applied to the smart grid. Our research aims to assess the existing standards through several aspects, such as coverage, purpose, and the significance to the real-world implementations. By evaluating best practice in the smart grid infrastructure, it is therefore helpful to understand its relevance to SLES and to identify the gap between the existing standards and the future requirements. There are around 100 existing standards addressing the cyber security issues, but this section we only review some of them that reflecting the main trend of the development in the

chronological order. The full list of standards included in the research can be found in the appendix.

The development of cybersecurity standards mirrors the trend of technological advancement, shown in Table 2. Initially, there were not any intelligent or smart control systems or devices in the system. Therefore, in the 1990s the cybersecurity protection was mainly addressed by enhancing the security of the physical assets. For instance, *IEEE 1264 Guide for Animal Deterrents for Electric Power Supply Substations* was proposed (Standard IEEE 1993). It defines types of intrusions and identified subsequent problems and impacts, evaluated by several parameters, such as intrusion location and seriousness of impacts. Correspondingly, relevant precaution and prevention measures are provided, such as physical obstacles and enclosure, security patrol and video surveillance. Later in 2000, *IEEE 1402 Guide for Electric Power Substation Physical and Electronic Security* was introduced and complemented the security protection from human intrusion. Besides existing measures against animal intrusion, IEEE 1402 also includes protection measures for electronics, such as virus scans, encrypting and dial-back verification. However, these protective measures are only briefly mentioned without details in depth.

With the development of cybersecurity protection, most standards focused on the design and management at a macro systematic level or a domain-specific level. *DHS Cyber Security Procurement Language for Control System* (Department of Homeland Security 2009) is an important documentation that combines many requirements into 11 high-level topics, such as system design, account and access control, end device management, physical and cyber threat and vulnerability detection. Each topic addresses a specific issue or concern in a control system, and describes a rationale,

Table 2 Categories of cybersecurity development

Development stage	Examples
Securing physical assets	- IEEE 1264 Guide for Animal Deterrents for Electric Power Supply Substations
	- IEEE 1402 Guide for Electric Power Substation Physical and Electronic Security
Macro-level management strategy	- DHS Cyber Security Procurement Language for Control System
	- NISTIR 7268 Guideline or Smart Grid Cyber Security
	- PAS 555 Cyber security risk—Governance and management—Specification
	- IEEE Std 11073–40101 Cybersecurity—Processes for vulnerability assessment
Cybersecurity of communication	- IEEE C37.240 Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems
	- IEC 62443 Industrial communication networks—IT security for networks and systems
Component specific	- IEEE 1686 Standard for Intelligent Electronic Devices Cyber Security Capabilities
	- Advanced Metering Infrastructure System Security Requirement
	- CEN/CLC/JTC 13 N 468 Protection Profile for Smart Meter
	- Security of the Advanced Metering Infrastructure
Data and information	- IEEE 1363 Standard Specifications for Public-Key Cryptography
	- IEEE P1912 Standard for Privacy and Security Framework for Consumer Wireless Devices
	- ISO/IEC TR 27019 Information technology—Security techniques—Information security management guidelines

from specification language to factory and site acceptance test measures. In addition, *NISTIR 7268 Guideline or Smart Grid Cyber Security* (Institute and of Standards and Technology 2012) specified a comprehensive framework for smart grid. The guideline includes five steps: use case selection, risk assessment, boundaries setting, proposing security requirements, and testing and certification. The NISTIR 7268 emphasised four high-priority challenges: more cost-effective and secure devices, more advanced cryptography and key management, more robust system and easier networking. North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) (Corporation et al. 2021) standards are compulsory for the whole electric system. The NERC CIP standard series highlights the importance of cybersecurity of the assets that should undertake regular security risk and vulnerability assessment and equip with mandatory minimum security management controls and recovery plans. It is also worth mentioning that NERC CIP emphasises significance of training authorised personnel with a sufficient cybersecurity awareness. In the UK, The British Standards Institution (BSI) issued *PAS 555 Cyber security risk—Governance and management—Specification* in 2013 (BSI 2013). It provides a framework that is not specific to the energy industry, but all types of organisations and business. It defines the outcomes of good cybersecurity practice. It considers not only the technical aspects of cyber security, but also the physical, cultural, and behavioural aspects, alongside effective leadership and governance.

The protection of communication network as part of industrial control and automation system was also addressed due to the proliferation of the Internet. In 2014, *IEEE C37.240 Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems* (IEEE 2014) was developed and published to present a set of baseline cybersecurity requirements dedicated to the communication system. It aimed to protect the security of interface between control systems and standardise the foundational requirements for communication components, such as access and use control, data integrity and confidentiality, network resource availability and timely response to events. Most importantly, it reemphasised the importance of monitoring and auditing security events and policies and conducting periodic security tests. Another instance is *IEC 62443 Industrial communication networks—IT security for networks and systems*, launched in 2010 (International Electrotechnical Commission 2018). It provides a detailed description regarding the elements and the development process of a cybersecurity management system for a control system and automaton technology. It also lists seven requirements, overlapped with the foundational requirements in IEEE C37.240, to achieve higher security levels. The security levels are considered as the functional requirements for the system, protecting from accidental information disclosure and unauthorised access and different level varies with the attacking method and activeness used by the attackers.

The increasing complex electronic devices implemented then shifted the focus towards the specific component or technology in the system. *IEEE 1686 Standard for Intelligent Electronic Devices Cyber Security Capabilities* was published in 2013 (IEEE 2013). The standard series detail a set of compulsory requirements for the electronic devices, such as an interface to change user accounts, keeping full sequential audit history, and monitoring security-related events. The standard also requires that all electric devices

should have certain level of cryptographic features to ensure the device functionality and secure communication. Another example is *Advanced Metering Infrastructure System Security Requirement* (AMI-SECTF 2008) issued in 2008 in the US. It aims to provide a set of security requirements to ensure the high level of information assurance, availability, and security necessary to maintain a reliable system and consumer confidence. The requirement in the document can be generalised into three categories: (a) primary security services (aims to protect confidentiality and privacy, integrity, availability, identification, authentication, and authorisation); (b) supporting security services (such as detection, risk assessment, cryptography, and certificate); and (c) assurance services (such as accountability, and access control). Similar standards can also be found, such as *CEN/CLC/JTC 13 N 468 Protection Profile for Smart Meter* in the UK and Privacy and *Security of the Advanced Metering Infrastructure* in Netherlands.

The surge of electronic devices has markedly facilitated the digitalisation of energy system that needs to handle with substantial amount of information and data exchange. Therefore, joint efforts by academia and industry have been trying to propose relevant standards or protocols to ensure the data and information security. *IEEE 1363 Standard Specifications for Public-Key Cryptography* was firstly introduced in 2004 (Committee of the IEEE Computer Society 2009), aiming to produce a comprehensive document defining a range of common public-key techniques covering key agreement, public-key encryption and digital signatures. It includes different types of cryptographic techniques including traditional, identity-based, password-based, and lattice-based techniques and extensive discussions of security and implementation considerations. *IEEE P1912 Standard for Privacy and Security Framework for Consumer Wireless Devices* (IEEE 2020b) also focuses on data privacy and security, which defines a privacy scale where data can refer to personal identifiable information. The input of privacy data contributes to assessment tools to apply relevant necessary setting to the data, which is of great importance for the future applications at the end-user side. Meanwhile, more risk management guidelines are introduced to enhance the information security. For example, *ISO/IEC TR 27019 Information technology—Security techniques—Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry* (British Standard Institute 2013). It suggests that security requirements analysis and a complementary individual risk analysis should be undertaken before the use of control devices or software. IEEE 2144.1 *Standard for Cryptographic Protection of Data on Blockchain-Oriented Storage Devices* (IEEE 2020a) also presents a trusted IoT data management framework integrate with application, function and trusted carrier layers. The framework is applicable for data management in blockchain and IoT technologies and to business scenarios that employing internal data collection, change and sharing with external parties. *IEEE Std 11073-40101 Cybersecurity—Processes for vulnerability assessment* (Committee of the IEEE Engineering in Medicine 2021) proposing an auditable approach to identification and assessment of cybersecurity vulnerabilities and estimation of risks, which is an useful tool and can be used as reference method for future smart devices development.

Discussion and suggestion

Findings from the review of existing standards

The previous section has reviewed the development of cybersecurity standards and protocols that were defined and specified by industry and standard bodies. Many of them were developed to address security and privacy concerns and requirements in either control and wireless system and devices, or management strategy of cybersecurity issues. The requirements included in the standards differ from each other, in terms of technical details, the scope and the thematic coverage. Some publications extend or partially repeat requirements from other standards, and some are only supplementary documents to others.

Our findings suggest that there is a considerable number of existing standards or protocols that would apply to the application and infrastructure of SLES, such as industry automated and control system, electric vehicles, and intelligent electronic devices. Many standard bodies from different countries have contributed to the knowledge, such as BSI from the UK, IEEE and ANSI from the US. These standards are applicable to some specific component or industry of the infrastructure. For example, most of the standards proposed by IEEE defines and specifies very detailed technical security elements for the IoT. The works are applicable to many aspects and components in the SLES, including IoT architectural framework, physical and medium access control, and wireless devices with end-to-end security.

Another finding is that the standards are not comprehensive and some only address cybersecurity to some certain extent. The existing standards are highly fragmented that are specific to certain industry, such as NERC CIP for electric utility and IEC 62443 for general industry automation and control systems, while some security frameworks providing general guidelines applicable to any industry or organisation without technical details, such as PAS 555. Majority of the standards only focus on securing one or a few components or security features in the system by the design or for the operation. Many researchers suggest that the ambiguous definition of the smart city still hinders the application. Therefore, it will be even more difficult to provide a set of comprehensive guidelines on cybersecurity for SLES, because of the differences between SLES and smart cities, such as more localised governance bodies and more active prosumers' participation in energy supply. SLES will be heavily reliant upon substantial integration of IoT technologies and automated control and communication networks, which will make cybersecurity one of the primary goals. However, it would depend on clear definitions of SLES and explicit guidelines on its operation and governance. Therefore, relevant necessary and essential measures can be adopted to construct a robust and sophisticated smart local energy network in a more systematic fashion.

In addition, our finding also suggest that the information security is becoming increasingly important due to the growing penetration of IoT and digitalisation of the energy industry. Different standards were put in place to standardise the data encryption, transmission, storage, and format to enhance the interoperability between different system components. Additionally, relevant standards were also designed to protect personal data and privacy via both algorithm and edge device design. The complex requirements are imposed to ensure certain levels of security measures embedded in the electronic devices by the manufacturers to protect the cybersecurity of both the

system and users. However, HP conducted an assessment on 10 common IoT devices and they found each device had 25 vulnerabilities on average (HP 2015). For the future SLES applications, at near-consumer side, many IoT devices will be adopted to manage local generation and demand of consumers. For the local, distribution and transmission network, the timely and accurate communication will be critical to the system stability. The disparity in security features of the IoT devices can potentially cause problematic and even catastrophic issues. For this reason, we would recommend an adherence to certain standards must become as the norm of smart device development and sufficient and comprehensive standards are needed to be considered as the baseline standards that provides principles to ensure the scalability and flexible interpretability, which is also in line with the suggestions provided in Pishva (2017).

For this reason, the findings can help us understand how the existing standards can integrate with the SLES. For example, the substantial amount of data will be collected and exchanged during the daily operation, which makes the data safety and privacy protection extremely important. The potential peer-to-peer energy trading within the SLES can make the best use of the blockchain technologies and existing relevant standards such as *IEEE 2144.1* that ensure the data security in the devices and entities. In addition, standards like *PAS 555* can help us comprehend the critical role of cybersecurity and build an effective framework to assess and manage potential cyber threat, vulnerability, and attacks. As the result, a more active cyber threat prevention and detection mechanism will be added to the existing protection measure, further enhancing the cybersecurity of the SLES.

Cybersecurity suggestions for SLES planning and deployment

In the light of the emerging SLES, electric utility has been exposed to ever substantial challenges, especially cyber challenges, which may cause catastrophic impacts on the whole value chain of the power network. The legacy generation systems and clean-energy infrastructure without sufficient security design will likely suffer serious disruption of service and ransomware attacks against generation assets. The physical security weaknesses allow access to the grid control system and hence result in large-scale disruption of power to customers through remotely disconnecting services. At distribution level, limited security measures built into SCADA systems can cause disruption of reginal loss and disruption of service to customers. At network and end-user side, large attack surface of IoT devices such as smart meters and electric vehicles, will also possibly lead to theft of customer information, fraud, and service disruption.

The SLES aims to achieve an automated and local energy supply with high participation of prosumers with the help of highly penetrated IoT technologies. The difference in the operation and management of SLES and traditional power grid will contribute to the merging of information and operation technologies. For this reason, the challenges are brand-new and unprecedent, and can hardly be solved by using traditional cyber threat management strategies. Therefore, the researchers from academia and industry need to work on several things and we have made following recommendations.

Due to interdependency between the physical and cyber infrastructures, the cybersecurity of SLES should focus on protecting measures on both physical and cyber aspects. It is hard to detail every cybersecurity requirement here, but a good

comprehensive cybersecurity guideline should include following 15 aspects: access control, audit and accountability, configuration management, identification and authentication, incident response, media protection, planning, personnel security, information system and service acquisition and integrity, awareness and training, security assessment and authorisation, information and document management, physical and environmental security, risk assessment and management, and communication system protection.

In addition, for the industry, more efforts are needed to provide more affordable and cyber-secured devices and services and more innovative technologies should also be encouraged to apply in real applications. Technologies, such as blockchain and OpenFMB, can not only facilitate scaling up the SLES applications with secured assurance, but also can improve the integration with legacy infrastructures with enhanced data interoperability. More emerging techniques and concepts should also be utilised to influence the development of cybersecurity, such as AI and machine learning (Cui et al. 2020; Esmalifalak et al. 2017). The increasingly complex cyber environment will only result in ever challenging security issues. Instead of obeying a specific design, cybersecurity measures should also become more organics and autonomous. Continuous training and adaptation will equip the system with a capability to automatic detect and respond to new threats, such as predictive defence (Cerotti et al. 2019; Ahmed et al. 2018) and hybrid cloud (Talaat et al. 2020).

A good balance between the affordability and quality of cybersecurity should be achieved so that IoT products can be more easily accessed by consumers. In comparison, the government and regulator should set out clearly what standards are mandatory and regulate the data management. Clear definitions and guidelines on SLES should be considered as priority. A tailored cybersecurity management strategy needs to be made upon good comprehension of a system setup, operation, and governance. A few baseline standards are needed to address the system's baseline security requirements, so that relevant components or technologies can therefore be adopted to meet the minimum function and security requirements.

At last, compliance testing and certifications should also play an important role in SLES and the wider energy system. Although there may be technical standards to ensure the security at the application or development stage, the consistency should come across the whole SLES ecosystem, including transport and energy. For this reason, it is necessary to conduct testing and certification by an independent party, which can assure the regulators that a satisfied security level is provided in key SLES ecosystem actors by design. It would be beneficial to move closer to energy system integration supporting the optimisation of the whole system.

Conclusion

In this paper, an extensive investigation into existing technical standards addressing cybersecurity issues is carried out. Our findings suggest that a considerable number of standards or protocols pre-existing that would meet the requirement of the application and infrastructure of SLES. However, the standards are not comprehensive and some only address cybersecurity to some certain extent. The existing standards are highly fragmented that are specific to certain industry, while some security frameworks

providing general guidelines applicable to any industry or organisation without technical details. Majority of the standards only focus on securing one or a few components or security features in the system by the design or for the operation. Additionally, we also find that the information security is becoming increasingly important, and many standards are introduced to protect information security and personal privacy.

However, the successful development of SLES still needs more effort from multiple sides. A detailed cybersecurity guideline should include 15 main topics described in previous section. More efforts are needed from the industry to provide more affordable and cyber-secured devices and services to apply in real applications. The government and regulator should demonstrate a few baseline standards to address the system's baseline security requirements, so that relevant components or technologies can therefore be adopted to meet the minimum function and security requirements. Additionally, compliance testing and certifications should also be in place and carried out by an independent third party to ensure the components of SLES ecosystem with a satisfied security level by design.

Based on our findings and suggestions produced from this research, it is important to extend the research and further investigate how they can contribute to the design and operation of SLES. The future work will focus on proposing a framework for the detection and treatment to ensure the cybersecurity of SLES. Additionally, With the huge advancement of AI and machine learning in many verticals, there is increasing interest in applying AI techniques in in the energy sector. The SLES will benefit from ever more integrated smart technologies, but it also must encounter the inherent vulnerabilities and challenges. Attacks using advanced AI techniques can be more difficult to detect and mitigate, compared to threats seen in traditional energy networks. Therefore, future work can also investigate the potential AI-driven cyberattacks in SLES, particularly what system vulnerabilities they can exploit and impact, and how they can be managed and prevented in the context of system security, data governance, and privacy.

Appendix: Cybersecurity standards reviewed in the study

Standard	Year	Description	Coverage	Purpose	Highlights
IEEE Std 1264	1993	IEEE Guide for Animal Deterrents for Electric Power Supply Substations	Substation, Nonhuman intrusion	Counteract animals' intrusions	1) Define type of animal intrusions and possible problems; 2) Precaution and prevention measures, such as barriers and enclosures

Standard	Year	Description	Coverage	Purpose	Highlights
IEEE Std 1402	2000	IEEE Guide for Electric Power Substation Physical and Electronic Security	Substation, human intrusion	Counteract human intrusions	1) Define type of intrusions, including pedestrian, vehicular, projectile, electronic; 2) Define parameters and events influencing intrusions and subsequent problems; 3) Security criteria and management are proposed
IEEE 802.1AE	2006	Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security	Metropolitan Area Networks	Specifying provision of connectionless user data confidentiality, frame data integrity, and data origin authenticity	Specifies 1) requirements that devices need to comply with; 2) requirements for and definitions of MAC security; 3) management strategy of MAC security
ANSI C12.18	2006	Protocol Specification for ANSI Type 2 Optical Port	Communication between end-device and clients via optical port	To detail the criteria for the communication and details for implementing OSI 7-layer model	Specify the use of ANSI type 2 optical port for meter communications
ANSI C12.21	2006	American National Standard for Protocol Specification for Telephone Modem Communication	Utility communication over telephone modem	To specify requirements for communication amongst users and devices over switched telephone modem	Specify the use of telephone modem for meter communications
IEEE std 1619	2007	Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices	Data encryption in sector-based devices	Providing a cryptographic protection for data stored in constant length blocks	1) Defines specific of an architecture for cryptographically protecting data stored in constant length blocks; 2) provides an additional and improved tool for implementation of secure and interoperable protection of data residing in storage

Standard	Year	Description	Coverage	Purpose	Highlights
IEEE std 2600	2008	Standard for Information Technology: Hardcopy Device and System Security	Security requirements for hard-copy devices	Providing a guidance on security requirements for hard copy devices during manufacture, installation, and applications	1) To provide guidance in the secure architecture, design, and out-of-box configuration of HCDs for manufacturers; 2) To provide guidance in the secure installation, configuration, and use of HCDs for end users and their supporting organizations
ANSI C12.19	2008		Utility data table structure	Defining structures for transporting data to and from end devices	Defines a table structure for utility application data to be passed between an end device and a computer. Does not define device design criteria nor specify the language or protocol used to transport that data
ANSI C12.22	2008	American National Standard for Protocol Specification for Interfacing to Data Communication Networks	Utility data interoperability and security	Specify the transportation of data over various networks to advance interoperability and security amongst communication modules and meters	1) Describes the process of transporting C12.19 table data over a variety of networks; 2) Uses AES encryption to enable strong, secure Smart Grid communications, including confidentiality and data integrity, and is also fully extensible to support additional security mechanisms the industry may require in the future
IEEE 802.21a	2012	Standard for Local and Metropolitan Area Networks: Media Independent Handover Services—Amendment for Security Extensions to Media Independent Handover Services and Protocol	Metropolitan Area Networks	Protecting media independent handover services and mechanisms; Assisting proactive authentication to reduce the latency due to media access authentication and key establishment with the target network	1) to protect MIH messages, (D)TLS based protection when a PKI involved and EAP based authentication are introduced. 2) to reduce the latency, three key distribution mechanisms are introduced

Standard	Year	Description	Coverage	Purpose	Highlights
ANSI C12.22 (IEEE Std 1703)	2012		Interoperability among communications modules and meters	Accommodating the network messaging requirements of an advanced metering infrastructure	1) it uses advanced encryption standard to enable strong secure communications to protect confidentiality and data integrity. 2) the security model is extensible to support new security mechanism, but the cipher model cannot secret non-standard short messages
IEEE 1686	2013	IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities	IED	Addresses security regarding the access, operation, configuration, firmware revision and data retrieval from an IED, and communication encryption	1) IEDs should have open and documented interface to change user accounts, passwords, and roles. 2) IEDs should keep full sequential record of audit history (at least 2048 events). 3) IEDs should monitor security-related activities and inform SCADA through a real-time protocol. 4) IEDs should have certain cryptographic features to ensure the communication and functionality with the help of various techniques. 5) Firmware quality assurance shall follow IEEE std C37.231
IEEE Std 1363.3	2013	Standard for Identity-Based Cryptographic Techniques using Pairings	Identity-based cryptographic schemes based on the bilinear mappings over elliptic curve	Specify identity-based cryptographic techniques based on pairings	Techniques for identity-based encryption, signatures, inscription, key agreement, and proxy re-encryption, all based on bilinear pairings

Standard	Year	Description	Coverage	Purpose	Highlights
PAS 555	2013	Cyber security risk. Governance and management. Specification	A business-led, holistic approach to cyber security	Define the overall outcomes of effective cyber security	PAS 555 enables any organization to choose how it achieves the specified outcomes, whether through its own defined processes or the adoption of other standards and management systems. PAS 555 enables organizations to 1) Focus investment in the most appropriate way; 2) Minimize potential loss; 3) Improve operational effectiveness and efficiency; 4) Develop organizational resilience; 5) Improve loss prevention and incident management; 6) Identify and mitigate cyber security risk throughout the organization
TIA TSB-4940	2013	Smart Device Communications; Security Aspects	ICT operation security	Addressing only the management of cyber security related risk derived from or associated with the operation and use of information technology	Provide a framework that can protect communication security, including assessing external threat, vulnerability assets, and relevant approach to protect vulnerable assets
ISO/IEC 27001 –27005	2013	Information technology—Security techniques—Information security risk management	Information security risk management	Assisting the satisfactory implementation of information security in all types of organisations based on a risk management approach	It specifies how to 1) identify and assess the risks; 2) deal with the risks; 3) monitor the risks and risk treatments; 4) Keep stakeholders informed throughout the process

Standard	Year	Description	Coverage	Purpose	Highlights
IEEE C37.240	2014	IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems	Substation, interfaces	Minimum requirements for a substation program. Any utility's CS programme must balance technical, economic, and operational feasibility	1) Foundational requirements: access control, use control, data integrity, data confidentiality, restrict data flow, timely response to event, network work recourse availability. 2) Physical Security needs to ensure the secure access to the cyber assets. 3) Protection of data at the rest including file-type of IEDs (configuration files, data files, etc.) and hard copy information (IED instruction manuals, station drawings)
IEEE 2410	2015	Standard for Biometric Open Protocol	Biometric Open Protocol Standard	The Biometric Open Protocol Standard (BOPS) provides identity assertion, role gathering, multilevel access control, assurance, and auditing	1) BOPS introduces the security considerations, including identity assertion, role gathering, access control, audit and assurance; 2) how BOPS is realised in applications and relevant requirements
IEC 27019	2017	Information technology—security techniques—Information security controls for the energy utility industry	Energy management cybersecurity	Guidance on process control systems for utility industry for controlling and monitoring the production and generation, T&D	Specifies the cybersecurity requirements for several components, including central and distributed process control, monitoring, communication technology, advanced metering infrastructure, energy management system, software, firmware and remote maintenance system

Standard	Year	Description	Coverage	Purpose	Highlights
IEEE P2413	2020	Standard for an architectural framework for the Internet of Things	IoT architectural framework	Promoting cross-domain interaction and system interoperability and functional compatibility and accelerating the growth of IoT market	1) recognizes the evolving transformational integration and convergence across technology and application domains; 2) to provide an extensible integrated architectural framework that will continue to evolve and unify the standards creation effort; 3) also provide enough flexibility for different industries to adapt the acritude based on different needs
IEEE Std 11073–40101	2020	Cybersecurity—Processes for vulnerability assessment	Personal Health Devices and Point-of-Care Devices	Proposing an auditable approach to identification and assessment of CS vulnerabilities and estimation of risks	1) Emphasise the role of device manufacturers that should provide a device with sufficient security protection measures and without any hidden and undocumented functions; 2) Provide two good threat modelling approaches data flow diagram and STRIDE classification scheme (***S****poofing,* ***T****ampering,* ***R****epudiation,* ***I****nformation* ***D****isclosure,* ***D****enial of Service and* ***E****levation of Privilege*) 3) A scoring system is proposed to quantify vulnerabilities, which provides a rank and priority to each vulnerability

Standard	Year	Description	Coverage	Purpose	Highlights
IEEE 2144.1	2020	Standard for Cryptographic Protection of Data on Blockchain-Oriented Storage Devices	IoT, Blockchain, data	Proposing a framework of blockchain-based IoT data management	1) Define the roles of stakeholders in a IoT system, including data owner, data consumer, service provider, regulator/policy maker, etc. 2) specify blockchain-based data management lifecycle; 3) proposing trusted IoT data management framework integrate with 3 layers: application, function and trusted carrier layers, which all communicated and controlled by management and control panel
IEC 61969	2020	Mechanical structures for electrical and electronic equipment—outdoor enclosures	Design standard for outdoor enclosure	Establish basic environmental performance criteria for outdoor enclosure compliance	Defining design guidelines for outdoor enclosures and is applicable over mechanical, electromechanical and electronic equipment and its installation
IEC 61970	2020	Energy management system application program interface	Common Information Model for transmission network domain	Standardising the data format and enhance interoperability at transmission network level	301 Contains a standard data model defining the semantics of the information exchanged in a broad range of energy management system applications and later version 302 intended to ensure the data interoperability among transient stability software products. Later versions such as 45x, 452 and 453 tend to standardise the data profiles for state estimation and diagram layout profiles for data exchange

Standard	Year	Description	Coverage	Purpose	Highlights
ISO/SAE 21434	2020	Road vehicles-Cybersecurity engineering	Road Vehicle	Proposing a technical standard for automotive development that can demonstrate compliance with regulations in EU	The standard provides guidelines on how to manage cybersecurity strategies in different stages, including: overall management, during concept phase, during product development, and during production, operation and maintenance
IEEE P1912 (ongoing)	2021	Standard for Privacy and Security Framework for Consumer Wireless Devices	Privacy and security, consumer wireless device	Data privacy and security at end-user side	1) Define a privacy scale applied to data collected, processed or shared amongst services or network. 2) the input of privacy data contributes to assessment tools to apply relevant necessary setting to the data
DHS cybersecurity	2021	Cybersecurity Requirements for Critical Pipeline Owners and Operators	Pipeline owners and operators	Details basic requirements for pipeline owners and operators	1) Owners and operators must report confirmed and potential cybersecurity incidents. 2) Owners and operators must designate a Cybersecurity Coordinator to be available 24 h a day, seven days a week.; 3) Owners and operators must review current practices to identify and remediate gaps related to cyber risk and report all findings to both TSA and CISA within 30 days
IEEE Std 1363 series	2004–2008	IEEE Standard Specifications for Public-Key Cryptography	public-key cryptography techniques	Electronic privacy and authenticity	Introducing types of cryptographic techniques and speciation's of key agreement schemes, signature schemes, encryption schemes

Standard	Year	Description	Coverage	Purpose	Highlights
ISO 16484	2004–2020	Building Automation Controls network	Communication across devices	Enhancing interoperability amongst different vendors and equipment	1) Specify guiding principles for project design and implementation and integration of other systems into automation and control system; 2) specifies the requirements for the hardware to perform the tasks; 3) specifies the reequipments for overall functionality and engineering service; 4) defines data communication services and protocols for computer equipment used for building systems
IEC 62443	2009–2020	Industrial communication networks—IT security for networks and systems	Industrial and automation systems cybersecurity	Addressing and mitigating current and future security vulnerabilities in industrial automation and control systems	1) Specifies process requirements for the secure development of products used in an IACS and defines a secure development life cycle for developing and maintaining secure products; 2) Details the cybersecurity technical requirements for components making up an industrial automation and control system, including embedded devices, network, host and software applications; 3) specifies security capabilities enabling a component to mitigate threats for a given security level without compensating countermeasures;

Standard	Year	Description	Coverage	Purpose	Highlights
NIST SP 800–82	2011– 2021	Guide to Industrial Control Systems (ICS) Security	Industrial control system security	Securing industrial control system, while addressing their unique performance, reliability, and safety requirements	The document provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks
IEC 61850	2013–2021	Communication networks and systems for power utility automation	Communication network, Substation	Specifying communication network at substation	1) Using a data and object model to specify data format in system and devices; 2) establishing multi-vendor interoperability

Abbreviations

SLES	Smart local energy system
RTU	Remote terminal units
DER	Distributed energy resource
PLC	Programmable logic controllers
ICT	Information and communication technology
MTU	Master terminal units
IoT	Internet of Things
HMI	Human–machine interfaces
CPS	Cyber physical system
AMI	Advanced metering infrastructure
SCADA	Supervisory control and data acquisition
HAN	Home area network
DoS	Denial of service
WAN	Wide area network

Acknowledgements
We would like to thank Elena Gaura, Nandor Verba, and Rameez Asif for helpful insights and expertise that greatly assisted the research.

Author contributions
SD: Data curation, Writing—original draft, Methodology, Investigation. JC: Writing—review and editing. DF: Writing—review and editing. ZF: Writing—review and editing, Supervision, Resources. All authors read and approved the final manuscript.

Funding
This work was partially supported by the EPSRC EnergyREV project (EP/S031863/1). This work was also supported by the Smart Energy Network Demonstrator project (SEND, grant ref. 32R16P00706) funded by ERDF and BEIS.

Availability of data and materials
All data generated or analysed during this study are included in this published article.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

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

Received: 21 February 2022 Accepted: 3 June 2022
Published online: 21 June 2022

References

Ahmed S, Lee Y, Hyun SH, Koo I (2018) Feature selection-based detection of covert cyber deception assaults in smart grid communications networks using machine learning. IEEE Access 6:27518–27529. https://doi.org/10.1109/ACCESS.2018.2835527

Akhtar T, Gupta BB, Yamaguchi S (2018) Malware propagation effects on SCADA system and smart power grid. 2018 IEEE Int Conf Consum Electron ICCE 2018 2018;2018-Janua:1–6. https://doi.org/10.1109/ICCE.2018.8326281

Alanne K, Saari A (2006) Distributed energy generation and sustainable development. Renew Sustain Energy Rev. https://doi.org/10.1016/j.rser.2004.11.004

Alotaibi I, Abido MA, Khalid M, Savkin AV (2020) A comprehensive review of recent advances in smart grids: a sustainable future with renewable energy resources. Energies 13:6269. https://doi.org/10.3390/en13236269

AMI-SECTF (2008) AMI system security requirements. OpenSG;1:111

Andoni M, Robu V, Couraud B, Früh WG, Norbu S, Flynn D (2021) Analysis of strategic renewable energy, grid and storage capacity investments via Stackelberg-cournot modelling. IEEE Access 9:37752–37771. https://doi.org/10.1109/ACCESS.2021.3062981

Antonopoulos I, Robu V, Couraud B, Flynn D (2021) Data-driven modelling of energy demand response behaviour based on a large-scale residential trial. Energy AI 4:100071. https://doi.org/10.1016/J.EGYAI.2021.100071

Bao H, Lu R (2015) A new differentially private data aggregation with fault tolerance for smart grid communications. IEEE Internet Things J 2:248–258. https://doi.org/10.1109/JIOT.2015.2412552

Bayliss CR, Hardy BJ (2012) Smart grids. Transmission and distribution electrical engineering. Elsevier, Amsterdam, pp 1059–1074. https://doi.org/10.1016/B978-0-08-096912-1.00027-7

Berthier R, Sanders WH, Khurana H (2010) Intrusion detection for advanced metering infrastructures: requirements and architectural directions. In: 2010 First IEEE international conference on smart grid communications, pp 350–355. https://doi.org/10.1109/SMARTGRID.2010.5622068

Boyson S (2014) Cyber supply chain risk management: revolutionizing the strategic control of critical IT systems. Technovation 34:342–353. https://doi.org/10.1016/j.technovation.2014.02.001

British Standards Institute. Information Technology—Security Techniques—Information Security Management Guidelines Based on ISO/IEC 27002 for Process Control Systems Specific to the Energy Utility Industry

Brooks S, Garcia M, Lefkovitz N, Lightman S, Nadeau E (20117) An introduction to privacy engineering and risk management in federal systems. Gaithersburg, MD. https://doi.org/10.6028/NIST.IR.8062

BSI (2013) PAS 555:2013 Cyber security risk—governance and management

Burger S, Chaves-Ávila JP, Batlle C, Pérez-Arriaga IJ (2017) A review of the value of aggregators in electricity systems. Renew Sustain Energy Rev 77:395–405. https://doi.org/10.1016/j.rser.2017.04.014

Cerotti D, Codetta-Raiteri D, Egidi L, Franceschinis G, Portinale L, Dondossola G, et al (2019) Analysis and detection of cyber attack processes targeting smart grids. Proc 2019 IEEE PES Innov Smart Grid Technol Eur ISGT-Europe 201. https://doi.org/10.1109/ISGTEUROPE.2019.8905716

Chaudhry SA, Nebhen J, Yahya K, Al-Turjman F (2021) A privacy enhanced authentication scheme for securing smart grid infrastructure. IEEE Trans Ind Inf. https://doi.org/10.1109/TII.2021.3119685

Cleveland FM (2008) Cyber security issues for advanced metering infrastructure (AMI). IEEE Power Energy Soc. 2008 Gen. Meet. Convers. Deliv. Electr. Energy 21st Century, PES. IEEE 2008:1–5. https://doi.org/10.1109/PES.2008.4596535

Committee of the IEEE Computer Society M (2009) IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices. IEEE Std 13631-2008 2009:1–81

Committee of the IEEE Engineering in Medicine S, Society B (2021) IEEE Std 11073–40101™-2020, Health informatics—Device interoperability—Part 40101: Foundational—Cybersecurity—Processes for vulnerability assessment

Couraud B, Robu V, Flynn D, Andoni M, Norbu S, Quinard H (2022) Real-time control of distributed batteries with blockchain-enabled market export commitments. IEEE Trans Sustain Energy 13:579–591. https://doi.org/10.1109/TSTE.2021.3121444

Cui L, Qu Y, Gao L, Xie G, Yu S (2020) Detecting false data attacks using machine learning techniques in smart grid: a survey. J Netw Comput Appl 170:102808. https://doi.org/10.1016/J.JNCA.2020.102808

Department of Business Energy and Industry Strategy, Office of Gas and Electricity Markets. Upgrading Our Energy System. 2017.

Department of Homeland Security (2009) Cyber Security Procurement Language for Control Systems.

Ding Y, Decker C, Vassileva I, Wallin F, Beigl M (2011) A smart energy system: distributed resource management, control and optimization. IEEE PES Innov. Smart Grid Technol. Conf. Eur. https://doi.org/10.1109/ISGTEurope.2011.6162720.

Electronics Projects Focus (2020) Smart Grid Technology Working Operation and Applications 2020. https://www.elprocus.com/overview-smart-grid-technology-operation-application-existing-power-system/. Accessed 30 Jun 2021

Elliott D (2019) Renewable energy in the UK: past, present and future. Springer International Publishing, Cham. https://doi.org/10.1007/978-3-030-04765-8

Energy digitalisation taskforce (2022) Delivering a digitalised energy system. London

Esmalifalak M, Liu L, Nguyen N, Zheng R, Han Z (2017) Detecting stealthy false data injection using machine learning in smart grid. IEEE Syst J 11:1644–1652. https://doi.org/10.1109/JSYST.2014.2341597

Ford R, Maidment C, Vigurs C, Fell MJ, Morris M (2021) Smart local energy systems (SLES): a framework for exploring transition, context, and impacts. Technol Forecast Soc Change 166:120612. https://doi.org/10.1016/j.techfore.2021.120612

Grochocki D, Huh JH, Berthier R, Bobba R, Sanders WH, Cardenas AA, et al (2012) AMI threats, intrusion detection requirements and deployment recommendations. 2012 IEEE 3rd Int Conf Smart Grid Commun SmartGridComm 2012:395–400. https://doi.org/10.1109/SMARTGRIDCOMM.2012.6486016
Gunduz MZ, Das R (2020) Cyber-security on smart grid: threats and potential solutions. Comput Networks 169:107094. https://doi.org/10.1016/J.COMNET.2019.107094
Hong J, Liu CC, Govindarasu M (2014) Detection of cyber intrusions using network-based multicast messages for substation automation. 2014 IEEE PES Innov Smart Grid Technol Conf ISGT 2014. https://doi.org/10.1109/ISGT.2014.6816375
HP (2015) HP study finds alarming vulnerabilities with Internet of Things (IoT) home security systems. Strateg Focus Software, Corp News Financ Prod Serv 2015. https://www.hp.com/us-en/hp-news/press-release.html?id=1909050#.YMd94TZKhgE. Accessed June 14, 2021
Huseinović A, Mrdović S, Bicakci K, Uludag S (2020) A survey of denial-of-service attacks and solutions in the smart grid. IEEE Access 8:177447–177470. https://doi.org/10.1109/ACCESS.2020.3026923
IEEE (2013) IEEE Std 1686–2013 Standard for Intelligent Electronic Devices Cyber Security Capabilities. IEEE 2013
IEEE (2014) C37.240-2014—IEEE Standard cybersecurity requirements for substation automation, protection, and control systems | IEEE Standard | IEEE Xplore 2014. https://ieeexplore.ieee.org/document/7024885. Accessed June 15, 2021
IEEE (2020a) 2144.1-2020—IEEE Standard for Framework of Blockchain-based Internet of Things (IoT) Data management. https://ieeexplore.ieee.org/document/9329260 . Accessed June 15, 2021
IEEE (2020b) P1912—Standard for privacy and security framework for consumer wireless devices
International Electrotechnical Commission (2018) IEC 62443-4-1:2018 Security for industrial automation and control systems 2018. https://webstore.iec.ch/publication/33615. Accessed June 15, 2021
Islam SN, Baig Z, Zeadally S (2019) Physical layer security for the smart grid: vulnerabilities, threats, and countermeasures. IEEE Trans Ind Inf 15:6522–6530. https://doi.org/10.1109/TII.2019.2931436
Jurcut A, Niculcea T, Ranaweera P, Le-Khac N-A (2020) Security considerations for internet of things: a survey. SN Comput Sci 1:193. https://doi.org/10.1007/s42979-020-00201-3
Karampour A, Ashouri-Talouki M, Ladani BT (2019) An efficient privacy-preserving data aggregation scheme in smart grid. ICEE 2019—27th Iran Conf Electr Eng. 1967–71. https://doi.org/10.1109/IRANIANCEE.2019.8786482
Keerthisinghe C, Chapman AC, Verbič G (2019) Energy management of PV-storage systems: policy approximations using machine learning. IEEE Trans Ind Inf 15:257–265. https://doi.org/10.1109/TII.2018.2839059
Kirli D, Couraud B, Robu V, Salgado-Bravo M, Norbu S, Andoni M et al (2022) Smart contracts in energy systems: a systematic review of fundamental approaches and implementations. Renew Sustain Energy Rev 158:112013. https://doi.org/10.1016/J.RSER.2021.112013
Koolen D, Sadat-Razavi N, Ketter W (2017) Machine learning for identifying demand patterns of home energy management systems with dynamic electricity pricing. Appl Sci 7(11):1160. https://doi.org/10.3390/app7111160
Labib NS, Brust MR, Danoy G, Bouvry P (2019) Trustworthiness in IoT—a standards gap analysis on security, data protection and privacy. IEEE Conf Stand Commun Network, CSCN 2019:1–7. https://doi.org/10.1109/CSCN.2019.8931393
Li D, Peng W, Deng W, Gai F (2018) A blockchain-based authentication and security mechanism for IoT. Proc. - Int. Conf. Comput. Commun. Networks, ICCCN, vol. 2018, July. https://doi.org/10.1109/ICCCN.2018.8487449
Lin J, Yu W, Yang X (2016) Towards multistep electricity prices in smart grid electricity markets. IEEE Trans Parallel Distrib Syst 27:286–302. https://doi.org/10.1109/TPDS.2015.2388479
Liu S, Liu XP, Saddik A El (2013) Denial-of-Service (dos) attacks on load frequency control in smart grids. 2013 IEEE PES Innov Smart Grid Technol Conf ISGT 2013. https://doi.org/10.1109/ISGT.2013.6497846
Lu T, Guo X, Xu B, Zhao L, Peng Y, Yang H (2013) Next big thing in big data: the security of the ICT supply chain. Proc Soc 2013:1066–1073. https://doi.org/10.1109/SocialCom.2013.172
Manbachi M (2018) Impact of distributed energy resource penetrations on smart grid adaptive energy conservation and optimization solutions. Operation of distributed energy resources in smart distribution networks. Elsevier, Amsterdam, pp 101–138. https://doi.org/10.1016/B978-0-12-814891-4.00005-9
Mengelkamp E, Bose S, Kremers E, Eberbach J, Hoffmann B, Weinhardt C (2018) Increasing the efficiency of local energy markets through residential demand response. Energy Inform 1:1–18. https://doi.org/10.1186/s42162-018-0017-3
Menniti D, Pinnarelli A, Sorrentino N, Vizza P, Burgio A, Brusco G, et al (2018) A real-life application of an efficient energy management method for a local energy system in presence of energy storage systems. Proceedings of 2018 IEEE International Conference Environment and Electrical Engineering. 2018 IEEE Ind. Commer. Power Syst. Eur. EEEIC/I CPS Eur. 2018. https://doi.org/10.1109/EEEIC.2018.8494629
Mocrii D, Chen Y, Musilek P (2018) IoT-based smart homes: a review of system architecture, software, communications, privacy and security. Internet of Things 1–2:81–98. https://doi.org/10.1016/j.iot.2018.08.009
Mohammadpourfard M, Weng Y, Pechenizkiy M, Tajdinian M, Mohammadi-Ivatloo B (2020) Ensuring cybersecurity of smart grid against data integrity attacks under concept drift. Int J Electr Power Energy Syst 119:105947. https://doi.org/10.1016/J.IJEPES.2020.105947
Mokhtar M, Robu V, Flynn D, Higgins C, Whyte J, Loughran C et al (2021) Prediction of voltage distribution using deep learning and identified key smart meter locations. Energy AI 6:100103. https://doi.org/10.1016/J.EGYAI.2021.100103
National Institute of Standards and Technology (2012) Nist framework and roadmap for smart grid interoperability standards, release 1.0. Smart Grid Cybersecurity Guidel. Interoperability Stand., vol. 0, p. 19–133
National Institute of Standards and Technology (2014) Guidelines for smart grid cybersecurity. Gaithersburg, MD. https://doi.org/10.6028/NIST.IR.7628r1
Norbu S, Couraud B, Robu V, Andoni M, Flynn D (2021) Modeling economic sharing of joint assets in community energy projects under LV network constraints. IEEE Access 9:112019–112042. https://doi.org/10.1109/ACCESS.2021.3103480
North American Electric Reliability Corporation (2021) CIP Standards n.d. https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx . Accessed June 15, 2021
Ofgem (2017) Future supply market arrangements—call for evidence. 1–9

Pishva D (2017) Internet of Things: security and privacy issues and possible solution. Int. Conf. Adv. Commun. Technol. ICACT, Institute of Electrical and Electronics Engineers Inc.; p. 797–808. https://doi.org/10.23919/ICACT.2017.7890229

Rajasekaran RG, Manikandaraj S, Kamaleshwar R (2017) Implementation of machine learning algorithm for predicting user behavior and smart energy management. 2017 Int Conf Data Manag Anal Innov ICDMAI 2017. 24–30. https://doi.org/10.1109/ICDMAI.2017.8073480

Rodríguez-Molina J, Martínez-Núñez M, Martínez J-F, Pérez-Aguiar W (2014) Business models in the smart grid: challenges, opportunities and proposals for prosumer profitability. Energies 7:6142–6171. https://doi.org/10.3390/en7096142

Sha K, Wei W, Andrew Yang T, Wang Z, Shi W (2018) On security challenges and open issues in Internet of Things. Futur Gener Comput Syst 83:326–337. https://doi.org/10.1016/j.future.2018.01.059

Standard IEEE (1993) IEEE 1264–2015—IEEE guide for animal deterrents for electric power supply substations. IEEE Stand 1993:54–59. https://doi.org/10.1109/IEEESTD.1993.119208

Sunny MR, Kabir MA, Naheen IT, Ahad MT (2020) Residential energy management: a machine learning perspective. IEEE Green Technol Conf 2020;2020-April:229–34. https://doi.org/10.1109/GREENTECH46478.2020.9289737

Talaat M, Alsayyari AS, Alblawi A, Hatata AY (2020) Hybrid-cloud-based data processing for power system monitoring in smart grids. Sustain Cities Soc 55:102049. https://doi.org/10.1016/J.SCS.2020.102049

Xie L, Mo Y, Sinopoli B (2011) Integrity data attacks in power market operations. IEEE Trans Smart Grid 2:659–666. https://doi.org/10.1109/TSG.2011.2161892

Yang Q, Yang J, Yu W, An D, Zhang N, Zhao W (2014) On false data-injection attacks against power system state estimation: modeling and countermeasures. IEEE Trans Parallel Distrib Syst 25:717–729. https://doi.org/10.1109/TPDS.2013.92

Zhang Z, Wang Y, Xie L (2018) A novel data integrity attack detection algorithm based on improved grey relational analysis. IEEE Access 6:73423–73433. https://doi.org/10.1109/ACCESS.2018.2884504

Zhang Y, Kasahara S, Shen Y, Jiang X, Wan J (2019) Smart contract-based access control for the internet of things. IEEE Internet Things J 6(2):1594–1605. https://doi.org/10.1109/JIOT.2018.2847705

Publisher's Note