Journal of Infrastructure, Policy and Development 2024, 8(15), 8631.
https://doi.org/10.24294/jipd8631

Review

A review on cybersecurity for distributed energy resources: Opportunities for South Africa

Oliver Dzobo[*], **Lucas Tivani, Lindani Mbatha**

University of Johannesburg, Johannesburg 2092, South Africa
*** Corresponding author:** Oliver Dzobo, oliverd@uj.ac.za

CITATION

Dzobo O, Tivani L, Mbatha L. (2024). A review on cybersecurity for distributed energy resources: Opportunities for South Africa. Journal of Infrastructure, Policy and Development. 8(15): 8631. https://doi.org/10.24294/jipd8631

ARTICLE INFO

Received: 15 August 2024
Accepted: 5 September 2024
Available online: 13 December 2024

Abstract: Distributed Energy Resources (DERs), such as solar photovoltaic (PV) systems, wind turbines, and energy storage systems, offer many benefits, including increased energy efficiency, sustainability, and grid reliability. However, their integration into the smart grid also introduces new vulnerabilities to cyber threats. The smart grid is becoming more digitalized, with advanced technologies like Internet of Things (IoT) devices, communication networks, and automation systems that enable the integration of DER systems. While this enhances grid efficiency and control, it creates more entry points for attackers and thus expands the attack surface for potential cyber threats. Protecting DERs from cyberattacks is crucial to maintaining the overall reliability, security, and privacy of the smart grid. The adopted cybersecurity strategies should not only address current threats but also anticipate future dangers. This requires ongoing risk assessments, staying updated on emerging threats, and being prepared to adapt cybersecurity measures accordingly. This paper highlights some critical points regarding the importance of cybersecurity for Distributed Energy Resources (DERs) and the evolving landscape of the smart grid. This research study shows that there is need for a proactive and adaptable cybersecurity approach that encompasses prevention, detection, response, and recovery to safeguard these critical energy systems against cyber threats, both today and in the future. This work serves as a valuable tool in enhancing the cybersecurity posture of utilities and grid-connected DER owners and operators. It allows them to make informed decisions, protect critical infrastructure, and ensure the reliability and security of grid-connected DER systems in an evolving energy landscape.

Keywords: cyberattacks; cyber physical space; cybersecurity for DER; cybersecurity framework; cybersecurity regulations; distributed energy sources (DER); smart grid cybersecurity

1. Introduction

Power utilities worldwide are increasingly focused on transitioning to clean and sustainable energy sources like solar and wind (Dzobo et al., 2011). This shift is crucial for reducing greenhouse gas emissions and mitigating climate change. To maximize the efficiency and effectiveness of integrating renewable energy sources, a smart grid is essential (Faquir et al., 2021; Mishra et al., 2020). This involves the integration of Information and Communication Technology (ICT) with electrical systems. This technology integration enables real-time monitoring and control of Distributed Energy Resources (DERs). The integration of ICT and DERs into the smart grid leads to improved efficiency and sustainability in the energy sector. Real-time monitoring and control allow for better resource management, grid stability, and response to fluctuations in energy supply and demand. The transition to a smart grid and the widespread use of DERs introduce new challenges for cybersecurity

(Gunduz and Das, 2020; Langer et al., 2015). The increased connectivity and data exchange in the smart grid create vulnerabilities that cyber attackers may exploit. Conducting risk assessments and implementing robust cybersecurity measures specific to the DER environment is therefore crucial to ensure the secure and reliable operation of Distributed Energy Resources in this evolving energy landscape.

A smart grid is a complex, interconnected system that leverages digital technology to optimize energy distribution and management (EUAC 2013; Langer et al., 2015; NIST, 2014a). It integrates a wide array of components and technologies to enable real-time monitoring, control, and decision-making for improved grid efficiency and sustainability. The smart grid facilitates two-way data exchange, allowing for not only the collection of data from various sources but also the ability to send control commands back to those sources. Communication networks are essential for the remote monitoring, control, and management of the smart grid. They enable data exchange and communication between various components of the smart grid. The smart grid includes a wide range of physical processes, such as power plants, data management systems, energy storage systems, communication infrastructure, sensors, actuators, smart meters, Internet of Things (IoT) devices, and control systems. Sensors and microprocessors are crucial components of the smart grid. They measure and control physical processes, providing real time data and enabling precise control. Control systems play a vital role in making decisions based on the information collected from sensors and other sources. This decision-making ensures the stability and reliability of the grid. Knowledge management systems are responsible for storing, analyzing, and sharing the information collected from various sources. This enhances the overall efficiency, reliability, and sustainability of the smart grid.

The integration of DER into the smart grid expands the potential cyberattack surface due to interconnectedness (Gunduz and Das, 2020; Mishra et al., 2020; NIST, 2014a). The various components and systems become potential entry points for cyber attackers. While remote monitoring and control offer numerous benefits, they can also introduce vulnerabilities if not properly secured. Unauthorized access to these systems can lead to disruption or compromise of DER operations. The communication protocols used in DER systems can be exploited by cyber attackers. They may intercept or manipulate communications between devices, potentially causing data breaches or control issues. Inadequately secured data transmission channels can be exploited for eavesdropping or data manipulation, compromising the confidentiality and integrity of data. Relying on third-party services for various functions can introduce risks, particularly if those services do not adhere to robust security standards. Integration with third-party providers should therefore be carefully managed. Outdated firmware and software are often susceptible to known vulnerabilities. Keeping these components up to date is essential for mitigating cybersecurity risks. Supply chain vulnerabilities can introduce risks at the manufacturing and distribution stages. Malicious actors may compromise components during production, affecting the security of the DER systems. Human behavior and actions play a significant role in cybersecurity. Inadequate training, poor password management, and risky behavior can increase the vulnerability of

DER systems. Each of these factors pose unique threats to the functionality and security of DERs.

One example of smart grid cyber-attack is the one that happened on the Ukrainian power grid in December 2015 (USA, 2021). It was a highly sophisticated and coordinated attack that resulted in a widespread power outage affecting over 200,000 customers. The cyber attackers gained access to the control systems of three regional power distribution companies in Ukraine. The attackers used a combination of spear-phishing emails, malware, and other tactics to gain access to the systems and disrupt the power supply. The attackers were able to take control of the power distribution systems and remotely disconnect the power supply to the affected areas. The attack caused significant disruption and economic losses, with some parts of Ukraine experiencing power outages for up to six hours. This cyberattack demonstrated the potential consequences of a successful cyberattack on critical infrastructure, highlighting the need for improved cybersecurity measures and preparedness. Following the attack, Ukrainian authorities and international cybersecurity experts conducted a thorough investigation to identify the root cause of the attack and prevent similar incidents in the future. The investigation revealed that the attackers had used sophisticated malware, known as Black Energy, to gain access to the control systems of the power distribution companies. The malware was able to evade detection by security software and use advanced encryption techniques to communicate with the attackers’ command and control servers. The Ukrainian government and power distribution companies have since implemented several cybersecurity measures to improve the resilience of the country’s power grid. These measures include regular risk assessments, vulnerability scans, and employee training to ensure that personnel are aware of cybersecurity risks and best practices. The government has also established a national cybersecurity centre to coordinate and respond to cyber incidents and improve the overall cybersecurity posture of critical infrastructure. South Africa is undergoing changes in its power grid and it is expected to have a significant increase in DER integration (Owusu-Mante, 2020). As DER integration increases the digitalization of the power grid is also expected to increase and thus increasing the cyberattack space. This paper highlights some of the challenges in addressing cybersecurity of DER systems and opportunities that can be exploited by South Africa in preparation for a whole digital power grid. According to the knowledge of authors of this paper, there have not been any research study that addresses the issue of cybersecurity of DERs in the South African context. This paper is therefore expected to provide useful information to different stakeholders involved in integration of DERs into the power grid such as power utilities, manufacturers and government bodies. The information is expected to help them develop robust cybersecurity measures that will ensure the security and integrity of interconnected smart grids. The contributions of this research paper are as follows:

- Provide a comprehensive review of Distributed Energy Resources (DER) network support features that increase the cyberattack surface
- Identification and analyses of possible cyber threats in DER networks
- Provide a comprehensive review of cybersecurity frameworks and standards for DERs and provide recommendations for establishing a baseline level of cybersecurity for DER deployment in DER networks.

The remainder of this paper is arranged as follows: Section II presents the methodology that was adopted to select the various sources that were used to conduct the comprehensive literature review; Sections III and IV provide the motivation and the DER network support features that increase the cyberattack space respectively; In Sections V and VI the DER cybersecurity frameworks and standards are reviewed and discussed. The recommendations and future directions are presented in Section VII.

2. Methodology

This literature review utilized various sources including industry and government publications, academic technical papers, and public domain sources to conduct a comprehensive investigation.

2.1. Industry and government publications

The study analyzed South African publications on the history and future power grid, selecting relevant ones based on subject matter, as illustrated in **Figure 1**. A database was created to summarize and report on cybersecurity for DER.

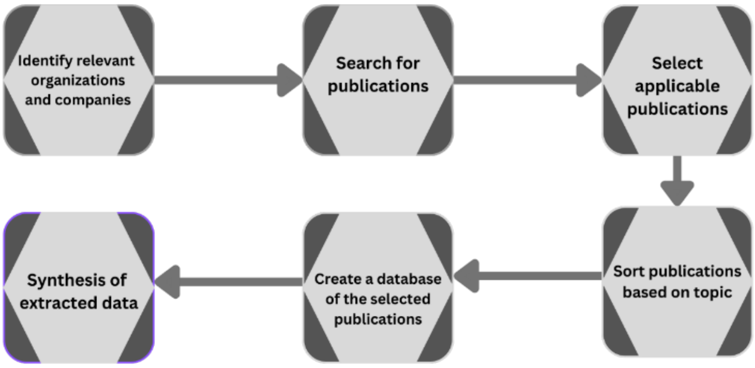
Identify relevant organizations and companies
Search for publications
Select applicable publications
Sort publications based on topic
Create a database of the selected publications
Synthesis of extracted data

Figure 1. Procedure adopted for selection of government publications.

2.2. Academic technical papers

The selection of academic technical papers was guided by guidelines from (Kitchenham and Charters, 2007), as illustrated in **Figure 2**.

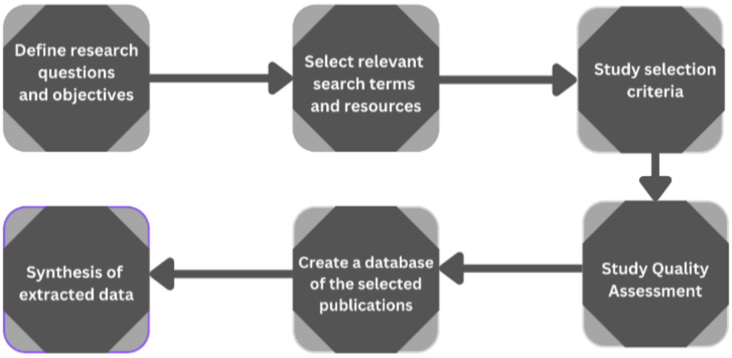
Define research questions and objectives
Select relevant search terms and resources
Study selection criteria
Study Quality Assessment
Create a database of the selected publications
Synthesis of extracted data

Figure 2. Procedure adopted for selection of academic technical papers.

Academic technical papers were sourced from the Web of Science database, including MDPI, IEEE, Elsevier, and Springer, using specific criteria for inclusion and exclusion. Relevant studies were sorted based on publication date, title, abstract, conclusion, and content review, including insights on current practices and trends.

3. Motivation

The South African government's commitment to advancing the adoption of renewable energy is indeed a significant development in its efforts to combat climate change and transition to a more sustainable energy system. Its commitment to achieving net-zero emissions by 2050 is in line with the global climate goals established in the Paris Agreement (Calitz and Wright, 2021; Owusu-Mante, 2020). This means that the country aims to balance its greenhouse gas emissions with removals, either through emissions reductions or carbon removal techniques. One of the key initiatives in this direction is the South African Renewable Energy Independent Power Producer Procurement Programme (REIPPPP) (Calitz and Wright, 2021; Owusu-Mante, 2020). REIPPPP is designed to encourage private sector involvement in grid-connected renewable energy projects. This approach leverages private investments to expand renewable energy capacity, reducing the burden on the government and public finances. The IRP 2010 is a comprehensive plan that outlines South Africa's energy generation mix. It sets ambitious targets for renewable energy generation, with a goal of reaching 17,800 MW of renewable energy capacity by 2030 (Owusu-Mante, 2020). This plan provides a clear roadmap for the country's energy transition. These initiatives reflect South Africa's commitment to diversifying its energy mix. By expanding renewable energy capacity, the country reduces its dependence on fossil fuels, which is not only important for mitigating climate change but also for enhancing energy security and reducing the impact of energy price fluctuations. DER adoption significantly contributes to sustainability by reducing the reliance on fossil fuels. DER, especially when coupled with energy storage, offers resilience benefits. During major disasters and power grid outages, DER can provide emergency power, enhancing community resilience. This capability ensures essential services remain operational in critical situations (Notton, et al., 2018). The integration of DER aligns with the broader transition toward a digitally interconnected power grid. This transformation introduces automation and enhanced connectivity, which drives efficiency and improves energy management. As DER systems become more automated and interconnected, they become potential targets for cyber attackers. These attackers continually evolve their techniques to target both information technology (IT) and operational technology (OT) systems of DER systems. Addressing cybersecurity challenges is therefore crucial for the entire DER industry ecosystem to ensure the reliability and security of power grid.

4. DER network support features

The integration of Distributed Energy Resources (DER) into the smart grid expands the cyberattack space (Faquir et al., 2021; Gunduz and Das, 2020; NIST, 2014a). The network support features that increase the cyberattack space in DER systems include (Mishra et al., 2020; NIST, 2014a).

- Interconnectedness: The interconnected nature of DER systems makes them vulnerable to a range of cyber threats. Older, legacy infrastructure often lacks modern cybersecurity considerations. This makes it more susceptible to cyberattacks, as these systems may not have the security features and updates needed to defend against evolving threats. Retrofitting or upgrading these systems to meet current security standards is essential. Newly integrated DER systems are increasingly interconnected with various devices, applications, and networks, both internally within the utility infrastructure and externally through the internet. This interconnectedness is essential for efficient operation but also creates multiple entry points for cyberattacks such as data breaches, denial-of-service attacks, malware infections, unauthorized access, and ransomware attacks, which can disrupt operations, compromise sensitive data, and pose physical safety risks.
- Remote monitoring and control: Remote monitoring and control are essential features of DER systems. They allow operators to access real-time data, make adjustments to settings, and perform maintenance tasks without physically being present at the site. This convenience is critical for efficient operations, especially when managing a distributed network of energy resources. Remote access and control enhance operational efficiency, reduce response times to issues, and enable predictive maintenance. These capabilities can optimize energy production, distribution, and consumption, ultimately contributing to cost savings and grid stability. The same remote capabilities that offer numerous benefits can also create security concerns. Without proper security measures, remote access points can become entry points for cyberattacks. Attackers may exploit these vulnerabilities to gain unauthorized access, disrupt operations, or manipulate settings. Unauthorized access to DER systems can result in various adverse outcomes, such as altering energy production or consumption, causing grid instability, or tampering with sensitive data.
- Communication protocols: DER devices, such as solar panels, wind turbines, and energy storage systems, rely on communication protocols to exchange data and commands. These protocols enable devices to communicate with each other, with central control systems, and with external entities like grid operators or utility providers. Communication protocols are essential for the seamless operation and control of DER systems. However, vulnerabilities in these protocols can be exploited by cyber attackers. These vulnerabilities may include weaknesses in protocol design, improper implementation, or outdated versions that lack security enhancements. Cyber attackers can exploit these vulnerabilities to intercept or manipulate communication between DER devices. They may eavesdrop on the data being exchanged, modify commands, or inject malicious data, leading to various adverse outcomes.
- Data transmission: Much of the data generated by DER systems is sensitive in nature. It can include data related to energy production, consumption patterns, load forecasting, and even information about system vulnerabilities or maintenance schedules. This data is typically transmitted within the DER

system and to external entities, such as utility providers, grid operators, or energy management systems. The data exchange is crucial for efficient energy management and grid stability. The security of this data is of paramount importance. If it’s not adequately protected, malicious actors can exploit vulnerabilities to intercept sensitive data in transit, manipulate or alter data to provide false information, data privacy violations of individuals or organizations by gaining access to data.

- Third-Party services: Many DER systems depend on third-party services to enhance their capabilities. These services can include data analytics platforms, energy management software, predictive maintenance solutions, and more. Third-party services provide DER operators with specialized expertise and tools, allowing them to make more informed decisions, optimize energy production, and maintain the reliability of their systems. Integrating third-party services into DER systems introduces potential security risks, as these services may not have the same level of security measures in place as the primary operator’s infrastructure. Third-party services may rely on a global supply chain for hardware and software components. Malicious actors can exploit vulnerabilities at various points in the supply chain to compromise the security of the services. Insecure connections to third-party services can become entry points for cyberattacks, potentially leading to unauthorized access and data breaches.
- Firmware and software updates: DER devices require regular updates to address security vulnerabilities, improve performance, and add new features. Outdated firmware or software in DER devices can become attractive targets for cyber attackers. As security vulnerabilities become known, attackers may exploit these weaknesses to gain unauthorized access, manipulate operations, or compromise data integrity. Security updates are particularly crucial to mitigate evolving cyber threats. DER devices are often dispersed across various locations, making it challenging to coordinate and execute updates. DER devices are interconnected with other components of the smart grid, meaning updates can have cascading effects that need to be carefully managed. DER systems can consist of various devices, each with its own firmware and software requirements, making updates diverse. Updates can temporarily disrupt device operations, requiring careful scheduling to minimize impact on energy production and distribution.
- Supply chain risks: Components used in DER systems, including hardware and software, may come from various suppliers and manufacturers. This supply chain diversity introduces variations in the origin, quality, and security features of these components. One significant risk in the supply chain is the presence of counterfeit or tampered components. Malicious actors may introduce counterfeit or manipulated hardware or software into the supply chain, which can compromise the security and functionality of DER systems. Components from different suppliers may have their own set of security features and potential vulnerabilities. These variations in security features make it challenging to maintain a consistent security posture across the DER

environment. Managing security across this heterogeneous environment can be very challenging.

- Human factors: Insider threats refer to the risk of individuals within an organization, such as employees or contractors, intentionally or unintentionally causing harm to the organization’s security, data, or operations. One of the key factors in mitigating insider threats and human errors is the level of training, awareness, and education among personnel with access to DER systems. Insufficient training and a lack of awareness can lead to poor security practices and risky behavior. Human errors are unintentional actions or mistakes that can compromise cybersecurity. These errors can include misconfigurations, accidental data exposure, and other inadvertent actions that may weaken security.

To address these challenges, robust cybersecurity measures must be implemented across DER networks, including encryption, access controls, regular updates, intrusion detection, and monitoring (Miessler, 2015; Pishva, 2017; NIST, 2014a). Additionally, risk assessments should be conducted to identify and prioritize potential threats and vulnerabilities specific to the DER environment.

Potential threat scenarios targeting DER systems

Attacks against Distributed Energy Resources (DERs) can have far-reaching consequences due to the interconnected nature of these systems and their dependencies on various devices, communication networks, and third-party services. The following are potential threat scenarios that target DER systems (ENA, 2020; He et al., 2016; Miessler, 2015; NESCOR, 2015; Pishva, 2017; Turner et al., 2015; Wu et al., 2018). It should be noted that the examples given are not exhaustive.

- Malicious DER Commands Sent Through Utility-Wide Area Network (WAN) Scenario: Cyberattacks on the remote communication between power utilities and DERs. Attackers disrupt, deny, or tamper with messages, potentially leading to disruptions in smart grid operations, cascading failures, and destabilization of the system. Attack methods: Exploiting network protocols, misusing cryptographic operations, gaining unauthorized access to power utility and DER systems.
- Malware or unauthorized access to smart inverters and DER controllers Scenario: Attackers gain access to or infect smart inverters and DER controllers, impacting the stability and efficiency of smart grid operations. These devices, including battery and electric vehicle (EV) controllers, can be manipulated, tampered with, or provide false information, affecting power quality and overall energy management. Attack methods: Malware infection, unauthorized access to controller interfaces, exploitation of vulnerabilities in device firmware.
- Manipulation of Data in Communication Networks: Scenario: Attackers intercept and manipulate data exchanged between DER devices and other components in the smart grid. Attack methods: Manipulating network protocols, exploiting vulnerabilities in communication infrastructure, or using man-in-the-middle attacks to intercept communications.

- Supply chain attacks on DER components: Scenario: Malicious actors compromise components used in DER systems at various points in the supply chain, such as during manufacturing or distribution. Attack methods: Tampered components may introduce vulnerabilities or backdoors, potentially leading to unauthorized access or system manipulation.
- Insider Threats and Human Error: Scenario: Insiders with access to DER systems, intentionally or inadvertently, cause security incidents or operational disruptions. Attack methods: Exploiting vulnerabilities in communication channels, software, or human errors that lead to data exposure.
- Unauthorized access to Third-Party services: Scenario: attackers gain unauthorized access to third-party services, which are integrated with DER systems for functions like data analytics or energy management. Consequences: Compromised third-party services can lead to data breaches or disruptions in DER operations.
- Denial-of-Service (DoS) Attacks: Scenario: Attackers launch DoS attacks against DER devices, rendering them temporarily inoperable. This disruption can affect energy production, distribution, and grid management. Attack Methods: Overwhelming devices with excessive network traffic or exploiting software vulnerabilities to crash or freeze devices.

5. Cybersecurity framework for DER

A cybersecurity framework is an essential tool for organizations, especially those involved in managing smart grids (NIST, 2014a). Such a framework provides a structured approach to identifying, addressing, and mitigating cybersecurity threats and risks (EUAC, 2012; NIST, 2014a; NCFSA, 2015). Proactive cybersecurity measures are crucial for safeguarding critical infrastructure, including smart grids. Preventing cyberattacks and ensuring the resilience of energy distribution networks are top priorities. To effectively address cybersecurity threats, organizations must have a clear understanding of baseline operations within their systems (NIST, 2014a). This knowledge serves as a foundation for detecting anomalous cyber activity. Detecting unusual or anomalous cyber activity is a key component of a robust cybersecurity strategy. Early detection allows for timely response and mitigation.

Distributed Energy Resources (DER) cybersecurity involves multiple domains and stakeholders (ENA, 2020; EUAC, 2012; NIST, 2014a). These parties play integral roles in ensuring the security and resilience of DER systems. Collaboration is essential for addressing cyber threats, implementing security measures, and protecting energy distribution networks. **Figure 3** illustrates how best practices from various domains can inform DER cybersecurity. This comprehensive approach helps organizations establish a strong foundation for a comprehensive DER cybersecurity program.

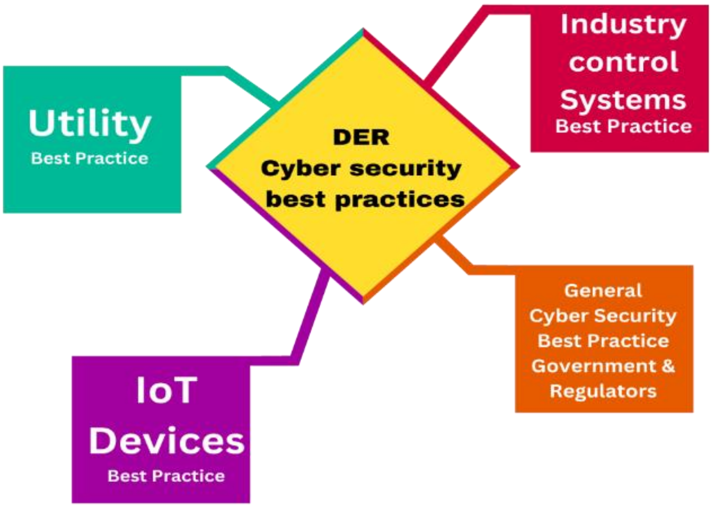

Figure 3. Cybersecurity best practices of different domains.

The figure underscores the critical importance of collaboration and coordination among various domains and stakeholders in building a resilient and secure Distributed Energy Resources (DER) ecosystem. Each stakeholder brings unique expertise and responsibilities to the table, contributing to the overall cybersecurity and stability of the smart grid. Each stakeholder brings their unique knowledge and expertise to the cybersecurity domain. Collaboration allows the sharing of insights and experiences to collectively address emerging cybersecurity challenges. Combining the efforts of power utilities, manufacturers, industry associations, and standards bodies creates a holistic approach to cybersecurity, covering various aspects of DER systems, from operations to device security. Aligning with industry standards and best practices ensures consistency and compliance with recognized cybersecurity guidelines, promoting a higher level of security across the ecosystem. Effective collaboration enables stakeholders to respond quickly to emerging threats, vulnerabilities, or incidents, mitigating potential risks and ensuring the stability of the smart grid.

Power utilities: Power utilities are central to the operation of the smart grid and the integration of DER systems. They are responsible for managing and operating the smart grid, ensuring the security and resilience of their networks, and maintaining reliable energy distribution. Their expertise lies in understanding the operational aspects of the smart grid, making them essential for its day-to-day functioning and cybersecurity.

Manufacturers of DER devices and components: Manufacturers of DER devices, including IoT (Internet of Things) and industrial control systems, play a pivotal role in building cybersecurity features into their products. They are responsible for developing secure hardware and software components, adhering to cybersecurity standards, and implementing best practices. This helps ensure the security of the DER devices and components that are integrated into the smart grid.

Industry associations and standards bodies: Industry associations and standards bodies have a crucial role in establishing and promoting cybersecurity standards and best practices within the energy industry. They provide guidance and frameworks to enhance the security of DER systems and the smart grid. Compliance with these standards helps create a unified approach to cybersecurity.

5.1. NIST cybersecurity framework

The NIST created the NIST Cybersecurity Framework, a collection of best practices and recommendations, to assist enterprises in managing cybersecurity risks and safeguarding vital infrastructure, including smart grid technologies (NIST, 2014a; NIST, 2014b; NIST, 2014c). The framework offers a flexible and scalable method for managing cybersecurity risk and is built on five key functions: identify, protect, detect, respond, and recover. The NIST cybersecurity framework standards are displayed in **Figure 4** (NIST, 2018).

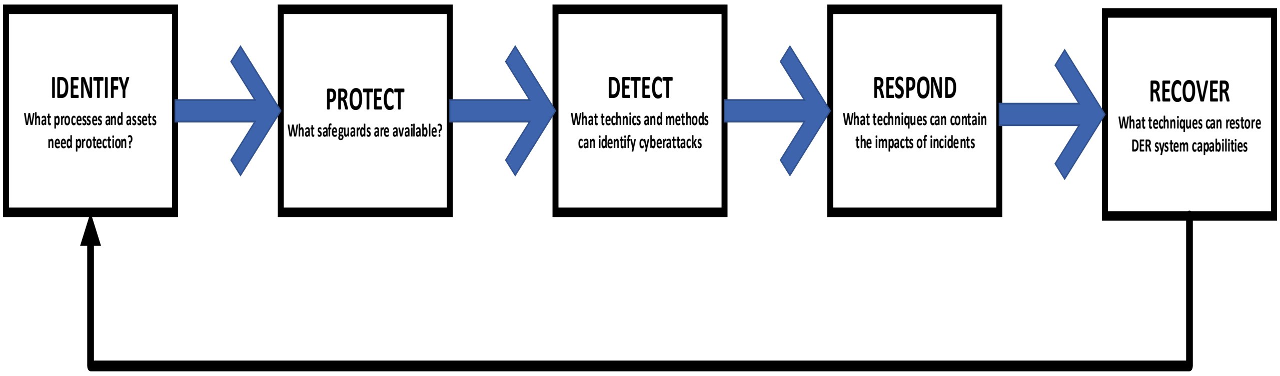
IDENTIFY
What processes and assets need protection?
PROTECT
What safeguards are available?
DETECT
What technics and methods can identify cyberattacks
RESPOND
What techniques can contain the impacts of incidents
RECOVER
What techniques can restore DER system capabilities

Figure 4. NIST cybersecurity framework guidelines.

To protect against numerous cyber threats and attacks that can jeopardize the security and reliability of smart grid systems, cybersecurity in DER systems requires a complete strategy. It also entails analyzing the threat landscape, managing risks, building secure communication infrastructure, control system security, endpoint security, data security and privacy, incident response and recovery, regulatory compliance, awareness and training, and data security and privacy.

One example of a comprehensive cybersecurity best practice program is one adopted by Duke Energy (EPRI, 2020). Duke Energy is one of the largest electric power holding companies in the United States and has implemented a comprehensive cybersecurity program to protect its smart grid system. The program is designed to identify and mitigate cybersecurity risks and ensure the secure and reliable operation of the company’s power generation, transmission, and distribution systems. The Duke Energy cybersecurity program includes regular risk assessments, vulnerability scans, and employee training to ensure that all personnel are aware of cybersecurity risks and best practices. The company also employs advanced security tools and technologies, including firewalls, intrusion detection systems, and Security Information and Event Management (SIEM) tools, to monitor and protect its systems from cyber threats. To further enhance its cybersecurity posture, Duke Energy has also established a Cyber-Security Operations Centre (SOC) that operates 24/7 and is staffed with cybersecurity experts. The SOC is responsible for monitoring the company’s networks and systems for potential threats, investigating any incidents, and responding to cyber-attacks. Duke Energy’s cybersecurity program also includes regular audits and third-party assessments to ensure compliance with regulatory frameworks and standards, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the North American Electric Reliability Corporation (NERC) CIP standards (Marron, 2021). Overall, Duke Energy's cybersecurity program is a best practice for protecting critical infrastructure from cyber threats. The program demonstrates the importance of regular risk assessments, employee training, and the use of advanced security tools and technologies to mitigate cybersecurity risks and ensure the secure and reliable operation of smart grid systems.

5.2. Standard reviews

Cybersecurity standards are essential for ensuring the security and resilience of digital systems and networks (Jansen and Jeschke, 2018; NIST, 2014a; NIST, 2014b); NIST, 2014c; NESCOR, 2015; Sullivan et al., 2016; Theron and Lazari, 2018). This is especially crucial within industries like energy and DER, where critical infrastructure is at stake. Different countries have developed their own cybersecurity standards and frameworks, tailored to address the unique challenges and requirements of their respective industries. These standards often encompass broader cybersecurity guidelines applicable to DER and the energy sector as a whole. Currently, there is no comprehensive list of specific DER cybersecurity standards that have been developed by different countries. The field of DER standards is still in its infancy, and there is no single, widely-adopted standard to apply. Several countries and organizations are actively working toward securing DER systems and have published guidance related to DER cybersecurity (ENA, 2020). This indicates a growing awareness of the importance of cybersecurity in this sector. The creation of cybersecurity standards for DER systems should be specific, outcome-focused, and flexible (NIST, 2014a). These standards should avoid causing compatibility issues with international approaches, ensuring that they can be applied effectively.

The NIST Cybersecurity Framework is a widely recognized set of guidelines that provides a comprehensive approach to managing and mitigating cybersecurity risks and is relevant to critical infrastructure, including DER systems (Stouffer et al., 2014; Theron and Lazari, 2018). In South Africa, while there may not be specific standards or guidance exclusively tailored for DER systems, existing legislation, such as the Protection of Personal Information Act (POPIA) (RSA, 2013) and the Cybercrimes Act (RSA, 2021), indirectly addresses certain aspects of cybersecurity. These laws include provisions related to data protection, secure data processing, and the criminalization of cyber-related offenses. POPIA focuses on the protection of personal information and includes measures related to the secure processing and storage of such data. While its primary focus is on data privacy, its provisions can be seen as contributing to broader cybersecurity practices. The Cybercrimes Act in South Africa criminalizes a range of cyber-related offenses and provides a legal framework for prosecuting cybercriminals. This legislation is instrumental in addressing and mitigating cybersecurity threats. **Table 1** illustrates the wide range of cybersecurity standards and guidance adopted by different countries. These standards serve as valuable references for developing and enhancing cybersecurity practices in the energy sector and DER systems (ENA, 2020; NCFSA, 2015; RSA, 2021).

Table 1. Summary of relevant standards and guidance.

Source	**Document**	**Observations**
IEC 62443	Industrial Automation and Control Systems Security	• Leading standard for ICS security and network architecture. Sections include system design guidance and requirements. Not all sections are published. • The Health and Safety Executive (HSE) inspectorate guidance is based on this and vendors widely adopting. • Part 2-1 Includes mapping to ISO 27001. • Whilst not DER specific, this is useful for the industrial control components of DER.
IEC 62531	Security for information exchange in power systems	• Aimed at covering gaps in IEC 62443. • Covers low level technical controls useful for power systems.
NIST SP800-82	Guide to ICS Security	• Contains a holistic review of relevant components for cyber security. • Whilst not DER specific, serves as a good baseline for the ICS components of DER implementations.
NIST SP800-53	Security and Privacy Controls for Information Systems and Organisations	• Exhaustive list of security controls for Information Systems. • Whilst not DER specific, serves as a good base for a checklist of security principles and controls.
NIST	NIST Framework for Improving Critical Infrastructure	• Covers risk management and high level organisational processes. • More relevant for DNOs and National Grid for organisational and policy structures.
ANSSI	ANSSI Cyber Security for Industrial Control Systems	• Focus is on Industrial Control Systems. • Useful as an overview of how to assess the level of risk associated with a control system and the appropriate measures needed to secure them.
NCSC	• UK NCSC – NIS regulations Guidance to Industry (January 2018) • Security of Network and Information Systems Government response	• EU Network and Information Systems Directive from May 2018 to ensure cyber security risks managed for UK CNI or equivalent. • This is supplemented by the CAF.
ISO 27019	ISO 27002 applied to Process Control Systems in the energy industry	• Summarises IT controls to deliver cyber security and how they may be extended for process control environment for energy delivery systems. • Mainly of use to the network operators.
UK HSE-OG 0086	HSE supplementary guidance in addition to the NCSC CAF	• Not directly relevant for DER connections. • Could be used as an example of where organisations have added extra fields to supplement the CAF.
IEEE 1547	Family of standards for interconnecting DERs to distribution grids	• In the UK, these are in the form of the G98 and G99 connection codes. • Only covers electrical connection and does not contain cyber security guidelines.
NREL	DER Cyber Security Standards	• Copy of a presentation introducing the creation of DER cyber security standards. • Still in development and currently limited to basic controls. This is expected to change.
NREL	An overview of DER interconnection: Current practices and emerging solution	• Summarise the considerations, practices and emerging solutions. • Does not aim to recommend or dictate practices. • Contains generic cyber security guidelines.

Table 1. (*Continued*).

Source	Document	Observations
Sandia National Laboratories	Cyber security primer for DER vendors, Aggregators and Grid Operators	• Contains many general cyber security principles and background information.
POPIA	Protection of Personal Information (POPI) Act 4 of 2013	• Data protection law that aims to protect the personal information of individuals. • Secure processing and storage of personal data
Cybersecurity Act 19 of 2020	Cybercrimes Act 19 of 2020	• Criminalizes various cyber-related offenses, such as unauthorized access to computer systems, data breaches, cyber fraud, and cyber extortion • Legal framework for prosecuting cybercriminals and addressing cybersecurity threats

6. Discussion

South Africa has implemented key legal regulations, including the Protection of Personal Information Act (POPIA) and the Cybercrimes Act, to address cybersecurity concerns (NCFSA, 2015; RSA, 2021). These regulations are essential for protecting personal data and criminalizing unauthorized access and modification of computer material. They provide a foundation for addressing cybersecurity issues. While these regulations are valuable, they offer a relatively traditional view of cybersecurity. They may not fully encompass the complexities and challenges posed by emerging technologies like IoT and smart grids. The absence of legal cases regarding product liability in the IoT and smart grid context creates uncertainty about how courts might react in such cases. As these technologies become more widespread, legal precedents will likely be set. IoT devices generate vast amounts of data, and addressing issues related to data ownership, processing, use, and security is a significant challenge (Kobara, 2016; Pishva, 2017; Miessler, 2015; Radanliev et al., 2018). Multiple stakeholders, both commercial and public, are involved, making it crucial to establish clear guidelines and standards for data management. The duty to notify users of any loss of personal data, as stipulated in the POPIA data protection law, aligns with the principles of the EU data protection Directive 95/46/EC. This demonstrates the influence of international data protection standards on South African regulations. The rapid evolution of technology requires legal regulations to evolve as well. Policymakers and legal authorities must stay up-to-date with emerging technologies and potential cybersecurity challenges to create effective and relevant legal frameworks.

The DER cybersecurity industry is still in its early stages, and power utilities are learning through experimentation and trial and error. This approach can lead to the development of effective and efficient cybersecurity initiatives but also poses risks due to its evolving nature. Regulatory frameworks and technical standards often lag behind industry developments. As a result, the industry tends to create de facto cybersecurity frameworks and guidelines. While this approach can be suitable in some cases, it may neglect the important principle of "*security by design*" and leave infrastructure and citizens vulnerable to cyber-physical breaches. The lack of appropriate cybersecurity frameworks can lead to power utilities becoming either overly centralized or overly privatized. Striking the right balance is crucial to prevent stifled innovation, maintain control, and protect infrastructure and citizens from risks. It is paramount to strike a balance that encourages responsible innovation while adhering to security by design principles. This balance ensures that technological advancements can proceed at a reasonable pace without compromising security and resilience. As the main owner of critical infrastructure, the government plays a pivotal role in ensuring the cybersecurity of DER systems. Taking appropriate steps to establish and enforce cybersecurity standards and minimizing liability in the event of incidents is essential to safeguard the interests of citizens.

The literature review shows that the smart grid industry has yet to adopt mandatory cybersecurity standards. This means that there are no universally required guidelines or regulations for ensuring the security of smart grid technologies. Prescriptive cybersecurity standards are essential for the smart grid, given that many tech vendors in this industry are small and medium enterprises (SMEs) and startups. These standards provide clear, detailed, and enforceable requirements that can help ensure consistent cybersecurity practices. A study conducted by HP of 10 IoT devices used in smart grids revealed that these devices, on average, had 25 vulnerabilities each, totaling 250 vulnerabilities across the 10 devices (Pishva, 2017). This underscores the pressing need for robust cybersecurity measures in the smart grid sector. Addressing security issues in the smart grid cannot be the responsibility of a single vendor or manufacturer. Instead, adherence to specific cybersecurity standards must become the norm in the development of smart grid devices. This implies a collaborative approach across the industry to establish and implement standards.

Incidents like the cyberattack on the Ukraine power grid underscore the critical need for strong collaboration of various stakeholders to develop a comprehensive cybersecurity measure in smart grids. This includes power utilities, manufacturers, government authorities, and other actors in the smart grid ecosystem. These incidents serve as important lessons in the protection of critical infrastructure. To date, there appears to be no appropriately defined strategy for smart grids in South Africa. The government can play a central role in defining and implementing a harmonized cybersecurity framework that encompasses all relevant stakeholders. This framework should integrate cybersecurity standards and a robust risk management approach. he government's role in this context should be that of a coordinator. By bringing together all stakeholders and facilitating the creation of a cohesive cybersecurity framework, the government can ensure a unified and effective approach to cybersecurity in the smart grid. While there may be sufficient regulation in place regarding data protection, handling extensive data and securing consent, especially with the proliferation of DER devices and smart grid technologies, can pose challenges. Ensuring that data handling is compliant with privacy and data protection laws is a critical aspect of cybersecurity in this context.

While there is a wide range of communication protocols for power systems equipment, there are relatively few standardized protocols for DER equipment. This makes the choice of communication protocols a critical consideration in the integration of DER systems into smart grids. Some commonly used communication protocols for DER equipment include IEEE 1815 (Distributed Network Protocol 3 or DNP3), SunSpec Modbus, and IEEE 2030.5 (Smart Energy Profile or SEP 2.0)

(Martins et al., 2018; Sadan and Renz, 2020). These protocols facilitate communication between DER equipment and the broader smart grid infrastructure. IEEE 1547-2018, which provides guidelines for DER interconnection, may support other proprietary protocols if mutually agreed upon by the electric power system and DER operator. However, it's important to note that IEEE 1547–2018 does not specifically address cybersecurity (Sadan and Renz, 2020). The implementation of secure communication networks is vital for protecting sensitive data transmitted within smart grid systems. Secure communication is critical to ensure the integrity and confidentiality of data exchanged between DER equipment and the broader power grid. Different regulations and standards, such as NRS 097-2-1 and SAGCRPP, specify requirements for DER systems, including communication capabilities (NERSA, 2017, 2019). These regulations may mandate the use of specific communication protocols and monitoring devices, especially for larger DER systems. In some cases, regulations like SAGCRPP require the installation of power quality monitoring devices for DER systems larger than a certain capacity. These devices ensure compliance with power quality standards and monitor aspects like flicker, harmonics, and voltage unbalance.

Finally, Compliance with cybersecurity standards in Distributed Energy Resources (DER) systems should be incorporated from the earliest stages of application or code development. This security by design approach ensures that cybersecurity is an integral part of all products and technologies within the smart grid ecosystem. Third-party actors, including tech vendors, manufacturers, and service providers, should be subject to compliance testing and certification. This process should be conducted annually to verify that these entities are aligning with the established cybersecurity guidelines and standards. The compliance testing and certification process should be carried out by independent third parties, such as internal or external auditors. This independent assessment ensures objectivity and credibility in evaluating adherence to cybersecurity standards. The results of compliance testing and certification provide a reasonable level of assurance to regulatory bodies that key actors in the smart grid ecosystem are following cybersecurity guidelines and standards. This is essential for maintaining the security and integrity of the smart grid.

7. Recommendations and future directions

The recommendations for a robust cybersecurity framework in DER systems include implementing the following:

Secure communication: Implement secure communication protocols and networks for DER systems. This includes the use of standardized, secure communication protocols like DNP3 or SunSpec Modbus. Secure communication ensures the integrity and confidentiality of data exchanged between DER equipment and the power grid.

Data encryption: Apply data encryption to protect sensitive information. Data encryption ensures that data is securely transmitted and stored, making it difficult for unauthorized parties to access or tamper with data in transit or at rest.

Authentication: Implement robust authentication mechanisms to ensure that only authorized users or devices can access and control DER systems. Strong authentication helps prevent unauthorized access and unauthorized control of DER equipment.

Access control: Implement access control measures to restrict access to critical systems and data. Limiting access to authorized personnel and devices helps reduce the attack surface and enhance security.

Incident response plan: Develop and maintain a well-defined incident response plan. This plan should outline procedures for detecting, mitigating, and recovering from security incidents, ensuring a swift and effective response to threats.

Regular updates and training: Keep security measures up to date with regular updates and patches. Additionally, provide training and awareness programs for personnel involved in the operation and maintenance of DER systems to ensure they are well-informed about cybersecurity best practices.

Compliance with regulations: Ensure compliance with relevant regulations and standards specific to DER systems and the energy sector. Adherence to regulatory requirements helps maintain legal and security standards.

Network segmentation: Implement network segmentation to divide the network into separate, isolated segments. This practice helps contain potential security breaches, preventing lateral movement of attackers within the network. By segmenting the network, you can limit the impact of a security incident and protect critical assets.

Security awareness and training: Provide ongoing security awareness and training programs for all personnel involved in the operation and maintenance of DER systems. Well-informed and trained employees are the first line of defense against cybersecurity threats, as they can recognize and respond to potential risks effectively.

Vendor security evaluation: Conduct thorough security evaluations of vendors and third-party service providers. Assess their cybersecurity practices and ensure that they align with your organization’s security standards and requirements. Vendor security evaluations help reduce supply chain risks and vulnerabilities.

Collaboration and information sharing: Foster collaboration and information sharing within the industry and with relevant authorities. Sharing threat intelligence, best practices, and lessons learned with peers and organizations can enhance collective cybersecurity efforts. Collaborative initiatives can provide valuable insights and early warning about emerging threats.

These recommendations outline a robust cybersecurity posture for DER deployments in DER systems, requiring tailored measures and regular updates to address unique risks and characteristics.

8. Conclusion

The integration of DERs into the energy system necessitates robust cybersecurity measures to ensure the security and integrity of interconnected smart grids. Cybersecurity is foundational for safeguarding critical infrastructure and maintaining reliable energy distribution. Establishing comprehensive regulatory standards is vital. These standards provide a framework for cybersecurity practices, ensuring that all stakeholders in the energy sector, including DER operators, adhere to best practices and security protocols. This paper provides a review of literature on cybersecurity for DERs systems. This information can be used as a guide by different stakeholders involved in integration of DERs into the power grid such as power utilities, manufacturers and government bodies.

Funding: This research was funded by the South African National Energy Development Institute (SANEDI) grant number: PA-000225, project reference no. PA-000225-TO-04-UJ-VF, theme: POWER GRID DIGITALIZATION. Opinions and conclusions are those of the authors and are not necessarily attributable to SANEDI. The work is supported and part of collaborative research at the Centre of Applied Research and Innovation in the Built Environment (CARINBE). The APC was funded by the University of Johannesburg.

Conflict of interest: The authors declare no conflict of interest.

References

Calitz, J. & Wright, J., 2021. Statistics of utility-scale power generation in South Africa in 2020, South Africa: http://hdl.handle.net/10204/11865.

Dzobo, O., Malila, B. & Sithole, L., 2011. Proposed framework for blockchain technology in a decentralised energy network. Protection and Control of Modern Power Systems, 6(3), pp. 1 - 11.

ENA, 2020. Distributed Energy Resources – Cyber Security Connection Guidance. [Online] Available at: https://www.energynetworks.org/publications/distributed-energy-resources-(der)-cyber-security-connection-guidance [Accessed 21 July 2023].

EPRI, 2020. CoNEd and Duke Energy Evaluate Cyber Security with Technical Assessment Methodology. [Online] Available at: https://www.epri. com/research/products/3002017786 [Accessed 20 July 2023].

EUAC, 2012. Appropriate security measures for smart grids, 2012. [Online] Available at: https://www.enisa.europa.eu/ publications/appropriate-security-measures-for-smart grids [Accessed 20 July 2023].

EUAC, 2013. Smart grid threat landscape and good practice guide. [Online] Available at: https://www.enisa.europa. eu/publications/smart-grid-threat-landscape-and-good-practice-guide [Accessed 20 July 2023].

Faquir, D., Nestoras, C., Kalopoulou, O. & Maglaras, L., 2021. Cybersecurity in smart grids, challenges and solutions. AIMS Electronics and Electrical Engineering, 5(1), p. 24–37.

Gunduz, M. Z. & Das, R., 2020. Cyber-security on smart grid: Threats and potential solutions. Computer Networks, Volume 169(107094), p. 1–17.

He, H, Maple, C, Watson, T, Tiwari, A, Mehnen, J, Jin, Y & Gabrys, B, 2016. The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence. Vancouver, Canada, 24 – 29 July 2016, IEEE Congress on Evolutionary Computation.

Jansen, C. & Jeschke, S., 2018. Mitigating risks of digitalization through managed industrial security services. AI and Society, 33(2), pp. 163-173.

Kitchenham, B. & Charters, S., 2007. Guidelines for performing systematic literature reviews in software engineering, Keele University and Durham University Joint Report: Technical Report EBSE 2007-001.

Kobara, K., 2016. Cyber physical security for industrial control systems and IoT. IEICE TRANSACTIONS on Information and Systems, E99-D (4), pp. 787-795.

Langer, L., Smith, P. & Hutle, M., 2015. Smart grid cybersecurity risk assessment. Vienna, Austria, 2015 International Symposium on Smart Electric Distribution Systems and Technologies (IEEE).

Marron, J., 2021. Mapping of NIST Cybersecurity Framework v1.1 to NERC CIP Reliability Standards, National Institute of Standards and Technology. [Online] Available at: https://doi.org/10.18434/mds2-2348 [Accessed 21 July 2023].

Martins, J., Gomes, V. & T, M., 2018. On the use of IEC 61850-90-7 for smart inverters integration. 9th International Conference on Intelligent Systems 2018, 25 - 27 September, pp. 722-726.

Miessler, D., 2015. Securing the internet of things: Mapping attack surface areas using the OWASP IoT top 10. San Fransisco, USA, RSAConference2015.

Mishra, S, Anderson, K, Miller, B, Boyer, K & Warren, A, 2020. Microgrid resilience: A holistic approach for assessing threats, identifying vulnerabilities, and designing corresponding mitigation strategies. Applied Energy, Volume 264(C).

NCFSA, 2015. Government Gazette. State Security Agency, National Cybersecurity Framework for South Africa, Government Gazette, [Online] Available at: https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf [Accessed 20 July 2023].

NERSA, 2017. NRS 097-2-1: 2017 Small-scale embedded generation Section 1: Utility Interface, South Africa: Eskom.

NERSA, 2019. Grid Connection for Renewable Power Plants (RPPs) connected to the Electricity Transmission System (TS) or Distribution System (DS) in South Africa: Version 3.0, South Africa: Eskom.

NESCOR, 2015. Electric Sector Failure Scenarios and Impact Analyses - Version 3.0, California, USA: EPRI.

NIST, 2014a. Guidelines for Smart Grid Cybersecurity: Vol.1, Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements., USA: NIST.

NIST, 2014b. Guidelines for Smart Grid Cyber Security: Vol.2, Privacy and the Smart Grid., USA: NIST.

NIST, 2014c. Guidelines for Smart Grid Cybersecurity: Vol.3, Supportive Analyses and References., USA: NIST Interagency/Internal Report (NISTIR) - 7628 Rev 1, https://doi.org/10.6028/NIST.IR.7628r1.

NIST, 2018. Framework for Improving Critical Infrastructure Cybersecurity, April 16, 2018. [Online] Available at: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf [Accessed 20 July 2023].

Notton, G, Nivet, M.L, Voyant, C, Paoli, C, Darras, C, Motte, F & Fouilloy, A, 2018. Intermittent and stochastic character of renewable energy sources: Consequences, cost of intermittence and benefit of forecasting. Renewable Sustainable Energy Reviews, Volume 87, p. 96–105.

Owusu-Mante, S., 2020. South Africa’s 2019 IRP renewable energy targets. [Online] Available at: https://www.climatepolicylab.org/communityvoices/2020/5/13/south-africas-2019-irp-renewable-energy-targets [Accessed 20 July 2023].

Pishva, D., 2017. Internet of Things: Security and privacy issues and possible solution. PyeongChang, Korea (South), 2017 19th international conference on advanced communication technology (ICACT)., pp. 797-808.

Radanliev, P, De Roure, D.C, Nicolescu, R, Huth, M, Montalvo, R.M, Cannady, S & Burnap, P, 2018. Future developments in cyber risk assessment for the internet of things. Computers in Industry, Volume 102, pp. 14-22.

RSA, 2013. Protection of Personal Information (POPI) Act 4 of 2013. [Online] Available at: https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf [Accessed 20 July 2023].

RSA, 2021. Cybercrimes Act 19 of 2020. [Online] Available at: https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf [Accessed 20 July 2023].

Sadan, N. & Renz, B., 2020. New DER communications platform enables DERMS and conforms with IEEE 1547-2018 requirements. 2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), 12 - 15 Oct, pp. 1 -5.

Stouffer, K, Lightman, S, Pillitteri, V, Abrams, M & Adam, H, 2014. NIST special publication 800-82, revision 2: Guide to industrial control systems (ICS) security, Maryland, United States: National Institute of Standards and Technology.

Sullivan, D., Luiijf, E. & Colbert, E. J. M., 2016. Components of Industrial Control Systems. In: Cyber-security of SCADA and Other Industrial Control Systems. AG Switzerland: Springer International Publishing.

Theron, P. & Lazari, A., 2018. The IACS Cybersecurity Certification Framework (ICCF). Lessons from the 2017 study of the state of the art, Luxembourg: Publications Office of the European Union.

Turner, H. A., White, J., Camelio, J. & Williams, C. B., 2015. Bad parts: are our manufacturing systems at risk 615 of silent cyberattacks? IEEE Security and Privacy, 13(3), pp. 40 - 47.

USA, 2021. United States of America government, Cyber-Attack Against Ukrainian Critical Infrastructure. [Online] Available at: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 [Accessed 20 August 2023].

Wu, D, Ren, A, Zhang, W, Fan, F, Liu, P, Fu, X & Terpenny, J, 2018. Cybersecurity for digital manufacturing. Journal of Manufacturing Systems, Volume 48, pp. 3 - 12.