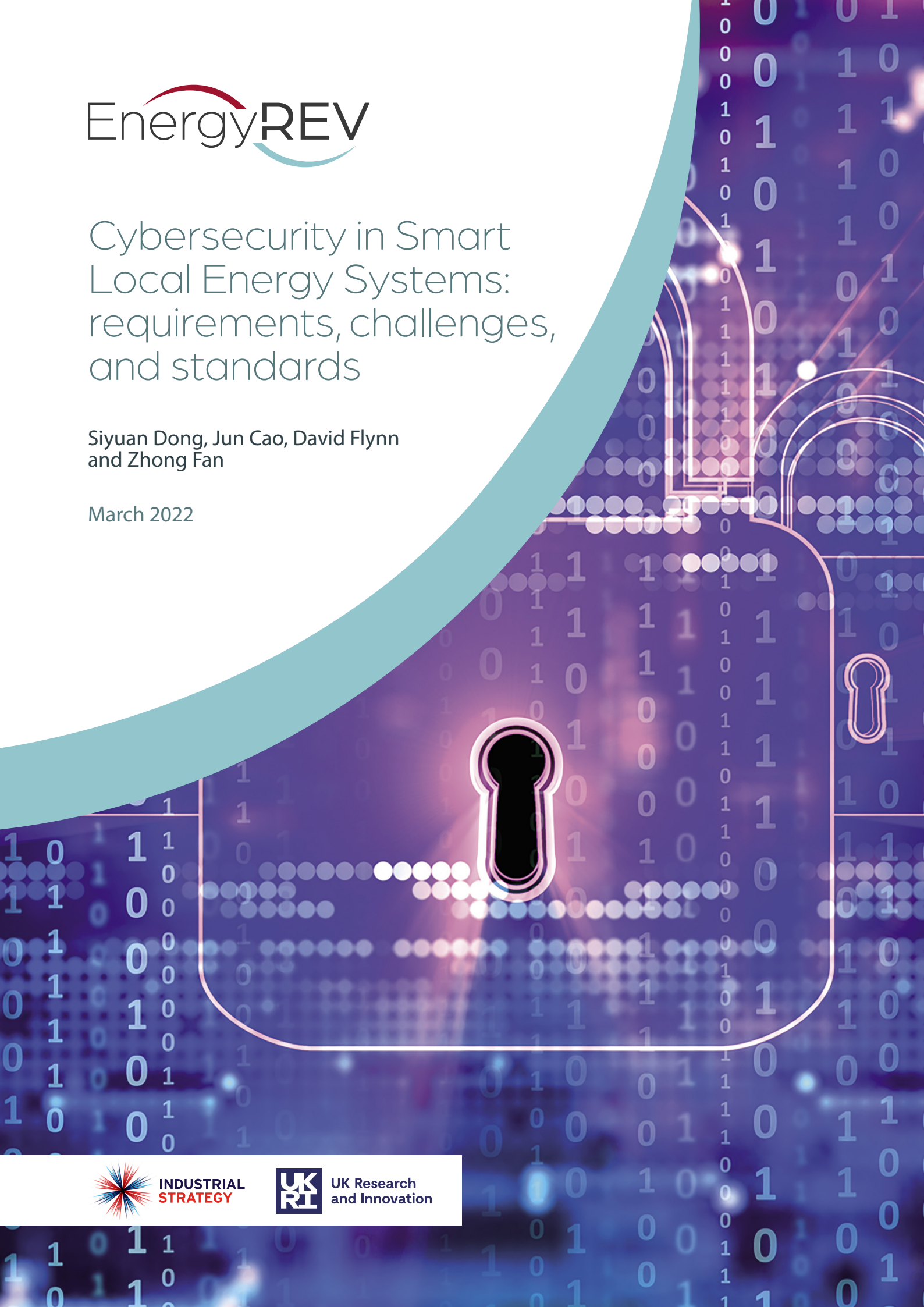
EnergyREV

Cybersecurity in Smart Local Energy Systems: requirements, challenges, and standards

Siyuan Dong, Jun Cao, David Flynn and Zhong Fan

March 2022



INDUSTRIAL STRATEGY

UK Research and Innovation

Authors

- Siyuan Dong | School of Computing and Mathematics, Keele University
- Jun Cao | School of Computing and Mathematics, Keele University
- David Flynn | James Watt School of Engineering, University of Glasgow
- Zhong Fan | School of Computing and Mathematics, Keele University

This report should be referenced as:

Dong, S., Cao, J., Flynn, D. and Fan, Z. 2022. Cybersecurity in Smart Local Energy Systems: requirements, challenges, and standards. EnergyREV, University of Strathclyde Publishing: Glasgow, UK.

ISBN 978-1-914241-06-2

Contents

Summary

Smart local energy systems (SLES) can support tailored regional solutions through the orchestration of cyber physical architectures that coordinate distributed technologies, with operational and forecasting models across all of the energy actors. Unprecedented access to new information, data streams and remotely accessible control can help achieve the multiple benefits of SLES. The expansion of the internet of things (IoT) and cyber-physical systems (CPS), means it is important both to design effective detection and management of potential cybersecurity issues, and to address the challenges of effective and adaptive governance. This should be built on standards to ensure the security of the IoT to minimise risk and harm to users.

This study conducts an extensive and critical investigation into existing standards and identifies areas to focus on in order to support the expanded adoption of cyber physical networks. Although existing standards and protocols are highly fragmented, they have been introduced to protect information security and personal privacy and the majority of them can meet the requirements of SLES.

For them to be effective four key things are needed:

- Good, comprehensive, cybersecurity guidelines that cover both physical and cyber infrastructures
- The industry needs to produce more affordable and cyber-secured devices and services
- Government and regulators should provide relevant guidelines on the minimum function and security requirements for applications
- Compliance testing and certifications should be in place and carried out by an independent third party to ensure that the components of the SLES ecosystem are designed to an acceptable security level.

Background and rationale

Opportunities

The SLES is a promising pathway for fast-track decarbonisation through "green" tech integration. Its advantages include effective provision of energy, enabling flexibility within and across energy vectors, improved resilience, and ability to cope with failure etc. SLES benefits from its complex information and communication technology (ICT) infrastructures because they can provide enhanced observability and distributed control on distributed energy resources (DERs). The smart elements include both physical smart devices and digital functionality such as artificial intelligence and analytics. The physical smart devices, consisting 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. 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 a system setup and operation and an autonomous and locally self-sufficient energy system can be achieved.

Challenges and potential risks

However, the "smart" nature of SLES means secure operation will no longer merely depend upon the secure physical status of the infrastructure, bringing the importance of cybersecurity to an unprecedented level. In a traditional system the utility companies usually have the ownership of the entire infrastructure or use a managed service. In either case they tend to prioritise cybersecurity during system acquisition and ensure that the correct security measures are in place. In SLES, emerging technologies, especially built upon IoT, are usually designed for easy adoption so that consumers can operate devices through home area networks (HANs) or wide area networks (WANs). The number of consumer-owned smart devices can easily outnumber those owned and operated by the utility. However, most consumers may not have the technical expertise or incentives to prioritise or maintain infrastructure security. This makes it hard for the utility or system operators to monitor and manage devices and leads to a disparity in security protection. To solve this problem, different networks need to be interconnected to ensure the utility companies can operate smart devices and DERs together with consumers in a collaborative manner.

Most IoT-based devices adopted in SLES are manufactured by third parties or private companies. The secure operation of the power system is based on a stable ICT supply chain, and any disruption of its components can lead to catastrophic impacts on the whole system. Many security concerns and incidents can be traced back to the inadequate management and risk of manufacturers and suppliers. In most real-life deployments, third parties or private companies are given access to key infrastructure assets and critical information without thorough reviews. Although this may contribute to faster service delivery and easier integration, it can lead to catastrophic impacts if not properly managed.

The use of HANs and WANs can also present security problems. On the positive side they make it easy to manage the system, allowing users and utility companies to obtain a more accurate understanding of consumer demand and the use of DERs. This means they can participate in more complex system operation, such as demand side response. However, using an external WAN can also increase the opportunities for attack, leading to private data breaches, device compromise, and even instability of the whole system. The substantial growth in smart appliances and DERs in the SLES will essentially increase cyber-physical interdependencies.

Cybersecurity of SLES

The increased use of IoT will enable SLES to integrate with existing energy networks, elevating the interdependence of the cyber and physical infrastructure to an unprecedented level. Successful SLES operation will be heavily reliant upon not only the physical security of the assets, but also the cybersecurity of the infrastructures. For this reason, SLES can easily attract some unexpected and unwanted threats and attacks. 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.

As a result management should consider not only the specific operational and privacy threats, but also strategic management for peer to peer trading networks and the wider network. There are three cybersecurity objectives: to protect information being stolen, compromised, or attacked. This is shown in Table 1, which provides the principles for cyber threats management.

Table 1 Cybersecurity objectives triads

Objectives	Content
Confidentiality	To protect personal privacy and proprietary information from unauthorised access. It emphasises the need for information protection, requiring relevant measures to ensure only authorised are allowed to obtain the information.
Integrity	To protect data and preserve it from any accidental or malicious modification. The data must not be changed in an unauthorised or undetectable manner. It involves maintaining the consistency, accuracy, and trustworthiness of data during storage, transmission, and usage.
Availability	To ensure the information is available when authorised users need to access it, even when the network is under attack and facing flooded traffic.

To meet the growth of distributed and integrated technologies into cyber-physical systems 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 in other markets, therefore it's important to understand current best practice in infrastructure security standards and protocols applied to the smart grid. Our research aims to assess the existing standards for coverage, purpose, and significance to real-world implementations. Evaluating best practice in the smart grid infrastructure is helpful for understanding how those standards are relevant to SLES and to identify the gap between existing standards and future requirements.

The development of cybersecurity standards

The development of cybersecurity standards mirrors the trend of technological advancement. Initially, there were no intelligent or smart control systems or devices in the system. Therefore, in the 1990s cybersecurity protection mainly consisted of enhancing the security of physical assets. Relevant precaution and prevention measures were provided, such as physical obstacles and enclosure, security patrols and video surveillance.

> IEEE 1264 Guide for Animal Deterrents for Electric Power Supply Substations and IEEE 1402 Guide for Electric Power Substation Physical and Electronic Security were proposed to protect assets from animal and human intrusions. They define types of intrusions and identify subsequent problems and impacts, evaluated by several parameters, such as intrusion location and seriousness of impacts. Relevant precautions and prevention measures are provided, such as physical obstacles and enclosures and video surveillance.

With the development of cybersecurity protection, most standards focused on design and management at a macro systematic level or an application-specific level. They emphasised the importance of cybersecurity of the assets and the importance of undertaking regular security risk and vulnerability assessment.

> The DHS Cyber Security Procurement Language for Control System combines many requirements into 11 high-level topics, such as system design, physical and cyber threat and vulnerability detection. Each topic addresses a specific issue or concern in a control system, and describes a rationale, from specification language to factory and site acceptance test measures.

The protection of communication networks as part of industrial control and automation system was also addressed to handle the proliferation of the Internet.

> IEEE C37.240 Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems aims to protect the security of interfaces between control systems and standardise the foundation requirements for communication components. It also highlights the importance of monitoring and auditing security events and policies and conducting periodic security tests.

The surge of electronic devices has facilitated the digitalisation of energy systems that need to handle substantial amounts of information and data exchange. As a result, joint efforts by academia and industry have been trying to propose relevant standards or protocols to ensure data and information security.

Advanced Metering Infrastructure System Security Requirement was issued in 2008 in the US. It aims to provide a set of security requirements to ensure a reliable system and consumer confidence. The requirement can be generalised into three categories: a) primary security services (aims to protect confidentiality and privacy, integrity, availability, identification); b) supporting security services (such as detection, risk assessment, cryptography and certificate); and c) assurance services (such as accountability, and access control).

IEEE P1912 Standard for Privacy and Security Framework for Consumer Wireless Devices focuses on data privacy and security, which defines a privacy scale where data can refer to personal identifiable information. It includes assessment tools that are of great importance for the future applications on the end-user side.

Meanwhile, more risk management guidelines have been introduced to enhance information security.

IEEE Std 11073-40101 Cybersecurity—Processes for vulnerability assessment proposes an auditable approach to identification and assessment of cybersecurity vulnerabilities and estimation of risks, which is a useful tool and can be used as a reference method for future smart devices development.

Findings and suggestions

Findings

The previous section has investigated the development of cybersecurity standards and protocols 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 the management strategy of cybersecurity issues. The requirements included in the standards differ from each other, in terms of technical details, scope and thematic coverage. Some publications extend or partially repeat requirements from other standards, and some are only supplementary documents to others.

Our findings suggest that a considerable number of existing standards or protocols would apply to the application and infrastructure of SLES, such as industry automated and control systems, electric vehicles, and intelligent electronic devices. The standards 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.

However, the standards are not comprehensive and some only address cybersecurity to a certain extent. Some are specific to certain industries, while others provide general guidelines that are applicable to any industry or organisation but provide no technical details. The majority of the standards focus on securing one or a few components or security features in the system. A systematic cybersecurity management framework is reliant upon clear definitions of SLES and explicit guidelines on its operation and governance.

Information security is becoming increasingly important due to the growing penetration of IoT and digitalisation of the energy industry. But it is hampered by the fact that different standards were put in place to standardise data encryption, transmission, storage, and format to enhance interoperability between different system components. Other standards were designed to protect personal data and privacy via both algorithm and edge device design. Complex requirements are imposed to ensure certain levels of security measures embedded in electronic devices by manufacturers protect the cybersecurity of both the system and users. For this reason, adherence to certain standards must become the norm for smart device development. Comprehensive standards are needed as the baseline to provide principles to ensure the scalability and flexibility of SLES.

Suggestions

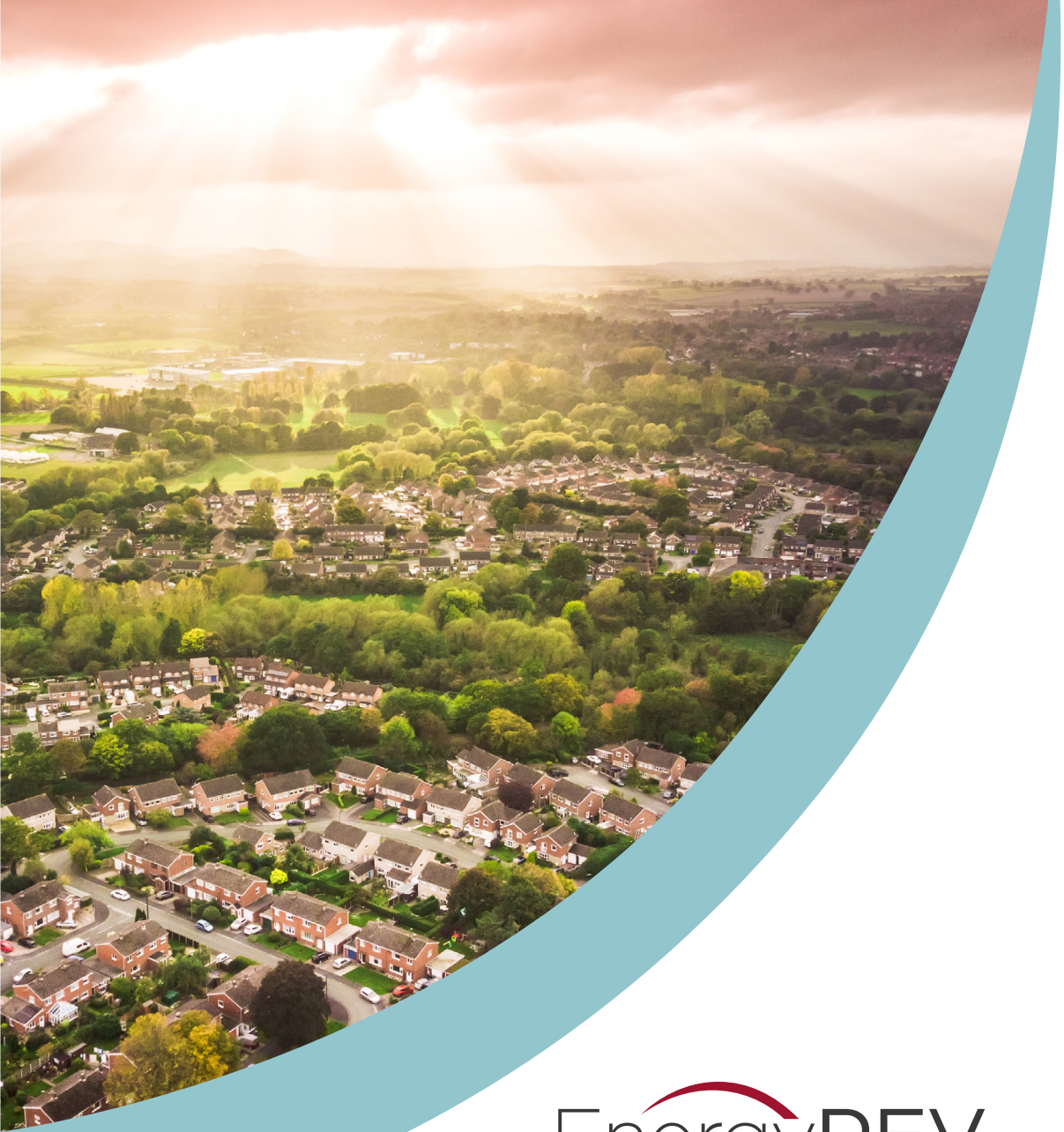
Due to the interdependency of physical and cyber infrastructures, the cybersecurity of SLES should focus on protecting both aspects. A good, comprehensive, cybersecurity guideline should include the following:

- 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
- Communication system protection.

For industry, more efforts are needed to provide more affordable and cyber-secured devices and services. More innovative technologies should also be implemented. A good balance between the affordability and quality of cybersecurity should be achieved so that IoT products can be more easily accessed by consumers.

Government and regulators should set out clearly what standards are mandatory and regulate data management. Clear definitions and guidelines on SLES should be a priority. A tailored cybersecurity management strategy needs to be based on a good understanding of system setup, operation, and governance. A few baseline standards are needed to address the system's minimum security requirements, so that relevant components or technologies can be adopted to meet minimum function and security requirements.

Compliance testing and certifications should play an important role in SLES and the wider energy system. The goal should be consistency across the whole SLES ecosystem. To achieve this it is necessary to conduct testing and certification by an independent party, which can assure regulators that a satisfactory security level is provided in key SLES ecosystem actors. It would be beneficial to move closer to energy system integration supporting the optimisation of the whole system.



EnergyREV

Want to know more?

Sign up to receive our newsletter and keep up to date with our research, or get in touch directly by emailing info@energyrev.org.uk

www.energyrev.org.uk

@EnergyREV_UK

info@energyrev.org.uk

About EnergyREV

EnergyREV was established in 2018 (December) under the UK's Industrial Strategy Challenge Fund Prospering from the Energy Revolution programme. It brings together a team of over 50 people across 22 UK universities to help drive forward research and innovation in Smart Local Energy Systems.

ISBN 978-1-914241-06-2

EnergyREV is funded by UK Research and Innovation, grant number EP/S031898/1

INDUSTRIAL STRATEGY

UK Research and Innovation