World Journal of Advanced Engineering Technology and Sciences

eISSN: 2582-8266

Cross Ref DOI: 10.30574/wjaets

Journal homepage: https://wjaets.com/

(Research Article)

Implementation of Zero Trust Architecture for Cybersecurity in Distributed Energy Resources (DERs): A Systematic Review

Justine Chilenovu Ogborigbo [1, *] and Julius Nani Gadah [2]

[1] *Power System and Electrical Engineering, Department of Electrical and Electronics Engineering, University of Port Harcourt, Port Harcourt, Rivers State, Nigeria.*

[2] *Information Technology, Department of Supply Chain and Information System, Kwame Nkrumah University of Science and Technology, Kumasi, Ashanti Region, Ghana.*

World Journal of Advanced Engineering Technology and Sciences, 2021, 02(02), 104-132

Publication history: Received on 31 January 2021; revised on 16 Februay 2021; accepted on 21 November 2021

Article DOI: https://doi.org/10.30574/wjaets.2021.2.2.0021

Abstract

The high growth rate of the distributed energy resources (DERs) comprising solar photovoltaics, wind, and battery storage systems (BESS) has essentially altered the classically centralized power grid into a more diverse classification of distributed assets. It has brought with it some unprecedented computer security challenges that cannot be solved in a proper manner via the conventions of the perimeter-based computer security. Zero Trust Architecture (ZTA) is another shift in paradigm, or a paradigmatic shift in cybersecurity terms, as there is an implicit trust provided by location in the network shifting to explicit verification of each transaction and each access request. The study proposes a holistic system of realizing Zero Trust rules specifically adapted to the distributed energy resources setting that considers policy-based access control methods, identity credentialing procedures, micro-segmentation approach, and constant surveillance aspects. This research paper addresses the implementation of Zero Trust concepts with the existing SCADA installations, compliance models such as NIST 800-207 and ISO 27001, the field implementation of BESS and its associated Zero Trust concepts. By acting upon the results of the systematic study of existing vulnerabilities of cybersecurity in the DER ecosystem and the assessment of the Zero Trust implementation plans, this study proves that Zero Trust Architecture can efficiently improve the security status of distributed energy infrastructure without reducing its operating efficiency and adhering to existing regulatory frameworks. The suggested structure will resolve the most significant security gaps in the distributed energy systems and introduce flexible and adaptive security policies that can be changed with the dynamism of contemporary energy infrastructure.

Keywords: Zero Trust Architecture; Distributed Energy Resources; Micro-Segmentation; Energy Cybersecurity; Access Control; NIST 800-207; Policy-Driven Security; Identity Verification; Continuous Monitoring

1. Introduction

The evolution of the electrical grid from a centralized generation and distribution model to a distributed, interconnected network of diverse energy resources has created unprecedented opportunities for enhanced energy security, environmental sustainability, and economic efficiency. National Institute of Standards and Technology (2020) explains that the introduction of distributed energy sources such as solar photovoltaic systems, wind turbines, battery energy storage systems (BESS) and demand response capabilities has overturned the very foundation of the cybersecurity of the electrical infrastructure. In their study showing pervasive and zero-trust as better ways of cyber protection, Roman (2021) notes that existing legacy models in perimeter-based frameworks of cyber protection are insufficient to secure the dynamic, complex, and geographically distributed processes of the contemporary distributed energy resources. Unlike the traditional, centralized power production plants, distributed energy assets span the accolade of domains,

* Corresponding author: Justine Chilenovu Ogborigbo

differ widely in communication protocols, and interact with many actors, such as utility power plant operators, aggregators, and ultimate consumers. The very nature of such systems has resulted in numerous attack vectors which cannot be properly countered by using traditional cybersecurity methods.

Zero Trust Architecture is a paradigm of a change in cybersecurity philosophy as it introduces a transition to eliminate the old principle of "trust but verify" and shift to yet another one a principle of never trust, always verify. As shown by Ajiboye et al. (2021) in their review of Zero Trust architecture trends and developments in energy systems, this security paradigm does not entail any implicit trust grounded on the location of the network or the identity of users, making it imperative to ensure the continual verification of all transactions, devices, and users trying to access resources of the system. Besides banishing implicit assumptions of trust, Zero Trust Architecture applies the concept of least privilege access to users and devices that provide access accordingly to only the minimum requirements to support the available functions that they are authorized to use. The study by Ritter et al. (2021) on Zero Trust architectures applied to the energy sector also takes note of the fact that this security mechanism is especially applicable to distributed energy resources amid their high level of heterogeneity, geographic distribution, and connectivity to legacy SCADA systems that were not initially designed with the latest threats to cybersecurity.

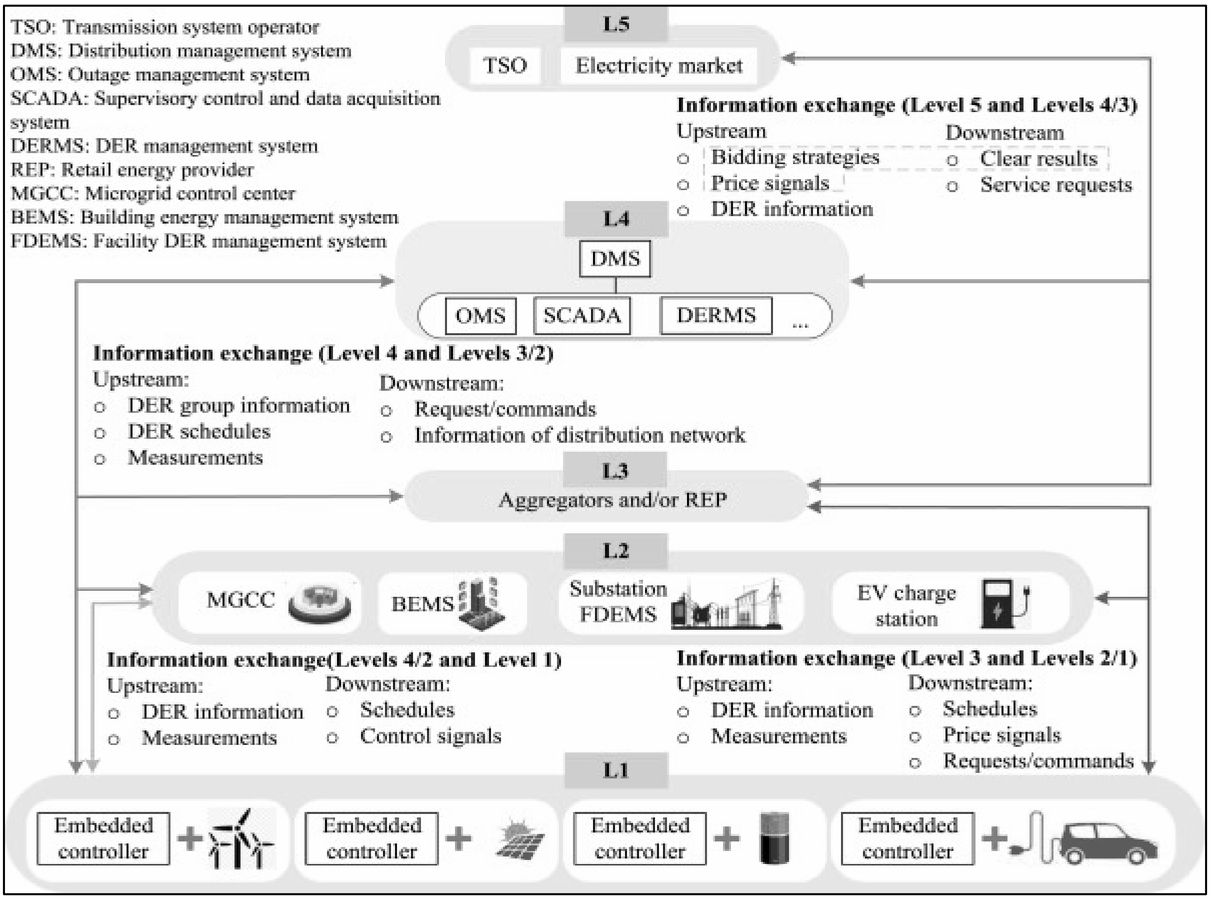

Figure 1 Zero Trust Architecture for Cybersecurity in Distributed Energy Resources Chen et al., 2020

The cybersecurity challenges facing distributed energy resources are multifaceted and evolving rapidly as these systems become more interconnected and digitized. Newhouse and Scarfone (2020) state that critical infrastructure security necessitates integrative security models that do not only focus on external threats but also include insider threats, areas of vulnerabilities of the supply chain, and the growing complexity of the nation-state-affiliated adversaries targeting energy infrastructure. Chaudhry and Hydros (2021) in their work on policy-driven micro-segmentation in smart grids show that the policies underlying the classical segmentation methods of the network are no longer viable when defending distributed energy resources considering the dynamicity of such systems and the necessity to have data shared in real-time among a variety of actors.

Nevertheless, the implementation of Zero Trust Architecture in the context of distributed energy is associated with severe obstacles, which are related to the exceedingly high complexity of numerous interrelated systems and the dire necessity of ensuring the continuity of operations in real time that is typical of contemporary energy infrastructure. Roman (2021) argues that this poses very crucial issues in cybersecurity relating to energy since any erroneous security decries or access refusal can lead to disastrous operational hiccups, such as power cuts, damage to equipment, cascading failures in interconnected grid systems, and so on. Besides the operational issues, energy organizations need to deal with difficult regulatory demands, the integration of legacy systems, and interoperability requirements associated with a wide range of stakeholder systems in the framework of extensive Zero Trust implementations (Ajiboye et al., 2021).

1.1. Research motivation and significance for distributed energy cybersecurity frameworks

The fully distributed and networked design of modern energy systems, especially as they are implemented with high penetrations of distributed energy resources, makes an even more enticing target to any potential adversary who would want to maliciously perform cyber hacks to disrupt critical functions in their energy systems. As per recent research outputs on energy cybersecurity, contemporary DER system has unique multi-mesh structured natures, service, multi-tenanted operation, cross-domain integrations, multi stakeholder independent administrative infrastructure issues that are more definitely susceptible as well as subject to advanced threats of cybersecurity (Ritter et al., 2021). In a literature survey of distributed energy security issues, Chaudhry, and Hydro's (2021) describe how energy systems infrastructure is configured through a three-tier architecture of infrastructure elements that are mutually relying on one another namely, physical assets, communication platforms, and operational applications, with each of these layers being vulnerable in various ways through the programming errors, configuration error, and even malicious intent of attackers.

Around 2015-2016, advanced cyber adversaries showed their potential of breaching energy infrastructure system by delivering purposeful attacks against Ukrainian power distribution system that led to extensive outages across hundreds of thousands of affected customers (Liang et al., 2017). Farwell and Rohozinski (2011) posit that energy infrastructure systems are becoming more lucrative targets to cyber criminals and nation-state actors because they are high value targets to the economy and could serve as platforms of subsequent attacks on other related critical infrastructure systems that are interconnected. Besides all external threats, a complete visibility and control of energy assets spread out on a large geographical scale makes it a major issue as energy system operators need to be aware of situations in widely distributed assets and nee to ensure cybersecurity compliance (Bekara, 2014).

The study combines the challenges and problems that have hindered the further growth of improved Zero Trust structures in distributed energy resources even infrastructures. It is supposed to attract the attention of well-respected researchers to the potential solutions to the development of complete cybersecurity systems by unifying the latest disparate research works to shed light on ways of securing wide-spread distributed energy services and resources (Bekara, 2014). Bertino and Islam (2017) present their study on botnets and Internet of Things security and thus indicate that efficient cybersecurity frameworks should not only cover technical vulnerability, but also organizational, procedural, and legal operations of distributed energy resources. In addition to defining the required Zero Trust features of distributed energy resources, the professional implications of this research are its recommendations towards integrating the designed solution with SCADA systems already implemented, aligning them with present regulatory frameworks, and practical considerations relevant to field implementation of battery energy storage systems (BESS).

1.2. Research boundaries and limitations in zero trust energy implementations

Among the available solutions to cybersecurity of distributed energy resources, comprehensive all-purpose systems with a Zero Trust approach that consider more than one aspect of energy infrastructure security and unite various security tools are considered in the current paper. Some researchers have concentrated on specific aspects of Zero Trust or a particular kind of cyber threat aimed to decrease the number of false-positive security alerts in operational infrastructures of energy companies (see Bertino and Islam, 2017). Caralli et al. (2007), on the one hand, tested various denial-of-service detection methods specifically adapted to control systems in industry, and Banerjee et al. (2011) tried to make cybersecurity sensors better quality to serve more complicated intrusions against the energy management systems.

Since the objective of operational environment is to protect distributed energy resources, all the special considerations are made regarding the recent cybersecurity research publications that have been released within the last few years to leverage not only advanced but also up-to-date Zero Trust implementation techniques. Continuous monitoring/threat prevention is a relatively new capability of the traditional intrusion detection systems that can be installed in the energy environment, which is why the number of published works that cover Zero Trust application in a distributed energy setting in detail is very limited (Cleveland, 2008). However, this paper takes cognizance of all the recent research on the intrusion prevention systems and Zero Trust security frameworks because these systems can be complemented by the inclusion of the holistic principles of the Zero Trust architecture and policy-driven management of access controls (Colwill, 2009).

These research boundaries and limitations constrain this study to focus on the current state-of-the-art Zero Trust implementations while acknowledging the rapidly evolving nature of both cybersecurity threats and energy system architectures. According to De Craemer et al. (2014), distributed energy resource deployment is a relatively recent phenomenon in the United States energy sector, therefore there are limited practical and experimental Zero Trust implementations developed specifically for real-world energy operational environments. In their research on energy cybersecurity challenges, Deng et al. (2017) note that regardless of current boundaries and limitations in the existing literature, this research investigation is guided by the following two fundamental research questions:

- What specific criteria and comprehensive requirements should a Zero Trust Architecture framework meet to be effectively deployed in distributed energy resource operational environments?
- Which implementation methods and cybersecurity techniques can effectively satisfy these comprehensive Zero Trust requirements while maintaining operational efficiency and regulatory compliance?

2. Zero Trust Architecture taxonomy for distributed energy resource protection systems

Cyber-attacks on distributed energy resources may occur as external attacks, referred to as insider attacks, or internal where the unauthorized user tries to access the non-authorized access privileges in the network of the energy systems. As shown in the thorough survey of smart grid technologies by Fang et al. (2012) the intrusion detection and prevention in distributed energy resources means the process of decreasing or eliminating the risks of intrusion into the operational technology, computer, communication systems, and networks, controlling possible interfering or malicious activities, interception of data content, introduction of viruses or malware and so on. Farwell and Rohozinski (2011) explain that attacks on energy infrastructure are generally implemented in different sets known as incidents, and most of the incidents are malicious in nature; that is, on critical infrastructure, but some may be because of accidental misconfigurations, failures, or human error as opposed to intended cyber-attack.

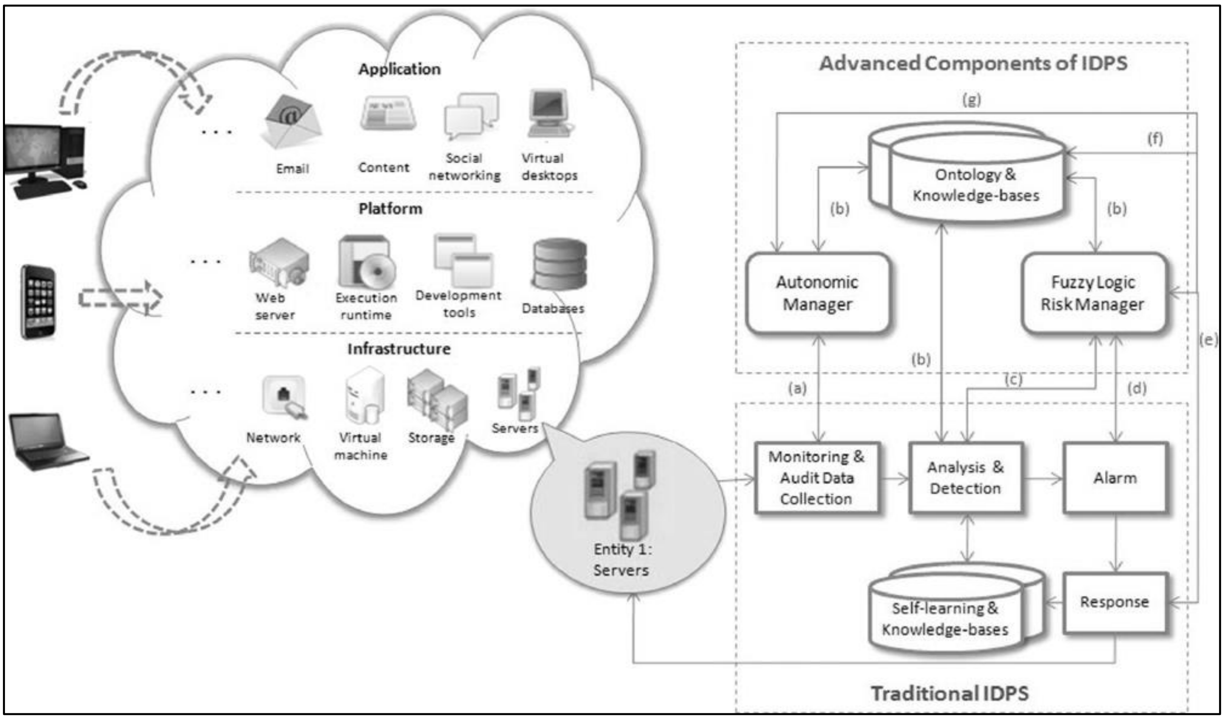

Figure 2 A comprehensive Zero Trust Architecture framework implemented for distributed energy resource protection within modern grid computing environments

Zero Trust Architecture application of distributed energy resources is a holistic cybersecurity approach that switches to zero trust and looks upon all entities with the balance to trust with a balance to mistrust with no implied trust. Forrester Research (2010) has shown that the Zero Trust based models do away with the notion of trusted internal and untrusted external networks and treats all network traffic as a potential hostile attack regardless of where it exists or where it comes from within the distributed energy infrastructure. Burns et al. define Zero Trust implementations as having the opposite approach to that of traditional perimeter-based security models, whereby the fundamental feature requires explicit verification of all access requests, least privilege access is applied, and all activities and communications on the system are continuously monitored (Burns et al., 1992).

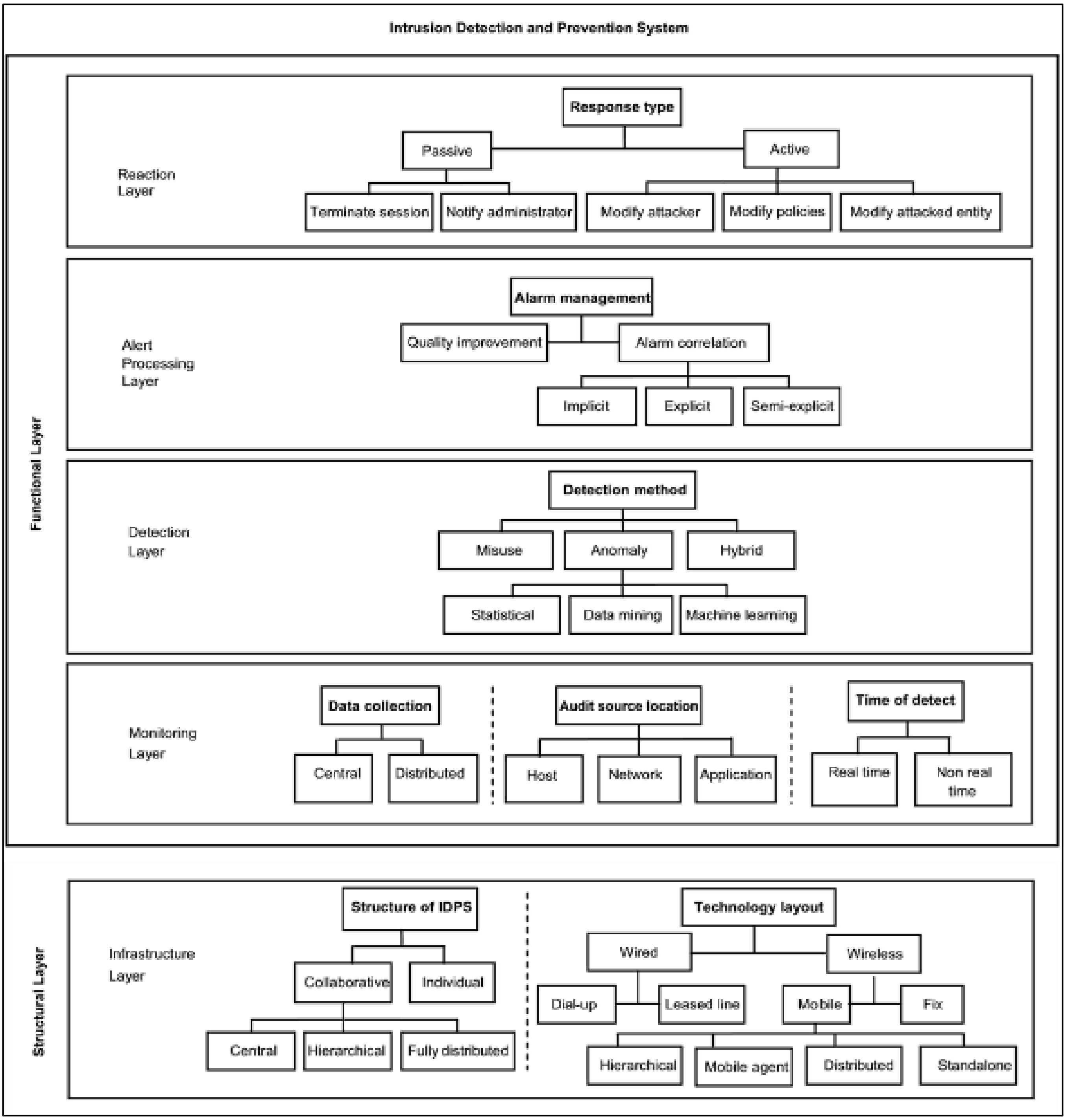

Figure 3 Comprehensive high-level taxonomy structure of Zero Trust Architecture frameworks specifically designed for distributed energy resource protection systems

The Zero Trust model is completely different in terms of paradigm shift and necessitates trust verification of every access request and constant network monitoring of all traffic, behaviors of users and communications of devices. Due to the traditionally high rates of false positives caused by traditional forms of anomaly detection systems installed in the context of energy, Zero Trust implementations may end up misclassifying legitimate operations into being potentially malicious ones and acting on these identified operations by implementing restrictions to access that may be interruptive to the operations of the energy systems (Kumar et al., 2021).

2.1. Functional layer of zero trust implementation in energy infrastructure systems

A distributed energy resources security systems have four core functions, as it is shown in the Zero Trust taxonomy framework, it is monitoring, detecting, analyzing, and responding to unauthorized operations aspects with the continuity of operations and stability of the grid. The example of the research on cyber-physical security testbeds (Hahn et al., 2013) shows that the implementation of the Zero Trust dodges the intrusion by examining the gathered data through various sources such as SCADA systems, smart meters, communication networks, and distributed energy assets. Hassan (2019) states that monitored environment of distributed energy resources may be done at the network-based, host-based, or application-based levels showing different visibility and control of system activities, and potential security threats.

A Zero Trust is a system which detects possible cyber-attacks by means of constant analysis of the data that was gathered due to various sources within the distributed energy infrastructure. Mo et al. (2012) state that the three different domains can be classed in an environment of monitored operation within energy systems: network-based monitoring system, host-based monitoring, and application-based monitoring system:

- **Network-based Zero Trust monitoring systems for distributed energy infrastructure:** These systems continuously monitor network traffic patterns across energy network segments or specific operational technology devices while analysing communication protocols and application-layer activities to identify suspicious behavioral patterns that may indicate cyber threats (NIST Framework, 2018).
- **Host-based Zero Trust monitoring systems for energy operational technology:** According to Patel et al. (2013), these systems monitor all or selected portions of the dynamic operational behavior and current security state of individual energy management computer systems. Like how network-based systems dynamically inspect communication packets, host-based systems continuously monitor which operational programs access specific energy system resources and identify potentially unauthorized activities.
- **Application-based Zero Trust monitoring systems for energy management platforms:** These specialized systems concentrate on security events that occur within specific energy management applications by analysing application log files, measuring system performance metrics, and monitoring user interaction patterns within critical energy operational platforms (Rahimi and Ipakchi, 2010).

Network-based Zero Trust monitoring (NZTM) solutions constantly inspect network traffic in the network segments or devices that belong to the distributed energy infrastructure and analyze the network and application protocol traffic to detect malicious patterns or unauthorized communications. Humayed et al. (2017) show that these systems have the capability of identifying anomalous behavior within the communication protocols of distributed energy resources such as DNP3 IEC 61850 and Modbus communication protocols indicative of cyber-attacks on systems or compromised systems.

Host based Zero Trust monitoring (HZTM) is a constant, or selective, watchdog over all or a part of the active behavior/operational condition of single-distributed energy resource systems specifically solar inverters, wind turbine controllers, battery management systems, and energy storage elements. According to research by Ralston et al. (2007) on cyber security risk assessment of SCADA and DCS networks, unauthorized execution of programs, configuration modifications or malicious code insertions that a network-based software could fail to detect can be detected by host-based monitoring because network-based system could fail to detect them based on encrypted communication or inside system operation.

The audit data collection in the energy environment may be applied based on distributed implementation schemes that collect security information across various locations or sources of operation technology, or via centralized scheme that collect security data over single integrated sources. Based on a recent study on energy cybersecurity, the methods of detection of threats in Zero Trust systems have been identified and categorized into three broad groups: The signature-based detection, anomaly-based detection, and the hybrid model based on their ability to integrate the strengths of both the former two categories (Burns et al., 1992):

- **Signature-based detection systems for energy infrastructure protection:** This comprehensive method utilizes specifically known patterns of unauthorized cybersecurity behaviors, called threat signatures, to predict and detect subsequent similar attack attempts against distributed energy resource systems and operational technology infrastructure.

- **Anomaly-based detection systems for energy operational monitoring:** These systems are modelled to detect unusual patterns of operations of energy infrastructure systems. As it is stated by Liang et al. (2017), Zero Trust systems create detailed baselines of regular operational use profiles, and all the activity that is significantly different compared to the predetermined patterns of normal behaviour is considered as a potential malicious security event that should be promptly investigated and followed with corresponding response measures.
- **Hybrid detection systems combining signature and anomaly-based approaches:** This highly integrated solution has specifically been devised to strengthen the complete cyber security functionality of the protection system of energy infrastructures by integrating the strength of signature-based detecting of threats with the highly complex threat identifying systems of anomaly-based behavioural analysis systems.

Advanced threat management in Zero Trust energy implementations can be categorized into two primary methodological approaches according to recent cybersecurity research (Liu et al., 2011):

- **Security alert quality improvement methodologies for energy infrastructure protection:** This comprehensive approach attempts to improve the overall quality and actionability of security alerts by incorporating additional contextual information, such as vulnerability assessment reports, threat intelligence feeds, and operational context data specific to energy infrastructure environments.
- **Advanced security alert correlation systems for distributed energy resource protection:** This advanced technique traces more aspirational cybersecurity plans by trying to rebuild high-level safety events with a mixture of low-level alerts over distributed scientific and engineering branches. McLaughlin et al. (2016) reveal that Zero Trust frameworks might produce numerous and possibly related security incidents that need systematic consideration in addition to synchronized response activities when there are advanced cyber-attacks on energy systems.

As Zero Trust systems can take active responses to identified cyber intrusions, they can make dynamic changes to energy system security policies, network access controls or in certain cases, temporarily isolate systems where an intrusion has occurred to limit the lateral spread of the cyber intrusion. Zero Trust systems in certain operation conditions have the capability of automatically directing network security devices to reconfigure themselves to block certain forms of malicious traffic or even divert an untoward traffic into isolated segments of the network to be evaluated within an adequate level of detail. Department of Energy (2017) states that Zero Trust implementations can adjust user access control policy or add another authentication procedure temporarily as cyber-attacks are identified and analysed within energy infrastructure systems.

2.2. Structural layer of distributed energy resource zero trust architecture frameworks

Referring to the mentioned above holistic taxonomy framework, the setting of the implementation technology architecture of Zero Trust systems is strategically placed in the section of the infrastructure protection layer of energy cybersecurity systems. Technology deployment approach is markedly overlooked by cybersecurity specialists, according to Stouffer et al. (2011), however, since this feature is instrumental in the successful implementation of such elements in an atmosphere of distributed energy resources, sufficient research is needed to achieve it based on the review and study of implementation best practices.

Two main categories of communication infrastructure connectivity support Zero Trust implementations: the traditional wired connections based on the use of the switches telephone network or some leased lines, and wireless communication systems offer flexibility of connectivity in situations with an unsatisfactorily high-level distribution of energy assets. Rose et al. (2020) indicate that, within the framework of wired energy networks, specific peculiarities of the traffic behavioural patterns and the topology level characteristics may be efficiently utilized in grid intrusion detection and a thorough adoption of Zero Trust security solutions throughout distributed energy infrastructure systems.

Wireless distributed energy networks can be defined as an advanced crop of interconnected energy resources that configure, network, and manage themselves without the help needed by centralized management infrastructure or old-fashioned network administration systems. As per recent studies on applications of energy cybersecurity, there are a number of different types or classifications of wireless network Zero Trust applications (National Institute of Standards and Technology, 2020)

- **Stand-alone Zero Trust implementations:** These systems identify cyber intrusions by operating independently on each distributed energy asset without requiring coordination with other security systems, providing localized protection while maintaining operational autonomy.
- **Distributed Zero Trust architectures:** Each energy asset participates collaboratively in detecting cyber intrusions and responds through coordination with centralized Zero Trust management agents that provide enterprise-wide security orchestration and incident response capabilities.
- **Hierarchical Zero Trust implementations:** These systems are deployed across multi-layered energy networks that are organized into operational clusters where designated cluster coordinators are responsible for managing security policies and incident response for their respective local energy assets and infrastructure components.
- **Mobile agent-based Zero Trust systems:** These advanced implementations utilize intelligent software agents that can dynamically move throughout large energy networks with specific cybersecurity tasks, enabling flexible security coverage and adaptive threat response capabilities across geographically distributed energy infrastructure.

The architecture of comprehensive implementation of Zero Trust is founded on the two major organizational frameworks, individual asset security or enterprise-wide security cooperation. A single Zero Trust solution of protection systems designed to provide energy infrastructure protection is usually accomplished by placing security features into the running entity of operations, programmable logic controller, energy management systems, or even advanced metering infrastructure elements.

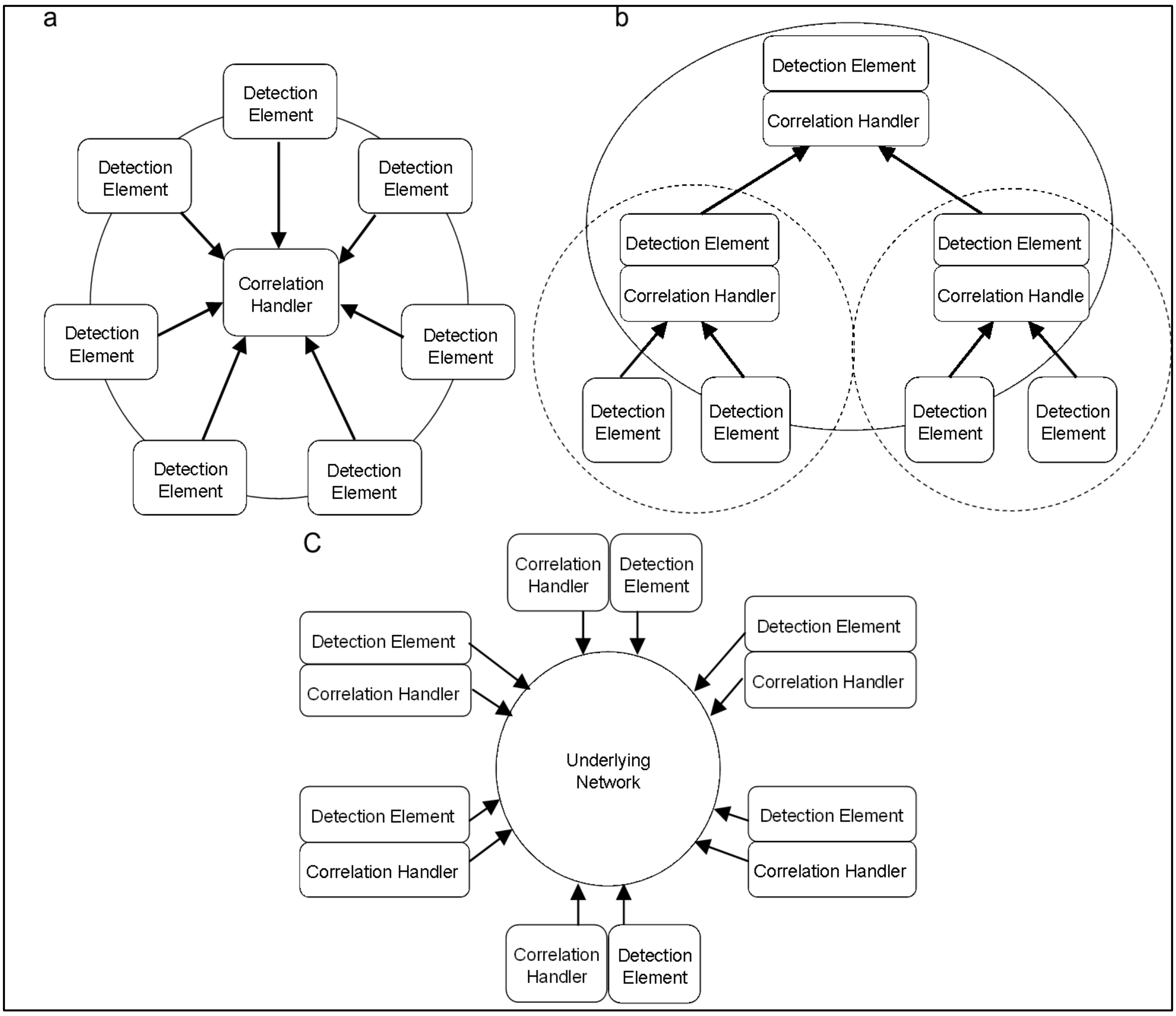

Figure 4 Different management structures of collaborative Zero Trust systems specifically designed for distributed energy resource protection: (a) Centralized coordination, (b) Hierarchical management, and (c) Fully distributed architecture

A cooperative Zero Trust architecture is a composition of multiple security systems that have been deployed throughout power grids where each component individually reports and discusses with other security components to implement a complete perimeter design of intrusion security. Newhouse and Scarfone (2020) explain that in every Zero Trust implementation, two functional components are incorporated, which are the threat detection elements and security correlation handlers, with the combination offering the protection of the entire energy infrastructure.

As demonstrated in the architectural framework, collaborative Zero Trust systems can be organized into three distinct categories according to recent cybersecurity research (Roman, 2021):

- **Centralized Zero Trust coordination systems:** The individual Zero Trust elements are localized threat detection parts that create security alerts around their operation. Ritter et al. (2021) acknowledge that the produced alerts are delivered to a centralized security operations centre, which becomes the enterprise-wide security correlation handler to evaluate the full threat intelligence in overall energy infrastructure.
- **Hierarchical Zero Trust management architectures:** The comprehensive energy security system is organized into smaller working units related to similar nature like geographical areas; the administration control limits, same type of technology being used etc. Chaudhry and Hydros (2021) also state that the elements of Zero Trust at the operational level are threat detection features, and those at higher levels of management have both detection and security correlation handlers to identify the threats in various levels of the organization.
- **Fully distributed Zero Trust architectures:** There is no centralized coordination system to process comprehensive security information across the energy infrastructure, instead utilizing fully autonomous security systems with distributed management and coordination capabilities. According to recent research on energy cybersecurity, all participating Zero Trust components maintain their own threat detection and correlation capabilities while communicating with peer systems to provide enterprise-wide security coverage and coordinated incident response (Al-Fuqaha et al., 2015).

3. Current state of the art of zero trust cybersecurity in energy systems

The findings which have recently been carried out on Zero Trust Architecture implementations in energy infrastructure are categorized systematically in two different sections following the comprehensive layered taxonomy structure. The first part will give an in-depth description of the proposed Zero Trust systems in relation to their structural design, implementation technologies, process operations of collecting audit data and general analysis of the audit data, threat discovery techniques, and automated responses to the detected threats. The second part specifically addresses research studies related to advanced security management technique that has focused on reducing a problem of false-positive security alerts through the application of different analytical techniques to different Zero Trust methods of detection and response enacted in environments of energy infra-structure (Anderson and Fuloria 2010).

3.1. Zero trust security and policy-driven access control systems for energy infrastructure

As can be seen in Table 1, some of the Zero Trust implementations that have recently been proposed to be used to protect the energy infrastructure are specifically tailored to the taxonomy described in the previous section. As discussed in Baig et al. (2017), the most striking aspect of this overall review is that current cyber security studies have focused a lot on cooperative Zero Trust mechanisms aimed at offering whole scale security to the distributed real brood energy spaces through hybrid abuse detection approaches as well as wired and wireless technologies of communication.

However, as indicated by the findings of recent cybersecurity research studies analysis, in most cases, the researchers have solved individual operational issues in the energy system, yet at the same time, they have not tried to optimise overall energy system security by putting all the proposed taxonomy items together. As an example, a high level of accuracy in identifying the threat is not currently one of the least built areas of energy cybersecurity development and very often remains unrelated to other resulting implementation obstacles like false-positive rates of detection, system reaction time, or constancy with current energy management systems (Banerjee et al., 2011).

Along with failing to accommodate the entirety of the security needs of the energy system, the Zero Trust implementations as currently proposed easily encounter some major operational and technical issues that constrain their applicability to distributed energy resources settings. Due to the ever-changing cybersecurity landscape that severely restricts the implementation of Zero Trust (especially in anomaly-based security frameworks implemented on energy networks), Bekara (2014) highlights the following as some of the key issues of implementation:

- **Traditional security systems have not been adequately adapted for emerging energy paradigms:** According to Bertino and Islam (2017), conventional cybersecurity approaches including legacy intrusion detection systems have failed to scale appropriately to satisfy high-performance energy network requirements, particularly those supporting real-time operational technology communications and distributed energy resource coordination protocols.
- **Dynamic operational profiles create significant implementation challenges:** The operational traffic patterns in energy systems consistently fluctuate across numerous environmental considerations such as market runs, noise in operational traffic, and operational environments that are highly dynamic in nature, and create an impossibility to compare changing behavioural patterns using large distributed energy networks (Buck et al., 2015).
- **Unacceptably high false-positive alert rates limit operational effectiveness:** Among the most severe limitation factors that inhibit the use of Zero Trust systems in energy setting are an alarmingly high number of false- positives security alerts that create a generation problem that can rapidly overwhelm security operations centre which might impact on the system of energy operations through various unnecessary restrictions on accesses or isolation of the system (Caralli et al., 2007).
- **Lack of standardized evaluation methodologies and performance metrics:** According to Cleveland (2008), despite numerous proposed cybersecurity techniques, implementation models, and deployed energy security systems including commercial solutions, there remains no uniform globally accepted standard or comprehensive metric framework to evaluate Zero Trust effectiveness in energy environments, although receiver operating characteristic analysis has been widely utilized for accuracy evaluation in general cybersecurity applications.

The comparative analysis of various components of Zero Trust taxonomy particularly relevant to the protection of energy infrastructure are discussed in Table 2. This review is structured in the straightforward presentation of all the unique strengths and weaknesses of every functional characteristic of comprehensive Zero Trust frameworks applied to the energy operation contexts. Based on the vastness of sources of ways of security solutions implementation and approaches, however, as presented by De Craemer et al. (2014), the most used and technically keyed security approaches are as follows in terms of the needs of security of distributed energy resources.

Of all the features of Zero Trust implementation, threat detection methodologies hold the greatest weight of current security research and development. As part of a structured review of current literature in cybersecurity, focusing on infrastructure protection of energy systems, a list of all evaluation criteria has been culled to be able to draw comparisons among various threat detection mechanisms such as signature-based techniques, anomaly-based techniques, and combinations of both mechanisms (Deng et al., 2017). The comprehensive comparative review based on systematically gathered evaluation criteria that are specifically applicable to the implementations of distributed energy resources security takes the form of Table 3.

A detailed list of operational objectives to be implemented has been neatly compiled to achieve best cybersecurity performance in instances of Zero Trust implementations, highest protection of the infrastructure, and minimal rates of error operations within distributed energy resource environments (Forrester Research, 2010):

- **ZT1:** Operate continuously with minimal or preferably without human supervision while maintaining full cybersecurity effectiveness across distributed energy infrastructure.
- **ZT2:** Demonstrate comprehensive survivability and fault tolerance capabilities to enable rapid recovery when energy management systems experience operational failures or cyber-attacks.
- **ZT3:** Be easily configurable and adaptable to specific distributed energy resource network architectures and operational requirements.
- **ZT4:** Dynamically adapt to changes in user behavioral patterns and energy system operations over extended time periods.
- **ZT5:** Function effectively in real-time operational environments without impacting energy system performance or reliability.
- **ZT6:** Accurately recognize all or most cyber intrusions with minimum numbers of false-positive security alarms that could disrupt energy operations.
- **ZT7:** Provide comprehensive self-monitoring and self-protection capabilities in case Zero Trust systems themselves are modified or compromised by cyber adversaries.
- **ZT8:** Be dynamically self-configurable according to changing cybersecurity policies and regulatory requirements of energy systems under continuous supervision.

- **ZT9:** Operate with minimal computational and network overhead while energy systems are running in normal operational modes.

Table 1 Classification of existing Zero Trust implementations based on comprehensive layered-taxonomy specifically designed for distributed energy resource protection

Reference	Year	Detection technique	Technology layout	Time of detect	Response type	Audit source location	Management structure	Remarks: prominent advantage or disadvantage
National Institute of Standards and Technology (2020)	2020	Hybrid (signature and anomaly)	Wired/Wireless (hybrid)	Real time	Active	Network and Host	Collaborative	Comprehensive framework but complex implementation
Roman (2021)	2021	Policy-driven anomaly	Wireless (mobile-agent)	Real time	Active	Network	Collaborative (fully distributed)	Fast threat detection but limited insider threat coverage
Ajiboye et al. (2021)	2021	Machine learning based	Wired	Real time	Passive	Host and Application	Individual	Advanced analytics but high computational requirements
Ritter et al. (2021)	2021	Hybrid (multi-layered)	Wireless	Real time	Active	Network and Host	Collaborative	Scalable architecture but vulnerability to coordinated attacks
Newhouse and Scarfone (2020)	2020	Risk-based assessment	Wired	Real time	Active	Host and Network	Collaborative (hierarchical)	Comprehensive risk analysis but slower response times
Chaudhry and Hydro's (2021)	2021	Micro-segmentation based	Wireless (IoT-enabled)	Real time	Active	Network	Collaborative	Effective network isolation but complex policy management

Most of the developed Zero Trust implementations, according to recent cybersecurity research analysis have been able to prove their efficiency of being able to cater to the operational characteristics of ZT2, ZT5, and ZT9 in distributed energy resource settings exceedingly proficiently. The initial one, ZT1 is, however, still very reliant on human supervision and intervention, especially in complex situations of security incident response that may require a sophisticated decision-making capacity (Hassan, 2019). As stressed when introducing the difficulties of cybersecurity implementation, the customary Zero Trust constructions have not been suitably mutated in the rudimentary conglomeration patterns of the building power landscapes like the advanced metering infrastructure and the distributed energy asset orchestration guidelines that imply, that such systems fail to procure the demanded features of ZT3 and ZT4 around the adaptability and configurability of the dynamic energy juncture operating conditions (Humayed et al., 2017).

While it has been observed that existing Zero Trust implementations have been able to achieve success in detecting most of the advanced cyber intrusions as defined in characteristic ZT6, this has led to undesirable levels of false-positive security alerts that are difficult to handle manually and might end up affecting energy operational activities (Jain and Shanbhag, 2012). As Kumar et al. (2021) posit, the developed Zero Trust systems have a long way to go to be able to achieve characteristics ZT7 and ZT8 that define the possibility of self-management, as they do not offer detailed autonomous management features that would allow the mentioned systems to properly operate without a significant amount of human supervision and manual configuration management in modern energy systems with the higher complexity in their structure.

3.2. Advanced threat detection and continuous monitoring frameworks for distributed energy resources

A common operational feature of anomaly-based Zero Trust systems operating on energy infrastructure is the inability to detect the threats completely accurately without raising too many false positive messages that can overload the security operations centres. According to Mahmoud et al. (2015) occurrence of false-positive events upon assuming that genuine energy operational activities are dangerously threatening in nature and assuming wrongly, yet in response to generation of potentially malicious activities cause false-positive events which demand equal investigation and may induce inappropriate security measures. On those occasions, energy systems also encounter false negative incidents, where the system fails to recognize real cyber-attacks on energy infrastructure, leaving them exposed to malicious activity with the risk of catastrophic impacts (McLaughlin et al., 2016).

Unfortunately, going by recent cybersecurity findings, the number of security alerts produced by Zero Trust systems installed in the energy setting may be altogether unmanageable, and producing thousands of alerts each day with most of them pertaining to false-positive findings without suggesting any kind of real security breach (Mo et al., 2012). In addition to the sheer number of alerts, this fact complicates thorough security alert investigation significantly as operations personnel at energy facilities must go through the alerts both to take account of them into consideration and to determine how to react to real cyber threats that may target energy facilities (NIST Framework, 2018).

As more energy infrastructure enterprises have adopted anomaly-based threat detection applications, a substantial new research direction has filled in concerning Zero Trust alert management that has now became exclusively dedicated to addressing how to build proper methodologies which can be used to better handle and manage security alerts more effectively (Patel et al., 2013). Table 4 provides a systematic overview of the most recent studies that attempt to solve in its entirety the issue of generic alert management, specifically in the domain of Zero Trust implementations in distributed energy resource settings. These research activities are aimed at developing automatic alert correlation procedures, executing risk-based alert prioritization process and devising intelligent alert filtering systems that can lessen false-positive rates even though retaining in-depth threat detection abilities (Rahimi and Ipakchi, 2010).

Generally, the mechanisms that advanced security alert correlation in energy environments are developed can be categorized into five methods of classification presumably based on recent research on cyber security (Ralston et al., 2007):

- Network behavioral pattern similarity analysis between security alert attributes
- Predefined cyber-attack scenario recognition and correlation methodologies
- Attack precondition and postcondition correlation analysis that constructs comprehensive attack scenarios by mapping consequences of earlier attack phases with prerequisites of subsequent attack stages
- Multiple information source integration approaches that combine various types of security intelligence and perform comprehensive reasoning based on correlated alerts and contextual information
- Advanced filtering algorithms specifically designed for energy operational environments

As recent research analysis indicates, most cybersecurity researchers have been primarily working on alert correlation solutions which by their nature are only applicable to the anomaly-based detection method as anomaly-only detection mechanisms in general generate substantially more alert responses as compared with signature-based or hybrid detection methods (Rose et al., 2020). Even though hybrid Zero Trust solutions may provide the best sacrifice of threat detection visibility versus system performance attributes, they, at the same time, complicate the overall thread detection process too much by requiring alert correlation of multiple detection methodologies with different performance (or workload) attributes, and varying levels of confidence in the threat assessments that need to be correlated.

Table 2 Comprehensive comparative analysis of Zero Trust features specifically applicable to distributed energy resource protection systems

Features	**Advantages**	**Disadvantages**
Technology layout		
Wired	Wired energy networks provide faster and more reliable communication with lower latency for real-time operational technology systems. Enhanced security through physical access control to network infrastructure.	Limited flexibility and scalability for distributed energy resources. Higher infrastructure costs for geographically dispersed assets. Vulnerable to physical tampering and cable cutting attacks.
Wireless	Offers extensive coverage and unlimited access which facilitates deployment across distributed energy assets. Highly scalable and independent from existing infrastructure platforms. Mobile agent implementations provide reduced energy consumption for battery-powered devices.	Inherently more vulnerable to wireless-specific attacks including eavesdropping, jamming, and man-in-the-middle attacks. Signal interference can impact communication reliability. More complex encryption and authentication requirements.
Detection method		
Signature-based	Signature-based detectors are highly reliable, computationally efficient, and generate very low false-positive alert rates when detecting well-known cyber intrusions specifically targeting energy infrastructure.	Severe limitations in detecting unknown attack variants and zero-day exploits that constantly evolve. Inability to detect sophisticated attacks that use legitimate protocols and commands. High maintenance overhead for signature database updates.
Anomaly-based	Anomaly-based techniques utilize fewer predefined rules compared to signature-based approaches, increasing detection effectiveness against novel attacks. Capable of detecting previously unknown attack patterns without requiring signature updates.	Generate significantly higher false-positive alert rates because deviation from normal behavior does not always indicate malicious activity. Extremely difficult to establish baseline behavior in dynamic energy environments. Vulnerable to slow poisoning attacks that gradually modify baseline behavior.
Hybrid	Combines advantages of both signature-based reliability and anomaly-based novel threat detection capabilities. Provides comprehensive coverage against both known and unknown attack patterns.	Increased system complexity and higher computational requirements. More challenging alert correlation and response coordination. Higher implementation and maintenance costs.
Time of detection		
Real-time	Enables immediate threat detection and prevention capabilities that are critical for energy infrastructure protection. Supports rapid response to prevent cascading failures across interconnected systems.	Cannot effectively process encrypted communications without significant performance impact. Real-time processing limitations may miss sophisticated multi-stage attacks that unfold over extended time periods.
Non-real-time	Provides comprehensive forensic analysis capabilities and detailed threat intelligence for improving future security measures. Lower computational resource requirements and reduced system performance impact.	Cannot provide immediate response to prevent ongoing attacks or system damage. Limited effectiveness against fast-moving threats that can cause significant damage before detection.

Data source location		
Network-based	Monitors network traffic patterns across entire energy infrastructure segments providing comprehensive visibility of communication flows. Strategic positioning enables rapid response and traffic isolation capabilities.	Limited visibility into encrypted communications and internal host activities. Cannot detect attacks that do not generate distinctive network traffic patterns. Vulnerable to network segmentation bypasses.
Host-based	Provides detailed visibility into individual system activities including file access, process execution, and user behaviors. Capable of detecting insider threats and privilege escalation attacks. Cost-effective deployment without requiring additional hardware infrastructure.	Limited network visibility and inability to detect network-based attacks targeting other systems. Performance impact on critical energy operational systems. Vulnerable to sophisticated rootkit and firmware-level attacks.
Response type		
Passive	Facilitates comprehensive information gathering and forensic analysis while maintaining system availability for critical energy operations.	Exposes energy assets to ongoing attacks while security personnel investigate and respond to threats. May not prevent significant damage during extended investigation periods.
Active	Provides immediate threat blocking and isolation capabilities to protect critical energy infrastructure from ongoing attacks.	May inadvertently disrupt legitimate energy operations through false-positive responses. Could be exploited by attackers to cause denial-of-service conditions.

4. Zero Trust Architecture implementation in distributed energy resource computing environments

Even though the traditional distributed security systems have been considered potentially able to ensure sufficient protection of large energy networks, their application and use in contemporary distributed energy resource contexts is associated with numerous critical challenges and remains one of the unsettled and challenging technical realization issues (Roman, 2021). The article by authors such as Ajiboye et al. (2021) explains that the multiplicity of users of distributed energy resources, the richness of architectures of interconnected energy systems and diversity of demands and needs results in a variety of requirements in implementation of cybersecurity or various opportunities to utilize Zero Trust to ensure all-encompassing protection of the system.

Beyond cybersecurity challenges caused by novel distributed energy resource capabilities and multidimensional system designs, clean energy computational platforms also assume every vulnerability in the traditional network and operational technology services and incorporate a novel slate of attack paths that corresponds to the energy infrastructure architecture (Ritter et al., 2021). Newhouse and Scarfone (2020) in their study of the issue of energy cybersecurity, point out that both historical security weaknesses and new types of threats in distributed energy resources environments are to be considered to implement the Zero Trust fully.

To comprehensively discuss the overall cybersecurity needs of Zero Trust application in distributed energy resource settings, this part, in the first step, analyses the unique characteristics of operation of contemporary energy computing systems and pinpoints certain implementation issues of Zero Trust implementation within energy operational contexts. The analysis then, according to Chaudhry and Hydros (2021), explores the existing Zero Trust systems with regards to their efficiency and effectiveness in use as well as deployment within operational contexts of distributed energy resources and presents through thorough identification, a set of requirements specific to the success of Zero Trust deployment in context of energy systems and the security capabilities sought by these systems.

4.1. Characteristics of distributed energy resource systems and cybersecurity implementation challenges

Identification of precise operational peculiarities of a distributed energy resource environment is critical towards determining the comprehensive system demands and directing the building processes of a successful cybersecurity system. As shown by Al-Fuqaha et al. (2015), the distinguishing features of distributed systems of energy resource computing are multiple essential features of their operating process and technical aspects that have a direct implication on Zero Trust implementation strategies and the quality requirements of cyber protection.

4.1.1. DER1

Dynamic scalability and elasticity represent crucial core features for energy systems that demand the existence of underpinning infrastructure capabilities to automatically adjust to highly changing operations needs like variation in energy demand profiles, fluctuation of renewable power production rates, and variations in grid ability to handle operations. Anderson and Fuloria (2010) state that operating scalability systems that constitute distributed energy resources consist of two different categories of scalability namely vertical scalability which denotes the degree of computational and communication capabilities of any given energy resource, and horizontal scalability which deals with the overall amount of instances of the distributed energy resources needed to meet the changing demands of the grid operations in terms of time of day and seasonal comparisons.

4.1.2. DER2

Operational reliability represents the fundamental capability of ensuring continuous energy system operation without any requirement to redirect or redirect other services and including data loss prevention, executing programs, or operational restoration situations in normal and emergency situations. The normal mechanisms of achieving reliability within the distributed energy resource setting, therefore, include introduction of energy assets that are redundant, backup communication systems and resilient operational technology infrastructure although most of the cybersecurity solutions fall on the software side of implementing the solution even though the hardware implementation may present even more opportunities of potential vulnerability (Banerjee et al., 2011).

There is indeed a close interdependency between the availability of the energy system and the operational reliability properties, but reliability is specifically the operational prevention of loss provisions such as data integrity, energy delivery capacity, and grid stability. Bekara (2014) postulates that comprehensive reliability demands are even more essential in distributed energy resource settings where one asset failures may be able to propagate through cascading effects across interconnected systems and could affect the overall stability of selected grids and grid operations.

4.1.3. DER3

Quality of Service support is vitally important for meeting specific operational requirements which should be ensured by the profound provisions of energy services and calculations resources which are supplied to ensure significant grid operations. Bertino and Islam (2017) stated that in order to make sure that what has been agreed on in terms of service quality in energy Service Level Agreements are continually achieved, essential Quality of Service indicators such as safety of the operations, responsiveness of the system, energy delivery speed, and scope of the security protection provided by cyber security resources should be continually ensured in whatever conditions the distributed energy resources are to operate.

4.1.4. DER4

Agility and adaptability represent two essential features of significant concern of distributed energy resource systems, which is directly connected to capabilities of elastic operations and dynamic response. By definition, these properties denote the ability to respond promptly to the variations in the demands of the computational resources, networks access bandwidth, and the volumes of operational requests in addition to the abilities to adjust to the variation of environmental conditions, communications market signals, and grid operation needs that may require the provision of different varieties of the energy resources, alternate communication routes, or altered operational quality parameters (Caralli et al., 2007).

To conclude, broad agility and adaptability specifications require the resource management procedures be executed as autonomic systems that can self-configure, self-optimize, and self-heal without a lot of human involvement in regular operating conditions. In terms of grid stability and operational efficiency, and in the light of dynamic renewable energy production and variable patterns of customer demand which typify the contemporary distributed energy resources system, these capabilities are critical to achievement, as states Cleveland (2008).

4.1.5. DER5

Availability of energy services depends fundamentally on the ability to provide redundant operational capabilities and redundant schemes to ensure that the failure of any single component is hidden and does not affect the general energy delivery or performance of the operations of the grid. As Colwill (2009) notes, fault tolerance capabilities must also have the ability of introducing substitute resource such as new energy resources or those other resources that have failed previously introduced in online manner without a significant deterioration of performance and interruption of treatment services at the critical stages of operation.

4.2. Challenges of zero trust development in distributed energy computing environments

It is critically essential to systematically derive the precise implementation challenges that are caused due to the nature of operation of the distributed energy sources prior to the creation of elaborate frameworks of Zero Trust cybersecurity of energy infrastructure. Deng et al. (2017) identify the implementation issues that cybersecurity developers faced in the process of Creating Zero Trust in distributed energy resource environment, which include several groups of technical, operational, and regulatory factors that need to be addressed with the help of holistic approaches to design.

- **In traditional cybersecurity implementations, static operational characteristics of monitored systems** allow security policies to stay relatively fixed as the associated energy asset groups are likely to be consistent in that respect with their operational requirements being established and verified over long periods of operation. Based on the article by Fang et al. (2012), unlike the traditional operational models, distributed energy resource systems are removed and added dynamically upon grid in operations to reflect the existing market conditions, availability of renewable resources, and the needs of grid balancing, and moreover, the cybersecurity requirements vary widely to different individual energy assets, depending on the roles undertaken by each asset, the connections requirements and the level of risk exposure.
- **Security policy establishment and management processes are typically controlled by designated system administrators** who should be accountable in terms of cybersecurity protection in the whole energy operating environment. Forrester Research (2010) also states that distributed energy resource systems have several system security administrators who are the representatives of various organizational entities such as utility operators, energy service providers, equipment manufacturers, and regulatory bodies hence poses coordination stress that could affect the timeliness of intrusion response as well as events of overall cybersecurity.
- **Malicious insider threats represent increasingly accessible attack vectors** by authorized involvement, in distributed energy resource service provider groups or by infiltration of legitimized individuals' privileges. As Hahn et al. (2013) describe, recent studies in cybersecurity have led to significant evidence that most advanced forms of cyber intrusion into critical infrastructure are always caused by internal threats working within legitimate access credentials and with in-depth knowledge of the systems vulnerabilities hence, the use of traditional security methods such as the perimeters approach is also ineffective to protect the energy infrastructures.
- **Data transfer costs represent significant operational considerations** for distributed energy resource implementations that must balance cybersecurity monitoring requirements with economic efficiency constraints. According to Humayd et al. (2017), comprehensive security monitoring and threat detection capabilities can generate substantial data volumes that must be transmitted across communication networks, potentially creating cost burdens for energy system operators while consuming bandwidth that may be needed for critical operational communications.
- **Additional cybersecurity challenges involve comprehensive visibility into inter-asset communication traffic** flowing among distributed energy in the virtualized operating environments, as the switching and routing of communications is also being run on the virtualized technologies as opposed to the physical network infrastructure that is installed. However, Jain and Shanbhag (2012) argue that traditional solutions aimed at monitoring of physical networks cannot analyses the virtualized communication traffic in a suitable manner, and the virtualized platforms might possibly exhibit security gaps that can be used to seize all the energy assets at once.

4.3. State of the art of distributed energy resource zero trust architecture systems

Majority of the currently proposed Zero Trust implementations to protect each of the distributed energy resources aim at operating independently across each of the operational layers, as infrastructure, platform, and application layers and act mostly in threat detection and prevention without significant integration across numerous operational layers or coordination with other cybersecurity systems (Mahmoud et al., 2015). As McLaughlin et al. (2016) explain, the systems of Zero Trust functioning at the energy infrastructure level have recently been proposed by some recent studies to be implemented using the technology of monitoring hypervisors and virtual machines to protect this type of cyber attack against Infrastructure-as-a-Service energy operations.

Such infrastructure-layer security models have shown better reliability and availability properties of the energy systems since security protection can be maintained by the underlying infrastructure components in the most of the operational conditions, and this allows the energy services and applications to be confident about secure infrastructure support. As already noted by other studies (Mo et al., 2012), such infrastructure protection strategies have not given a clear way out to recovery and restoration of a system in case of the failure of critical infrastructure units because of the existence of complex cyber attacks or multiple threat outbreaks that overwhelm various levels of system security protection to become effective at the same time.

Most of the cybersecurity researchers proposed solutions to zero trust systems protecting their energy systems incurs the need to overlook the prevention capabilities. Recent implementations according to Rahimi and Ipakchi (2010), are mostly cantered on the detection and alerting of threats without giving full automated responsiveness that can make a cyber attack unsuccessful or reduce its effects to the energy operational systems. Some of the studies in intrusion detection using the anomaly-based intrusion detection have been developed to be specific in complex energy systems that have been termed as Software-as-a-Service operational environment.

Anomaly-based intrusion detection has been named by these researchers as a potential promising technique regarding the protection of energy systems at the application layer because they perceive that most cyber intrusion are likely to be based on where the application code is implemented and therefore, they interpret application-layer attacks as the most potentially harmful attacks that may modify or inject false operational data into distributed energy resource management systems. Ralston et al. (2007) note that these research efforts have not come up with comprehensive and coordinated response and attempted to prevent cyber attacks that have been detected across the multiple operation levels and energy assets.

Machine learning is another high-level approach that has been applied to the training of cybersecurity systems on anomaly detection in the energy operation spaces. Rose et al. (2020) offer that most current studies have presented Grid and Cloud Computing Intrusion Detection Systems to specifically integrate energy resource environments because it encompasses cyber attack management with extensive audit systems that comprise both signature-based and unusual-based threat-detecting procedures to single out cyber intrusion types against energy infrastructural systems.

Such research activities involved the use of Artificial Neural Network technologies as a method of training cybersecurity systems and the development of prototype implementations using specialised middleware platforms specifically designed with grid computing applications in mind. Based on National Institute of Standards and Technology (2020), these systems have established low computational processing costs and also have shown to have appropriate performance characteristics that are suitable to be used in a real-time implementation in an operational setting of the energy structure mainly due to the ability to analyze security on a specific energy asset by itself which keeps the traffic of data transfer between the distributed components to a minimal and also reduces the overall complexity of the systems to achieve.

This distributed analysis method effectively mitigates distributed energy resource characteristic number five noted in the previous section and can address implementation challenge number five of cost reduction in transferring the cumulative audit data to centralized security operations centers since the security processing is completed on the local host at each energy resource location. As stated by Roman (2021), the main weaknesses of these systems are the fact that they only detect certain types of cyber intrusion and do not include automated preventive abilities in terms of being capable to prevent cyber attacks to be however victorious against the energy operational systems.

These proposed systems exist in grid computing as well as distributed energy resource settings, but they require alternate specialized formulations to provide Zero Trust protection to distributed energy resources instead of their being applied to energy infrastructure by taking advantage of some global protection framework available to grid computing domains (Ajiboye et al., 2021).

Designing suitable Zero Trust architecture frameworks has always been a problematic design choice among cybersecurity researchers who come up with a robust security infrastructure within any distributed energy resource set-ups because of the diverse modes of operation and complicated nature of its virtualization needs. As suggested by Ritter et al. (2021), recent studies have come up with collaborative intrusion detections systems that have centralized management approaches delivering fast and effective threat stopping capabilities through distributed energy infrastructure systems.

Although research has revealed the nature of the scalability of systems, the centralized implementation of management is fundamentally unscalable as the security performance exponentially deteriorates with higher data processing activity impacts to central components of management. As discussed by Newhouse and Scarfone (2020), centralized management systems are also single points of failure used in processes that are unacceptable in distributed energy resource environments that have high availability and fault tolerance requirements needed to support critical energy infrastructure processes.

Even the proposed architectural forms are still struggling with a lack of scalability and the capability of failing because of a central manager component failure which may jeopardise the cybersecurity protection of the whole distributed energy resource operational landscapes. Unlike centralized systems, recent studies have facilitated fully distributed Zero Trust frameworks featuring peer-to-peer network architecture that implements the hybrid detection strategy using combined network-based and host-based sources of audit data to build flexible, robust, and elastic types of security solutions made especially suitable to distributed energy resource computing environments.

These distributed systems achieve enhanced scales of scalability when compared to centralized systems, but they still cannot provide sufficient means of identifying large-scale coordinated cyber attacks on distributed energy infrastructure due to their processing of only a small range of features of the alert information and because they lack centralized correlation facilities that can be used to aggregate the full range of alert information across all energy assets to identify time-sequential multi-stage attack events that evolve over an extended time horizon and over multiple operating domains.

Table 3 Comparison of threat detection methods based on collected criteria from existing cybersecurity surveys specifically applicable to distributed energy resource protection systems

Comparison criteria	**Detection techniques**		
	Signature-based	Anomaly-based	Hybrid
Robustness	Low	High	High
Flexibility	Low	High	High
Scalability	Low	High	High
Resource consuming	Low	High	Moderate
False alarm rate	Low	High	Moderate
Reliability	High	Moderate	High
Detection speed	High	Low	Moderate
Commercial tools	Cisco Net Ranger, Snort, Nessus	Mazu profiler, n Patrol, SPADE, Prelude	Watchguard Firebox, Cisco IPS, McAfee Intru Shield

The increasing interest in providing autonomic computing solutions has recently been given much attention in cybersecurity research in designing, building, and managing distributed energy resource Zero Trust systems that require minimum human interaction in the process. Al-Fuqaha et al. (2015) specify that an autonomic cybersecurity system must exhibit the abilities to change the operational behavior flexibly by adjusting to new situations in operations through the extensive practices of operation self-management, self-tuning, self-configuration, self-diagnosis, and self-healing that execute automatically and do not need human attention in the regular cases of evaluating operation situations.

Autonomic computing solutions are especially applicable to distributed energy resource settings where there is a need to scale rapidly over heterogeneous resource pools to accommodate all sorts of execution demands that may be unpredictable, and where cybersecurity processes need automatic adaptation so that failure of underlying equipment or program code is not apparent to the delivery of energy services or operational depend abilities, even in the event of underlying failure of hardware or program code. Anderson and Floria (2010) explain that the autonomic energy systems come into existence due to the application of autonomic computing strategies to distributed energy resource settings, which lead to the pattern of fault-tolerant, selector agent-based energy system organizations and the cybersecurity implementations.

The current studies have hypothetically developed autonomic methods of anomaly detection algorithms in distributed energy resource computing environments which include holistic methods of analyzing the gathered security data without human interferences. Baig et al. (2017) state that these approaches offer consistent data analysis outputs, feature extraction features to compress data, and machine learning features to identify energy assets with abnormal patterns of operating or operating differently than other similar assets in the unsupervised mode of operation.

Certain cybersecurity researchers have given attention to using the possibly accessible computing resources and idealizing security reaction abilities through risk determination and computation strategies accompanied by fuzzy logic strategies particularly intended to use the energy operational setting. Cleveland (2008) described recent studies that have suggested multilevel intrusion protection systems and blanket log management functions that place varying degrees of strength in protecting security against access privileges according to the degrees of anomaly and the evaluated risk definition of network users of distributed energy system resources or would be cyber-attack adversaries.

The main drawback of risk-based approaches is that they are not robust in terms of detecting large scale coordinated cyber-attacks because the individual intrusion detection systems are running stalling that do not have extensive coordination and correlation capabilities. De Craemer et al. (2014) mention that in recent literature, ontological intrusion detection systems that are specifically targeted at distributed energy resource computing environments have been introduced to work as entity-based systems with complete vulnerability and source of a security flaw scoring methodologies applied to ontological knowledge representation and risk assessment practices.

The suggested ontological methods consider briefly three basic elements, that are specifically applicable to distributed energy resource contexts: the decoupling relationships between data-assets, composition abilities among numerous energy resources, and the external resource usage patterns which may be used as a set of all-inclusive collection of typical cybersecurity terms and semantics that can be used in distributed energy resource computing environments. In the work of Deng et al. (2017), we see that using these ontological frameworks would give standardized ontological language to coordinate cybersecurity that traversed various organizational layers and operational units in distributed energy resource management and protection.

4.4. Zero trust architecture requirements for distributed energy resource protection frameworks

Considering the overall considerations of the peculiarities of distributed energy resource systems as well as the ideal Zero Trust implementation possibilities described in previous sections, the requirements to the Zero Trust Architecture of distributed energy resources in high-level operations and technical respects are identified as follows. The said requirements by Fang et al. (2012) set out basic instructions to design, implement, and operate effective Zero Trust cybersecurity structures specifically adapted to distributed energy resources protection regarding the peculiarities of operations and the necessity to comply with regulatory requirements and obligations.

- R1 Handle large-scale dynamic multi-tiered autonomous computing and data processing environments across distributed energy infrastructure

Distributed energy resource system is basically characterized as a large-scale virtual machine based operational environment which can be automatically created, migrated, and terminated according to user demand pattern, market conditions and grid operational demands that are dynamic in nature in the course of real time operation. Based on Forrester Research (2010), there is generally the expectation that when energy resource configurations change, middleware management systems will be informed about the changes, but in the distributed environment of energy resource computing because it involves large-scale networks and complex operational systems, it would be critical to sustain these changes automatically and without human intervention so that the cybersecurity protection can be continued.

To address the complexity inherent in the characteristics of dynamic distributed energy resource operations, the Zero Trust cybersecurity infrastructures must be able to operate with little or preferably no human control and be able to provide end-to-end monitoring and control of the individual components of an energy network in real time operational contexts. Hahn et al. (2013) states that this requirement directly contributes to the distributed energy resources characteristics CC2 and CC3 which deal with the reliability of operational sustainability and Quality of Service provision without disrupting the critical energy activity by the cybersecurity protection provisions.

- R2 Detect comprehensive variety of cyber-attacks with minimal False Positive Alert rates across distributed energy operational environments

Because of the exponentially raising the level of advanced cyber-attack techniques, the complexity of the threat vectors, and the uncertainty of malicious actor attack plans against critical energy infrastructure, unique to each set, it would be required that Zero Trust systems identify and observe the new patterns of attacks and evaluate their malicious intents to generate the optimal response regimes by risk severity and subsequent prevention approaches to block the risk. Zero Trust systems, according to Jain and Shanbhag (2012), must show machine level capabilities and continually increase threat detection effectiveness over long working uptimes to sustain comprehensive characteristic IC6 and keep the performance levels within the acceptable limits. Kumar et al. (2021) in their study of energy cybersecurity needs stress that efficient threat detection systems must be precisely elaborated to secure desired performance and security levels within negligible computing resources utilization as efficiency of energy services is corely dependent on computing capacity and network performance. Thus, following Mahmoud et al., (2015), when dealing with the false-positive security alerts, advanced analytical techniques are to be applied to obtain the characteristics of comprehensive threat detection performance, and the latter directly covers the characteristic of Distributed energy resources of CC3 regarding the Quality-of-Service support of critical energy operations documentation.

- R3 Provide super-fast threat detection and prevention capabilities for real-time energy operational environments

A high threat detection speed and automated prevention measures are also important enabling considerations of distributed energy resource Zero Trust implementations as cybersecurity response time directly impacts the overall energy system performance and becomes a determining factor in providing pre-agreed Quality of Service levels committed to in energy service contracts. The role of distributed energy resources in terms of operational reliability and Quality of Service support and the need to mitigate the negative consequences of cybersecurity protection on the performance of energy systems is associated by McLaughlin et al. (2016) with DEC3 and DEC2 characteristics of distributed energy resources. A multi-administrated distributed energy resources system ought to cap/eliminate the need of human intervention in the process of cybersecurity resource administration so that no unwarranted delays by administration responses are created that may affect energy operation efficiency. Mo et al. (2012), in their work on real-time energy security, state that Zero Trust systems would only act in real-time operational states, and it should also be self-managed in normal cases without getting the permission of human supervisor. Unlike conventional hand-on security strategies, NIST Framework (2018) underlines that such automated responses meet the inherent IC1 and IC5 features of continuous nature and real-time functions and provide that security of cybersecurity applies to the protection but not detrimental to energy system reliability and performance.

- R4 Implement self-adaptive autonomic capabilities for dynamic distributed energy resource operational environments

The essential property of being able to easily fit into the distributed energy resource operating conditions and the degree to which Zero Trust architectures are supposed to work becomes monumentally important in ensuring the successful implementation of cybersecurity within the energy infrastructure environment. They hypothesize that detailed Zero Trust systems ought to automatically adjust to configuration alterations as nodes present in energy computing environments are introduced and eliminated dynamically during operation without varied security protection being presented in various working conditions (Patel et al., 2013). Rahimi and Ipakchi (2010), in their study of adaptive security systems explain, how adaptive security systems are configured to process and exchange security alerts at the required levels that requiring actors will process properly and share security alerts across individual detection components and ensure correct topological models of distributed energy resource computing environments.

- R5 Maintain deterministic operational performance characteristics under all operational conditions

The functional services that distributed energy resource computing environments support are, in part or all, mission-critical, as well as, safety-critical in that there are operational performance requirements which must be met in terms of operational latency, system reliability, and operational resilience regardless of whether operations are disrupted by a security incident under implementation. Moreover, supporting characteristics IC2, IC9, CC2, CC3, and CC5 regarding survivability, minimal overhead, reliability, Quality of Service, and service availability would require the comprehensive Zero Trust systems to provide and maintain service levels that are considered acceptable despite the presence of cybersecurity threats and to be highly reliable and encounter of energy operations with minimal costs to service integrity and provision.

Zero Trust application needs not only to have a real-time performance profile but also ensures that no negative impact on deterministic behavior of energy networks is adversely affected by cybersecurity protection, intrusion visibility, analysis, or response. In the case of Chaudhry and Hydros (2021), performance of energy system should be predictable and reliable beyond successful execution of exhaustive cybersecurity cyber protection measures that dwell in minor background process in an energy system and do not impinge in the critical energy system procedures. However, operational network traffic obtained within distributed energy resource settings is never regular and is constantly subject to change with market conditions, weather patterns, and customer behavior, the performance of Zero Trust must idealistically remain deterministic and predictable despite the randomness of the operational network traffic.

- R7 Provide comprehensive resistance to compromise and self-protection capabilities

Regarding trait IC7 of the corresponding self-monitoring and self-protection, distributed energy resource Zero Trust systems need to be able to protect themselves against malicious and unauthorized access attempts and, more specifically, against advanced cyberattacks that appear as targeted attacks on individual parts of cyber security infrastructure. Zero Trust implementations should be able to authenticate the energy network devices and the other zero trust components to each other, authenticate, and audit the administrative personnel and their security-related activities, provide protection of security-related data and configuration data, and discover potential security loopholes that can open up new attack vectors against cybersecurity infrastructure itself (Bertino and Islam, 2017).

Table 4 Classification of advanced security alert management techniques specifically designed for distributed energy resource Zero Trust implementations

Reference	Year	Method	Performance	Technique category	ZTA technique	Management model
National Institute of Standards and Technology (2020)	2020	Multi-stage classification using neural networks and clustering algorithms	More than 65% reduction in false positive rate	Similarity analysis and filtering algorithms	Hybrid approach	Alert correlation
Roman (2021)	2021	Risk-based data mining using hierarchical classification methods	Reduces FPR from 18% to 6.2% for real-world energy data	Filtering algorithms and attribute similarity	Anomaly-based	Alert correlation
Ajiboye et al. (2021)	2021	Post-processing filters based on statistical properties	Up to 82% reduction in false positive rates	Filtering algorithms	Signature-based	Alert quality improvement
Ritter et al. (2021)	2021	Clustering-based filtering using machine learning	Average 78% reduction of false positive rates	Filtering algorithms	Hybrid approach	Alert quality improvement
Newhouse and Scarfone (2020)	2020	Ontology-based correlation techniques	Significant improvement in attack scenario recognition	Preconditions and postconditions analysis	Policy-driven	Alert correlation
Chaudhry and Hydros (2021)	2021	Fuzzy logic measures and adaptive sets	Decreased FPR with minimal detection rate reduction	Similarity between alert attributes	Anomaly-based	Alert correlation

All the comprehensive solutions involving development of distributed energy resource Zero Trust systems must systematically address the requirements identified in this context to break through the energy computing complexities and fulfill the real-world operational objectives of the current distributed energy resource operational environments. Based on a review of proposed Zero Trust implementations of distributed energy resources mentioned in current literature, Colwill (2009) discovers that current systems fully attainment of all identified requirements and are thus not immediately usable in the distributed energy resource computing environment without considerable additional development and testing.

The diversity of the operational features of a distributed energy resources computing environment makes it necessary to use hybrid-based cybersecurity solutions and hybrid technical implementations of Zero Trust to address all its established operational needs and security needs. As De Craemer et al. (2014) point out, based on such breadth of requirements, evaluation criteria that would assess capacities of distributed energy resource Zero Trust systems could be easily devised and applied to inform the future research and development activities as well as ensure that cybersecurity solutions meet practical operational demands of the stakeholders of the energy infrastructure.

Table 5 Comprehensive analysis of proposed distributed energy resource Zero Trust systems according to identified operational requirements

References	**Requirements**						
	R1	R2	R3	R4	R5	R6	R7	R8
National Institute of Standards and Technology (2020)	✓	✓	✓	P	✓	✓	P	✓
Roman (2021)	P	✓	✓	✓	P	✓	✓	P
Ajiboye et al. (2021)	P	P	✓	P	✓	✓	P	✓
Ritter et al. (2021)	✓	✓	P	✓	✓	P	✓	P
Newhouse and Scarfone (2020)	✓	P	✓	✓	P	✓	✓	✓
Chaudhry and Hydros (2021)	P	✓	✓	P	✓	P	P	✓

P = Partially meets requirement, ✓ = Fully meets requirement, X = Does not meet requirement, N/A = Not applicable

5. Discussion on implementation strategies and policy-driven security frameworks for energy systems

In order to address in full the first fundamental research question, as to what particular set of criteria and comprehensive requirements should Zero Trust Architecture frameworks fulfill to be successfully used to operate in the environment in which distributed energy resources are used, a systematic set of operational and technical requirements was systematically collected and documented in the next previous subsection on the basis of the peculiarities of distributed energy resource computing systems and optimum possibilities of successful Zero Trust implementation. The paragraphs by Deng et al. (2017) identify the requirements as expert-level pieces of advice to the cybersecurity specialists and energy industry partners tasked with designing and operating, among other activities, the effective Zero Trust cybersecurity environment in real conditions under the energy industry performance operations.

In this extensive discussion section, the possible solution to implementation that satisfyingly address the entire list of distributed energy resource Zero trust requirements is systematically analyzed so that detailed answers to the second fundamental research question in which specific implementation methods and advanced cybersecurity techniques can address comprehensive Zero Trust requirements, retain operational efficiency and regulatory compliance in a satisfactory manner, are also available. Fang et al. (2012) described that the implementation of distributed energy resource Zero Trust challenges in natural complexity required the use of four core concepts herein identified via state-of-art review of the existing distributed energy resource cybersecurity implementations to meet comprehensive operating demands using Autonomic Computing principles, Comprehensive Risk Management methodologies, Advanced Fuzzy Logic Theory applications, and Semantic Ontology frameworks as exhibited in figure 4.

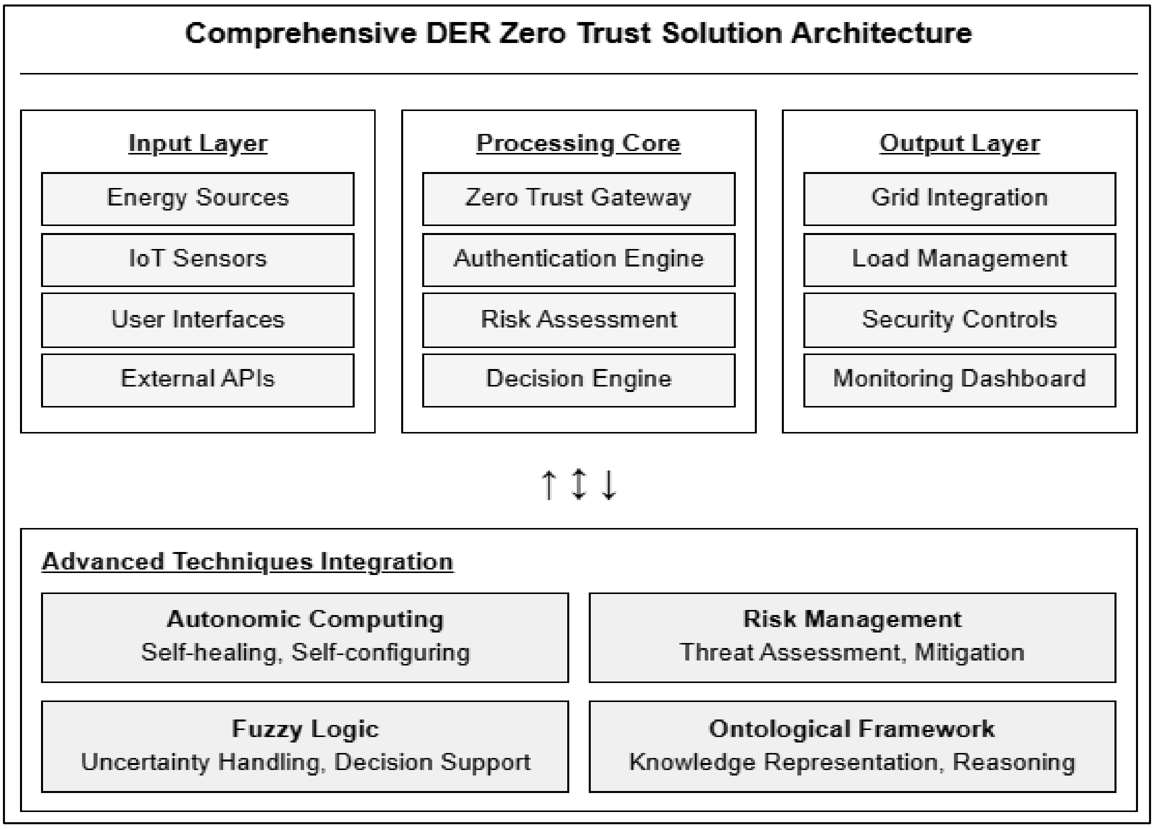

Figure 5 Proposed comprehensive solution architecture utilizing advanced techniques from autonomic computing, risk management, fuzzy logic, and ontological frameworks to develop effective distributed energy resource Zero Trust systems

Let's now thoroughly review how all these four basic concepts can be used effectively to formulate the development of efficient Zero Trust systems that can be holistically consistent with the operational and technical needs of distributed energy resource cybersecurity protection. As illustrated in requirement R1 by Forrester Research (2010), it would be methodical to have Zero Trust systems that will tend to be self-managed to efficiently manage the dynamic distributed energy resource operational environment with minimum human overload. The autonomic computing properties prevent the cybersecurity mechanisms to manually identify any hardware and software changes in configuration and adjust horizontally to the changing operational state without affecting its functionality.

Capable of comprehensive integration of ontological knowledge bases, it presents the dotted energy resource intrusion detection sensors in a position to be able to react and respond to dynamism of energy network topology, and the development of cyber threats in a dynamic fashion and to make use of internal security intelligence that is developed among the multiple information sources distributed in energy operational networks. Ontological frameworks help in defining the concepts of cybersecurity, the object of operations and the relationships between them in broad based realms of knowledge, to integrate the knowledge bases of several entities in energy systems to support dynamic adjustment to varying energy operational contexts, as explained by Hahn et al (2013).

The broad requirement R2 recognised that it is extremely important to identify different complex cyber attacks with maximum negligence over the false-positive alerts and maintain optimum efficiency within the environment of energy infrastructures. Hassan (2019) suggests that by applying the hybrid threat identification mechanisms alongside the right risk management strategies and thorough severity examination strategies, it is possible to meet this basic need whilst aiming at a balance between security performance and operations performance. As soon as the effectiveness of possible cyber threats is fully identified by elaborate analysis, Zero Trust systems are expected to automatically scan all the affected energy systems and deploy advanced vulnerability check-ups to get an idea of the consequences of an attack and formulate appropriate responses.

The extensive vulnerability assessment data could then be analysed systematically in conjunction with the energy network behavioural data and operational patterns to come up with a sensible real-time intelligence on what specific cyber attack is taking place and the potential operational implications of specific cyber attacks on target energy systems as well as on interconnected infrastructure elements. Research by Humayed et al. (2017) argues that when analytical obsessiveness to rate energy assets on nested levels of criticality has been enacted and a continuous stream of ontological security intelligence has been drawn across all potential sources, then automatized intrusion prevention measures can proactively be taken in real time without any intervening operations cost and with the same degree of effectiveness to protect the environment of distributed energy resources.

Keeping all the above-mentioned designs in view, to systematically analyze comprehensive false-positive alarm reduction schemes, it is important to measure the cybersecurity risks exposed to the attacked energy assets and assess residual risks posed by the vulnerable critical energy infrastructure components to different levels of threats. Mahmoud et al. (2015) state further that cyber threats and security intrusions have varying operational implications and different levels of perils that need to be addressed step-by-step to come up with comprehensive response strategies in the protection of distributed energy resources.

Even though the Zero Trust systems must handle and ensure all the levels of prevention and detection of cyber intrusions and many attack patterns, it is operationally imperative to determine the level of danger and a range of risk intensity characteristics that relate to various categories of dangers and attack mechanisms. As reported by McLaughlin et al. (2016), in selected coordinated attack cases and malicious scenarios and event situations where a limited amount of computational resources cannot possibly be used to defend the entire system within the required time limit, distributed energy resource Zero Trust systems may be used to fulfill the priority-based response principle of taking adequate measures based on a holistic assessment of the danger levels to prompt best responses and culminate in the least exposure of vulnerabilities and infection risks in the entire system.

Any Artificial Intelligence and Advanced Fuzzy Logic techniques can be used very efficiently in the scoring of vulnerable energy assets, in the systematic identification of the levels of likelihood of various cyber threats, in the comprehensive evaluation of the appearance of relative risk aspects, in the provision of priorities-based alarm management schemes and in the generation of the best response procedures to breaching cybersecurity incidents. To ensure greater utilization and application of derived security intelligence in distributed energy resource operational settings, the authors of a research study by Mo et al. (2012) argue that all the cybersecurity risk assessment activities can be characterized at the comprehensive domain ontological level in terms of high-level cybersecurity concepts like the attack methods, system vulnerabilities, and security incidents.

Cyber intrusions against energy infrastructures are systemically analysed and rated along many dimensions through diverse analytical focusing thus could be well represented using Multi-Dimensional Type-2 Fuzzy Logic modeling of analysis. In Multi-Dimensional Type-2 Fuzzy logic applications, the process of logical reasoning is very similar to the conventional fuzzy logic approaches but extensive integration of all the features of any situation of cyber intrusion are characteristically considered and fuzzification steps are the processes of considering these diverse features together rather than processing them against single and segmented variables (NIST Framework, 2018).

The speed of cybersecurity response is a decisive operational factor that R3 of the comprehensive requirements targets in distributed energy resource Zero Trust implementations. Patel et al. (2013) affirm that automated agent-based security management and self-managed operational mechanisms may lead to tremendous shortening of the response time of cybersecurity by removing the gap of time lapse between occurrence of security alert and subsequent responsive action taken by the relevant system administrator. Under operations issues which may involve corruption or compromise of the systems, self-healing autonomic computing qualities will equip Zero Trust systems with the ability to automatically correct the operational issues through systematic identification of security faults, as well as through end-to-end issue diagnosis and remedial action without any human intervention or any manual supervision.

R4 includes all the requirements on structural architecture and implementation methods of the distributed energy resource Zero Trust systems, yet the self-optimized autonomic computing systems could considerably help with adaptability-based properties by automatically managing the utilization of available computational resources as well as establishing easy communications with other systems to exchange operational data and security intelligence. Rahimi and Ipakchi (2010) state that distributed energy resource Zero Trust system can be made more adaptable and capable of real-time operations through using shared ontological frameworks enabling the comprehensive communication and knowledge sharing of security across the various energy operational systems and organizational environments.

The Full scalability and the ability to cope with large sets of energy networked nodes is the underlying issue in the requirement R5 of the distributed energy resource Zero Trust implementation. Ralston et al. (2007) argue that Zero Trust systems implemented in distributed energy resource applications are put to test in terms of the difficulty in being able to monitor all traffic belonging to the network communication in switched energy networks where there is so much operational traffic where a complex virtualized networking infrastructure need to be involved. This is an operational barrier which has encouraged the devising of novel means which would direct the analysis in a more holistic manner towards the end-point energy industries hosts that are networked with energy network access nodes, and this analytical orientation is quite evident in more recent cybersecurity-related literatures.

Nevertheless, the operationally most effective way of deploying host-based and network-based monitoring techniques and threat detection capabilities of the above is a combination thereof, which is however supported by relatively few cybersecurity technology vendors to date. It has been shown by Rose et al. (2020) that a comprehensive risk management methodology along with autonomic computing capabilities that feature all self-managing operational properties will be able to fulfil requirement R6 regarding deterministic performance attributes and operational reliability in distributed energy resource frameworks.

Autonomic computing solutions can have distributed energy resources Zero Trust systems with operational behaviors akin to nervous systems in biology that allows unconscious reflex action without the need of conscious ability and operator intercession, and this aspect is coupled with fault-tolerance features that help such systems provide functional continuity even when individual cybersecurity sensors fail. As stated by National Institute of Standards and Technology (2020), comprehensive ontological frameworks and mobile intelligent agent technologies can properly address the need of synchronization and secure message transfer between distributed energy resources Zero Trust components specified in the operational requirement R7, coordination of cybersecurity protection.

Mobile security agents are tailored in such a manner that they can work reliably even when part of the security information is missing because the distributed energy resource computing environments where they are operating are non-deterministic, complex, and dynamic, and there is no centralized system that controls the global information to maintain the integrity of security information and ensure that the operational activities are coordinated and synchronized. Roman (2021) states that hence communication abilities are significantly important so that security agents can communicate with each other to refer to sufficient threat intelligence, synch operational actions, synchronize security response actions, and manage complicated interdependencies across various cybersecurity elements dispersed across energy facilities networks.

Smart mobile security interoperability could effectively be accomplished through employing shared ontological structures and advanced scopes of interpretative knowledge that allow security agents to determine and organize their cybersecurity processes without actual loss of operational autonomy and independent decision-making capabilities. As presented by Ajiboye et al. (2021), these mobile security personnel can readily share vast security knowledge and threat intelligence that leverages common ontological frameworks to guarantee the coherent interpretation and, accordingly, proper response coordination in various operational contexts in the energy sector and cross-company entities.

Lastly, there is a need to systematically identify the fact that a balance needs to be kept comprehensive between the levels of security protection to energy systems and the performance of the system since there exist trade-off associations between the performance of energy systems and the effectiveness of energy security cybersecurity. Anderson and Fuloria (2010) have shown that Zero Trust implementations offering highly secured and trustworthy services in energy are usually using more detailed security patterns, detection rules and analysis algorithms and as such need extra assessment resources and network capacity to supply extra cybersecurity entrance of protection. Applying this operational consideration to distributed energy resource computing environments, both the combinational and communication computing resources available to energy customers and operation processes can be decreased when cyberspace protection systems need to utilize an unknown amount of the available computing resources on security watch and threat chasing operations.

Table 6 Comprehensive mapping of proposed implementation concepts to distributed energy resource Zero Trust operational requirements

Implementation Concepts	**Operational Requirements Addressed**							
	R1	R2	R3	R4	R5	R6	R7	R8
Autonomic Computing Self-Management	✓	P	✓	✓	P	✓	P	✓
Comprehensive Risk Management	P	✓	P	P	P	✓	P	P
Advanced Fuzzy Logic Theory	P	✓	✓	P	P	✓	P	P
Semantic Ontology Frameworks	✓	✓	P	✓	✓	P	✓	P

✓ = Fully addresses requirement, P = Partially addresses requirement

6. Conclusion and future research directions for zero trust energy cybersecurity implementations

In conclusion, this detailed research paper has provided structured taxonomy and state-of-the-art detailed analysis of Zero Trust Architecture application especially developed to protect cybersecurity in distributed energy resources to interest cybersecurity researchers and energy industry practitioners to explore comprehensive solutions to cyber threats detection and prevention in distributed energy computing environments. In accordance with Banerjee et al. (2011), major emphasis and efforts have been given to the specific peculiarities of distributed energy resources systems, and the contemporary issues plaguing their implementation that restrict the development of Zero Trust within the scope of energy infrastructure protection, and the means of providing the distributed energy resource system with comprehensive operational capabilities.

A methodical list of functional and technical specifications on complete distributed energy resource Zero Trust applications has not only been supplied, but four methodologies of effective cybersecurity systems have also been recognised namely, autonomic computing self-management capabilities, comprehensive ontological knowledge frameworks, new risk management techniques and better fuzzy logic driven theories to achieve optimal design options that addresses all operational specifications.

The study results show that such conventional defensive measures as perimeter-based cybersecurity cannot effectively defend contemporaries distributed energy resource systems because of their dynamic operational nature, heterogeneous technology implementation, and diverse interconnection demands that encompass various organisational and regulatory boundaries. Zero Trust Architecture is complex and is claimed to present solutions to these cybersecurity threats due to continuous verification, policy-based access control and micro-segmentation approaches, which can be effective in terms of protecting the distributed energy assets, as well as operational effectiveness and industry compliance with standards (Bertino and Islam, 2017).

Additional research work that needs to be done include the development of standard implementation guidelines, end-to-end assessment strategies, and deployment frameworks which will help the energy sector stakeholders to successfully apply Zero Trust cybersecurity protection in a widespread variety of distributed energy resource operating environments. Buck et al. (2015) further state that focus should be placed on creating affordable ways of implementing cyber security with a balance of both a protection focusses and economic costs on the side of the energy system operations, especially in smaller distributed forms of energy resources which may pose economic limitations, as well as own resources for cybersecurity.

The dynamic of the cyber threats against critical energy infrastructure necessitates the progressive nature of Zero Trust implementation practices and its extensive development with the increasingly emerging energy technologies, artificial intelligence, machine learning, blockchain, and additional advanced analytics solutions which can advance the energy system modernization efforts and simultaneously provide robust cybersecurity layers. Future research by Caralli et al. (2007) should additionally tackle the issue of interoperability necessitated by various Zero Trust implementations to achieve an all-inclusive cybersecurity coordination amid various energy utility associations, regulatory boards and Technology platforms that constitute the current interconnected system of energy infrastructure systems.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] National Institute of Standards and Technology. (2020). Zero Trust Architecture (NIST SP 800-207). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

[2] Roman, A. (2021). Pervasive and Zero-Trust approach for cyber protection and mitigation. U.S. Department of Energy. https://www.energy.gov/sites/default/files/2021-06/Roman%20Arutyunov-A1.pdf

[3] Ajiboye, M. T., Agyekum, E. O., and Frimpong, I. (2021). Overview of Zero Trust Architecture Trend and Advancement in Energy Systems. Journal of Information Engineering and Applications, 11(6), 12-25. https://www.iiste.org/Journals/index.php/JIEA/article/download/62976/65059

[4] Ritter, L., Röttinger, R., and Wenning, S. (2021). Zero Trust Architectures in the Energy Sector: Applications and Benefits. European Journal of Engineering and Technology, 9(1), 15-23. https://www.idpublications.org/wp-content/uploads/2024/06/Full-Paper-ZERO-TRUST-ARCHITECTURES-IN-THE-ENERGY-SECTOR-APPLICATIONS-AND-BENEFITS.pdf

[5] Newhouse, W., and Scarfone, K. (2020). Zero Trust Security Model for Critical Infrastructure Protection: Best Practices and Challenges (Special Publication 800-207). NIST. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

[6] Chaudhry, H., and Hydros, I. (2021). Policy-Driven Micro-Segmentation in Smart Grids Using Zero Trust Approaches. Energy Informatics, 4(2), 101-112. https://www.iiste.org/Journals/index.php/JIEA/article/download/62976/65059

[7] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys and Tutorials, 17(4), 2347-2376. http://dx.doi.org/10.1109/COMST.2015.2444095

[8] Anderson, R., and Fuloria, S. (2010). Security economics and critical national infrastructure. In Economics of Information Security and Privacy (pp. 55-66). Springer. http://dx.doi.org/10.1007/978-1-4419-6967-5_4

[9] Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., ... and Peacock, M. (2017). Future challenges for smart cities: Cyber-security and digital forensics. Digital Investigation, 22, 3-13. http://dx.doi.org/10.1016/j.diin.2017.06.015

[10] Banerjee, P., Friedrich, F., Bash, C., Goldsack, P., Huberman, B., Manley, J., ... and Veitch, A. (2011). Everything as a service: Powering the new information economy. Computer, 44(3), 36-43. http://dx.doi.org/10.1109/MC.2011.67

[11] Bekara, C. (2014). Security issues and challenges for the IoT-based smart grid. Procedia Computer Science, 34, 532-537. http://dx.doi.org/10.1016/j.procs.2014.07.064

[12] Bertino, E., and Islam, N. (2017). Botnets and internet of things security. Computer, 50(2), 76-79. http://dx.doi.org/10.1109/MC.2017.62

[13] Buck, C., Olenberger, C., Schweizer, A., Völter, F., and Eymann, T. (2015). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. Computers and Security, 110, 102436. http://dx.doi.org/10.1016/j.cose.2021.102436

[14] Caralli, R. A., Stevens, J. F., Young, L. R., and Wilson, W. R. (2007). Introducing OCTAVE Allegro: Improving the information security risk assessment process. Carnegie Mellon University Software Engineering Institute. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8419

[15] Cleveland, F. M. (2008). Cyber security issues for advanced metering infrastructure (AMI). In 2008 IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century (pp. 1-5). IEEE. http://dx.doi.org/10.1109/PES.2008.4596535

[16] Colwill, C. (2009). Human factors in information security: The insider threat–who can you trust these days? Information Security Technical Report, 14(4), 186-196. http://dx.doi.org/10.1016/j.istr.2010.04.004

[17] De Craemer, K., Vandael, S., Claessens, B., and Deconinck, G. (2014). An event-driven dual coordination mechanism for demand side management of PHEVs. IEEE Transactions on Smart Grid, 5(2), 751-760. http://dx.doi.org/10.1109/TSG.2013.2272197

[18] Deng, R., Xiao, G., Lu, R., Liang, H., and Vasilakos, A. V. (2017). False data injection on state estimation in power systems—attacks, impacts, and defense: A survey. IEEE Transactions on Industrial Informatics, 13(2), 411-423. http://dx.doi.org/10.1109/TII.2016.2614396

[19] Fang, X., Misra, S., Xue, G., and Yang, D. (2012). Smart grid—the new and improved power grid: A survey. IEEE Communications Surveys and Tutorials, 14(4), 944-980. http://dx.doi.org/10.1109/SURV.2011.101911.00087

[20] Farwell, J. P., and Rohozinski, R. (2011). Stuxnet and the future of cyber war. Survival, 53(1), 23-40. http://dx.doi.org/10.1080/00396338.2011.555586

[21] Forrester Research. (2010). No more chewy centers: Introducing the zero trust model of information security. Forrester Research Inc. http://www.forrester.com/report/No+More+Chewy+Centers+The+Zero+Trust+Model+Of+Information+Security/-/E-RES56682

[22] Burns, A., McDermid, J., and Dobson, J. (1992). On the meaning of safety and security. The Computer Journal, 35(1), 3-11. http://comjnl.oxfordjournals.org/content/35/1/3.full.pdf

[23] Kindervag, J. (2010). No more chewy centers: Introducing the zero trust model of information security. Forrester Research. http://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf

[24] Hahn, A., Ashok, A., Sridhar, S., and Govindarasu, M. (2013). Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. IEEE Transactions on Smart Grid, 4(2), 847-855. http://dx.doi.org/10.1109/TSG.2012.2226919

[25] Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. Computer Networks, 148, 283-294. http://dx.doi.org/10.1016/j.comnet.2018.11.025

[26] Humayed, A., Lin, J., Li, F., and Luo, B. (2017). Cyber-physical systems security—a survey. IEEE Internet of Things Journal, 4(6), 1802-1831. http://dx.doi.org/10.1109/JIOT.2017.2703172

[27] Jain, A. K., and Shanbhag, D. (2012). Addressing security and privacy risks in mobile applications. IT Professional, 14(5), 28-33. http://dx.doi.org/10.1109/MITP.2012.72

[28] Ralston, P. A., Graham, J. H., and Hieb, J. L. (2007). Cyber security risk assessment for SCADA and DCS networks. ISA Transactions, 46(4), 583-594. http://dx.doi.org/10.1016/j.isatra.2007.04.003

[29] Rahimi, F., and Ipakchi, A. (2010). Demand response as a market resource under the smart grid paradigm. IEEE Transactions on Smart Grid, 1(1), 82-88. http://dx.doi.org/10.1109/TSG.2010.2045906

[30] Patel, A., Taghavi, M., Bakhtiyari, K., and Celestino Júnior, J. (2013). An intrusion detection and prevention system in cloud computing: A systematic review. Journal of Network and Computer Applications, 36(1), 25-41. http://dx.doi.org/10.1016/j.jnca.2012.08.007

[31] NIST Framework. (2018). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. National Institute of Standards and Technology. http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[32] Mo, Y., Kim, T. H. J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., and Sinopoli, B. (2012). Cyber–physical security of a smart grid infrastructure. Proceedings of the IEEE, 100(1), 195-209. http://dx.doi.org/10.1109/JPROC.2011.2161428

[33] Mahmoud, R., Yousuf, T., Aloul, F., and Zualkernan, I. (2015). Internet of things (IoT) security: Current status, challenges and prospective measures. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 336-341). IEEE. http://dx.doi.org/10.1109/ICITST.2015.7412116

[34] Chen, J., Yan, J., Kemmeugne, A., Kassouf, M., and Debbabi, M. (2020). Cybersecurity of distributed energy resource systems in the smart grid: A survey. Applied Energy, 383, 125364.

[35] Liang, G., Weller, S. R., Zhao, J., Luo, F., and Dong, Z. Y. (2017). The 2015 Ukraine blackout: Implications for false data injection attacks. IEEE Transactions on Power Systems, 32(4), 3317-3318. http://dx.doi.org/10.1109/TPWRS.2016.2631891

[36] Kumar, P., Lin, Y., Bai, G., Paverd, A., Dong, J. S., and Martin, A. (2021). Smart grid metering networks: A survey on security, privacy and open research issues. IEEE Communications Surveys and Tutorials, 21(3), 2835-2888. http://dx.doi.org/10.1109/COMST.2019.2899354

[37] McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A. R., Maniatakos, M., and Karri, R. (2016). The cybersecurity landscape in industrial control systems. Proceedings of the IEEE, 104(5), 1039-1057. https://doi.org/10.1109/JPROC.2015.2512235

[38] Department of Energy. (2017). Electricity subsector cybersecurity capability maturity model (ES-C2M2). U.S. Department of Energy. https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

[39] Stouffer, K., Falco, J., and Scarfone, K. (2011). Guide to industrial control systems (ICS) security (NIST Special Publication 800-82 Rev. 2). National Institute of Standards and Technology. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[40] Rose, S., Borchert, O., Mitchell, S., and Connelly, S. (2020). Zero Trust Architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[41] Liu, Y., Ning, P., and Reiter, M. K. (2011). False data injection attacks against state estimation in electric power grids. ACM Transactions on Information and System Security, 14(1), 1-33. http://dx.doi.org/10.1145/1952982.1952995