Security Analysis of the Smart Grid Protocols

Author

Ohud Alsadi

Supervisor

Neetesh Saxena

Moderator

Shancang Li

A dissertation submitted in partial fulfillment of the requirements for the degree of:

Master of Cybersecurity

School of computer science and informatics

Cardiff University

Table of contents

Abstract

A smart grid is being called the "internet of energy" (Carter Sullivan 2020). It concerned with developing its own communication infrastructure in order to effectively interconnect its components and systems. This can only be done with efficient and essential protocols for seamless integration into its environment and interoperability between its applications and devices. This project will focus on analyzing the protocols applied in the smart grid, addressing the functions, security requirements, risks and proposed solutions. In addition to focusing on the management of energy flows and services in the smart grid through the use of communication protocols that allow interoperability of the smart grid. The purpose of the tool proposal is to make the integration of different protocols in one platform with other applications to meet consumer needs in energy monitoring. The proposed tool will be able to integrate protocols by choosing from more than one protocol based on the security requirements it provides in order to manage and monitor the energy flows of consumers and display the potential threat facing the consumer in its energy consumption page and provide a rapid response by choosing the appropriate action in addition to the presence of the protocols and updated.

Acknowledgment

First and foremost, I thank Allah for giving me the opportunity to complete this project.

I would like to express my sincere gratitude to my country, the Kingdom of Saudi Arabia, which gave me the opportunity to study and provided all the support I needed to complete my masters study.

I would also like to thank my supervisor (Dr. Neetesh), who gave me the opportunity to work on this project and helped me find answers to my questions and provided support and guidance.

Expressions of thanks do not fulfill the right of my family, especially my husband and children, thanks to their continuous support and unlimited encouragement, I was not able to complete the letter successfully

List of figures

List of Tables

List of abbreviations and Acronyms

SG	Smart Grid
DER	Distributed Energy Resources
NIST	National Institute of Standards and Technology
SM	Smart Meters
PQM	Power quality monitors
SM	Smart Meter
DA	Data Acquisition
DM	Data Management
SA	Substation automation
SAS	Substation automation systems
H/BA	Home/Building Automation
H/BAS	Home/Building Automation Systems
BAS	Building Automation Systems
DR	Demand Response
TLS	Transport Layer Security
CRC	Cyclic Redundancy Check
CA	Certificate Authorities
SHA	Secure Hash Algorithm
HMAC	Hash-based Message Authentication Codes
IEDs	Intelligent Electronic Devices
IDS	Intrusion Detection Systems
GUI	Graphical User Interface

Chapter 1: Introduction

1.1 Research Motivation

The global increase in industrial and commercial aspects has led to the emergence of many problems of shortages in energy supplies, which has made the world think about developing electricity grids from traditional grids to smart grids that are based on an electronically controlled system instead of a traditional electromechanically controlled system. It also makes the electricity industry more efficient than previously and provides the society with electricity in a safer and more sustainable way. The electricity network that provides energy to consumers is referred to as the "grid", while the integration of digital technologies with the electric power grid is called a smart grid (SG). However, the phrase "smart" refers to it having an internal operating system, scaling, and advanced processing capabilities (Khan et al. 2021).

Due to its ability to generate, transmit, and distribute renewable energy sources and electric vehicles, the SG is referred to as a "system of systems" (Pandey and Misra 2016). According to Mustafa (2015), the concept of the SG is an electrical network that has been enhanced with the capabilities of ICT to support electricity flows and two-way communication between network entities. Predictably, the use of bi-directional flows of electricity and information will improve the SG by providing it with smart features, such as customer involvement, self-healing and adaptive control and protection (Cintuglu et al. 2016). Because the SG uses advanced ICT to further improve its efficiency and provide environmental and economic benefits to the SG, so the increase in the number of devices and applications connected in the SG has led to the development of a variety of protocols that have become essential for network integration and the interoperability between devices and applications in the SG. This is because the protocol in general is a set of rules that permits two or more entities to exchange or transmit information and specifies what information is transmitted, when it is communicated, and how it will be communicated. SG-related protocols have been developed by several standards development organisations (SDOs): the International Electrotechnical Commission (IEC), the Institute of Electrical and Electronics

Engineers (IEEE), and the National Institute of Standards and Technology (NIST) (Kuzlu et al. 2017). However, although experts continue to develop SG systems and their protocols, the increase of SG size, and its expansion have led to an increase in attacks and the subsequent significant impact. Even though there are a number of protocols available for an SG in all of its systems, some problems and risks have remained a threat to achieving real-time security for SGs. Also, the abundance of protocols in SGs poses a compatibility challenge due to the heterogeneous nature of the SG. Thus, high-level computers exchange information with simple, low-power, low-computing devices. This leads to the emergence of vulnerabilities and security risks due to data aggregation in these devices, and one protocol cannot be fully translated into another protocol. In addition, denial-of-service attacks, which cause the grid's communication links to be interrupted or shut down, pose a risk to SGs. Therefore, attackers focus on discovering the vulnerabilities of these protocols and the challenges that hinder them in securing systems, so they should focus on analyzing the protocols and addressing their security vulnerabilities.

1.2 Research Statements

According to Yardley et al. (2013), NIST has spent a significant amount of time analysing the specifications for a number of crucial SG protocols, flagging up security and interoperability vulnerabilities for future correction. Because of this, the review process for SG protocols is useful, and, in terms of technique, is frequently comparable to reviewing any protocol as well as reviewing the system. Although there are updates and fixes for many of the protocols used in the SG, there is a complexity issue with new or recently established protocols that have not yet undergone any testing. Since the security of SGs attracted the interest of researchers and developers, they developed many protocols to solve some of the emerging problems. However, these protocols still do not fully address the security issues of SGs. Although some security mechanisms are implemented in smart devices and SG substations, the current security protocols used are not robust enough to resist several types of attacks (Zhang et al. 2016).

In order to improve the principle of cyber security in SG protocols, it is important that any attacks or vulnerabilities that have not been addressed in the applicable protocols are discovered and identified as soon as possible and that the most powerful preventive measures are chosen by improving these protocols or merging them with others in order to strengthen the system and reduce attacks in the future. Since information exchanged between SG devices and their utility servers may be vulnerable to man-in-the-middle attacks, replay, and impersonation, and can cause users' information to be modified and so affect their privacy, the security of SG communication protocols is the most important issue to protect this information from attacks.

1.3 Research Aims and Objectives

A number of protocols have been created as a result of the global adoption of the SG in order to make smart devices interoperable. These protocols cover the parts and operations of a power system. The purpose of this study is to provide a comprehensive analysis of the security aspects of protocols that are frequently used in an SG, starting with those related to the control centre, distributed generation, metering, demand response, and substations. In addition, it will investigate the comprehensive disclosure of security requirements and challenges that protocols still suffer from, and address the security risks in general in each of them.

Although there are other requirements to consider in order to provide security for an SG, securing and continually improving the protocols is in my opinion the most important task to secure the overall security of the SG as a whole, which is the desired goal of the research methodology.

Thus, the research objectives are as follows:

- to analyse the latest smart network protocols and identifying potential risks and weaknesses within these protocols
- to explore which security requirements the protocols contain and lack, and to provide security recommendations for the protocols selected to improve them.
- to investigate the proposed security tool through a platform that supports situational awareness for users in case of the event of a threat through monitoring the consumer’s energy usage.

1.4 Dissertation Outline

In addition to what was mentioned in this first chapter, this research is divided into six chapters. **Chapter 2,** provides an overview of the SG structure and of its systems and domains to pave the way for understanding the following chapters. In addition, it presents a security analysis of the protocols applied in SG platforms by mentioning the vulnerabilities and attacks of these protocols. Finally, the chapter gives a brief review of some research related to the improvement protocols applied in SGs. **Chapter 3** is concerned with presenting the chosen study methodology. **Chapter 4** represents the security requirements that are required to be met are explained. Furthermore, the proposed tool is presented. **Chapter 5** which is the Results and Evaluation, presents the security analysis of SG protocols by comparing the results obtained with the results of previous research and providing recommendations. **Chapter 6 ,** This chapter provides a conclusion and a summary of the findings in addition to available paths for possible future research.

Chapter 2: Background and Literature Review

2.1 Overview

This chapter is divided into three parts. The first part gives an overview of the components of an SG system's infrastructure, the SG subsystem, in order to facilitate an understanding of the following chapters. The second part discusses the current protocols used in SG systems from a cyber security perspective by discussing security risks, threats and vulnerabilities in protocols used, and the proposed solutions applied to overcome these attacks. Finally, previous works in the field of protocols proposed are presented.

2.2 SG systems and subsystems

2.2.1 Overview of SG systems

The SG is considered a power grid that is fully equipped with sensors connected in communication systems; these sensors function due to the latest information and signal processing technologies (Uddin et al. 2018) .

Smart energy, smart communications, and smart information systems are part of the smart infrastructure system. There are three main parts of the smart energy system, and these facilitate the bi-directional transmission of energy and information (energy generation grid, transmission grid, and distribution grid). The generation grid is responsible for the use of central power plants to produce electricity. After that, the generated electricity is escalated to the desired values using transformers and is then entered into the transmission grid, which in turn, delivers electricity to the distribution grids that contain a number of substations (Zhou et al. 2017).

2.2.2 SG subsystems:

The three sub-systems that make up the SG infrastructure are as follows (Sarwar and Asad 2016):

1) The smart energy subsystem

   This differs from the traditional power grid in that it is flexible enough to take in the energy share from the consumer side. As a result, the smart generation, transmission, and distribution components make up the core framework of the smart energy subsystem. For smart generation sectors, it includes the use of renewable energy, such as solar energy, wind, or hydropower. The distributed energy resources (DERs) are used in the SG smart generation system to reduce system capacity, boost reliability, and lower costs for centralised generating stations. The transmission network depends on improving the existing assets of overhead transmission lines, underground cables, substations, and transformers, to achieve minimum losses and maximum efficiency (Abdallah and El-Shennawy 2013). The last part of the smart energy subsystem is the smart distribution, which is the largest part of the power grid and is very important in the issue of the quality of energy provided to consumers.

2) The smart information subsystem

   This system is divided into two stages (Data Acquisition (DA) and Data Management (DM)). The first stage, DA, is done through smart meters or smart monitoring systems. Smart meters are put in customers' buildings to check the state of the system, to track their usage, and to collect diagnostic data, which may be sent to the control centre for invoicing and analysis. For smart monitoring systems, sensors are used; this is a crucial step in ensuring the system's security and ongoing operation. DM, on the other hand, strives to integrate, analyse, optimise, and process data obtained through data acquisition devices.

3) The smart communication subsystem.

   The communication network is the backbone of the SG architecture. Despite this, the needs and priorities of sub-systems in an SG differ according to their association with communication systems. It must be ensured that the communication between these systems is reliable and that privacy is guaranteed, whatever type of communication is used.

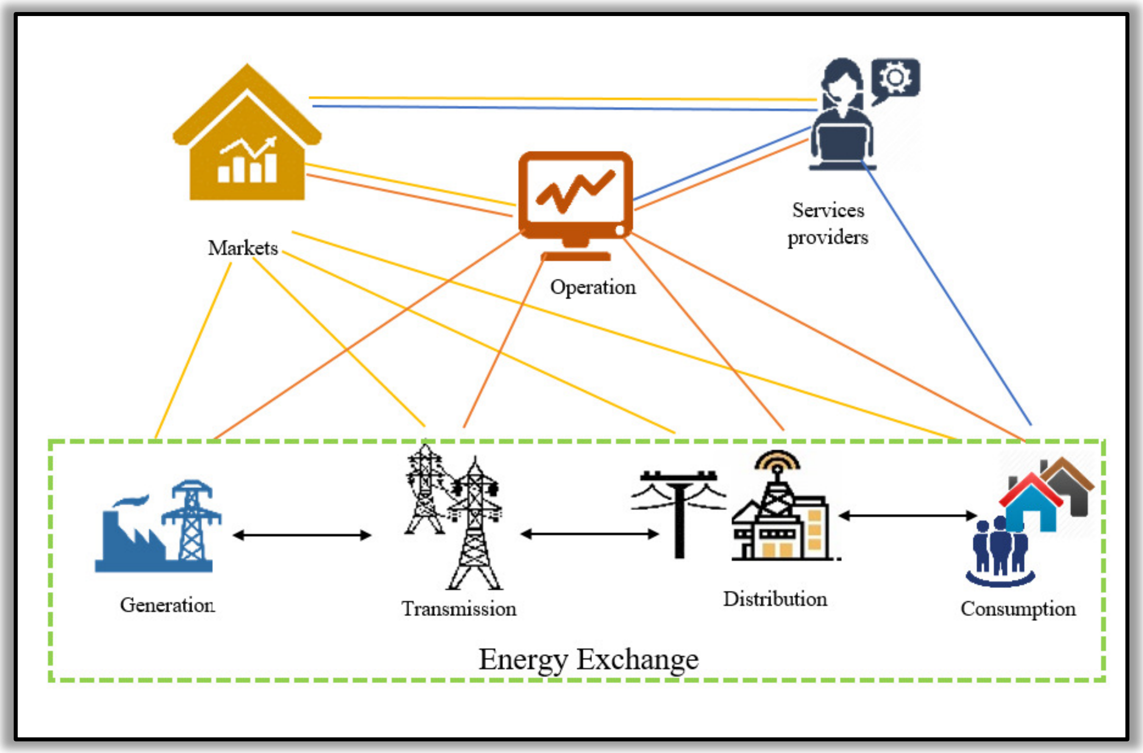


Figure 1: structure of SG, and energy exchange

2.3 SG domains

According to NIST (2014), the SG includes seven interconnected domains. Hardware, systems, or software can be found in each primary domain or sub-domain. The seven SG domains are shown in Figure 1. (Cintuglu et al. 2016) state the SG domains are :

1) Domain of the Consumer (customer): Consumers or end users are classified into three types: home, commercial, and industrial. Consumers may resort to changing their status from consumers to productive consumers who generate, store, and manage distributed energy as a result of the existence of the SG. Consumers are probably familiar with the physical cyber infrastructure of the SG as well as their actions and consequences in the grid.
2) Market Domain: This includes market management, aggregation, market operations, retail, and other related activities.
3) Domain of the Service Provider: Customer management, smart buildings, smart device installation, and utility bills in the SG are some of the most important applications of the service provider field.

4) Operational Area: This is the body responsible for both the safe and reliable operation of the power system. It contains energy management systems (EMS), which are responsible for the efficient functioning of power transmission level operations, while distribution management systems (DMS) are responsible for distribution level operations. This field also includes other operations, such as monitoring, control, protection, and analysis.
5) The Field of Bulk Generation: Through transmission lines, traditional large-scale energy is delivered, such as solar, nuclear, hydro, and thermal power plants, as well as wind farms, that interact within the field of transmission.
6) Transmission Domain: Regional transport operators or autonomous system operators (RTO/ISO) are responsible for the safe operation of the transmission domain. The energy generated in the bulk generating units is safely transferred to the distribution field via the transmission domain. Substations are the primary components in this field because they are responsible for reducing high voltage to the level of distribution through the electrical supply chain.
7) Distribution Domain: Its function is to connect the sending domains to the client domain. Loads, measuring points, small networks, and DERs are the most important components of this field.

2.4 SG protocols

SG systems, which use numerous protocols for each component of their systems, are complex. The growth of the SG and its fields makes it difficult to cover all the protocols in this paper. SG-related protocols have been developed by several SDOs, as mentioned earlier (Kuzlu et al. 2017). The commonly used protocols for SGs applications and domains are substation automation (SA) protocols (DNP3, Modbus, PROFIBUS), Home/Building Automation(H/BA) Protocols (BACnet, SEP 2.0) and Demand Response(DR) protocols (OpenADR, DRBizNet) that I will cover in this research. The protocols of these systems are designed to ensure reliability, accuracy, and efficiency in real-time operation.

The next sections of this chapter will be dedicated to searching for and comparing these protocols and choosing the best protocols from among these systems based on the security features they provide, taking into account the challenges and the biggest threats these protocols face.

2.4.1 SA Protocols

Systems for substation automation offer the distribution network and substation a high level of automation. Modern substation automation systems rely on interoperable protocols, Ethernet, and TCP/IP for communication across a common network backbone. To ensure the proper operation of substation automation systems, it is now necessary to take into account the security and dependability of communications.

- **Modbus**

Its use as a client or server to link the SCADA master station to the RTUs is among Modbus' most crucial applications. It was recently created to support Ethernet protocols and enable data transmission via TCP/IP networks. It is a protocol that is placed at level 7 of the OSI model and is an application-layer messaging protocol that is also used to achieve client-server communication between devices connected to the same network (Mohagheghi et al. 2009). It works on substation automation, industrial or building automation, and energy management.

- **DNP3**

These are industrial protocols that are used in SCADA systems for communication between SCADA base stations, Intelligent electronic devices (IED)s, and RTUs. The DNP3 protocol allows devices to share status data and automate substation management. Additionally, it offers the chance for quick transfers and time synchronisation. This protocol employs the IP group to send data messages that assist in controlling and monitoring the equipment at the electric power substation.

- **Profibus**

It is a "standard for fieldbus communication, used in industrial networks to support real-time command and control" (Watson et al. 2017). It is a master/slave protocol. This protocol links control units and automation systems with decentralized field devices. Two types of this protocol are in use (Profibus DP and Profibus PA), where DP stands for decentralized peripheral devices, which are used to operate sensors and actuators via a central console, and PA stands for process automation in which the protocol is used to monitor measuring equipment through the process control system (Bani-Ahmed et al. 2018).

- **IEC 61850**

The protocols based on IEC 61850 are dependent on implementing protection, control, and monitoring applications in distribution substations, and they rely on two TCP/IP protocols as part of their protocol suites (Falvo et al. 2013). The IEC 61850 protocol, which was approved in Europe and has features and capabilities similar to DNP3, has been used in this study. Additionally, this standard proposes using a local Ethernet network (LAN) to connect the substation automation equipment made by various manufacturers. Falvo et al. (2013) also stated that this LAN has gained widespread acceptance as part of the smart network for the transfer of data between smart electronic devices in power substations. The use of a direct data interchange between devices over the existing station bus and the ease with which TCP/IP and Ethernet technologies may be used to simply provide communications infrastructure are two benefits of IEC 61850 standard protocols.

2.4.2 H/BA Protocols

Automation of buildings and homes refers to the use of devices that can be managed and watched over by the home's technical systems. Utilising both wired and wireless technologies, systems are managed and monitored through two-way communications. Additionally, because this method makes a substantial contribution to energy conservation, it allows users the opportunity to manage their energy use in accordance with pricing and demand. Sensors, intelligent modules, actuators, and control units make up home and building automation.

- **SEP 2.0**

This is an interoperable protocol for connecting power devices to the network in a home environment. The HomePlug Alliance and Zigbee Alliance contributed to the creation of this protocol (Albano et al. 2014). It was initially released as Zigbee SE 1.x, which had simple and restricted security services and features. However, it was later improved and refined to SEP 2.0, which is an application layer protocol and is built on top of the Internet Protocol (IP) stack. Albano et al. (2014) also stated that this protocol supports HAN network gateways which have added new services, such as pricing information, user information, metering, programmable communication thermostat (PCT), load control, home displays (IHD), and more.

- **BACnet**

The Building Automation Control network, or BACnet, is a global standard for BACS communication (Hong et al. 2014). It is a communication protocol that promotes the interoperability of management, control, and building automation systems. Additionally, it offers data for applications involving building automation, including information on how to regulate lighting, ventilation, heating, and air conditioning. The goal is to specify data communication services and protocols for computer equipment used to monitor and control heating, ventilation, air conditioning, and refrigeration (HVAC&R) and other building systems, as well as to specify object-oriented representation of data transmitted between those devices (Tariq et al. 2012).

2.4.3 DR protocols

It is a mechanism used by utilities to achieve stability and balance in the SG. Demand response systems are used by customers, as they send alert signals to reduce their use of electricity during peak times.

- **OpenADR**

It is an open industry standard protocol for exchanging data between utilities or between electrical service providers and their customers. Based on the OASIS Energy Operation Standard, the OpenADR Alliance has developed product profile specifications (Ebeid et al. 2015). It also specifies the syntax and information contained in messages used in DR and DER, including emergency signals, dependability, regeneration status, and pricing signals, as well as the name, status, and identity of the event. This protocol is operated by DR service providers and clients, which are called Virtual Nodes (VENs). These virtual nodes are gateways whose job it is to control devices.

- **DRBizNet**

This is a versatile DR management system that employs distributed business process integration techniques in an SG environment to simplify and enable effective DR programs.

2.5 Literature Review

To accomplish the goals of the research, three areas were emphasised: analysing state of the art SG protocols, functions and security requirements in these protocols, and challenges protocols that still face. Then, potential risks and vulnerabilities within these protocols are identified and the proposed solutions to overcome these issues are discussed. Finally, there is an exploration of how to develop these protocols by adding improvements or security mechanisms to them and upgrading them, as well as the proposed related systems or tools.

2.5.1 Analysis Methods of SG Protocols

Many researchers in the field of protocols have used mechanisms to examine and test the effectiveness of their level of safety. Some of these mechanisms will be discussed in this section. For example, Yardley et al. (2013) suggested a mechanism that is a series of steps through the division of the system, and each component in the system is evaluated. The system is divided into interfaces, logic, protocols, and environment. Then, systematic steps are taken for the security review, which are as follows: first, collecting the system designs; defining the components of the system and the protocols applied in it and the environment in which it operates; third, collecting the specifications of the protocols in the system under test; fourth, evaluating the potential inputs and outputs in the system; fifth, analysing the data flow diagrams in the system; sixth, identifying threats to the system and its protocols; and seventh, evaluating the use of security controls. There are now many simulation and modelling methods for analysing protocols and evaluating the interaction between cyber infrastructure and power systems. Barenghi et al. (2012) proposed the idea of making tables for analysis by displaying the actors and assets (elements of the SG) involved in the usage and security management to analyse the security of the SG and all those who refer to the assets as one or more threats. Their idea is based on two steps. The first step is to identify assets and security from different perspectives through security analysis using validation using security tools. The second step is to analyse the class of attacks targeting the assets. In addition, there is another method proposed by Hahn et al. (2013) which is called the Testbeds; it is an effective tool used to test the algorithms and protocols of the smart network. Due to the nature of the network's complexity and its multifunctionality, the construction of electronic physical Testbeds for the experimental verification of SG protocols is also required. To do this, platforms for testing cyber-physical systems reliably assess the principles, architecture, and flaws of the SG (Cintuglu et al. 2016; Hahn et al. 2013). Real-time digital simulators are being utilised by various SG entities to create, analyse, and test cyber-physical components for electrical power systems on an increasing number of "hardware-in-the-loop test platforms" (Lauss et al. 2015). Wang and Lu (2013) conducted a comprehensive study and used a survey to cover the challenges in the smart network and its protocols. Their study was based on analysing security vulnerabilities through case studies, discussing attacks, and designing effective protocols for the smart network to achieve secure information delivery.

The method used in analysing protocols in this research is to first address the functions and security requirements of these protocols and then mention the challenges that are still encountered as shown in Table 1,2,3

2.5.1.1 Challenges on Protocols

Although there are many different communication protocols used in the SG, security was not initially considered when these protocols were being developed. However, since the SG system is currently connected to the Internet, efforts are being made by organisations like NIST and IEEE to incorporate security into the established protocols as new standards to protect the system from known threats. They will incur more costs because they will need to adjust many parameters in order to incorporate security into the protocols. Many researchers have also given more attention to specific protocols for individualized communications between various SG elements than they have given to the integration of protocols for compatible communication among themselves. Also, most of the protocols applied in the field of industrial systems and substation automation lack certain security measures, such as VPN encryption, authorisation, authentication, and firewalls. Commonly used protocols, like DNP3 or Modbus, do not have any built-in security mechanisms, therefore exposing the system to the public network; this could occur through improper system deployment, or the exploitation of a vulnerability could allow unauthorised parties to take control of the asset (Ferst et al. 2018). Solid efforts have been made to secure the infrastructure for these protocols, as happened with the DNP3 protocol, as authentication, known as Secure DNP3, was introduced into it. Tawde et al. (2015) discussed how although IEC 61850 is an open standard protocol, it is designed to solve equipment interoperability issues, and safety issues are not considered due to its lack of authentication in communication and because confidentiality and integrity are not guaranteed. On the other hand, because SEP 2.0 and OpenADR use the Transport Layer Security (TLS) protocol to provide message encryption and authentication, this method poses a challenge due to the complexity of TLS protocols and the vulnerabilities they contain.

The complexity and additional cost of secure versions of industrial protocols also make their implementation difficult. Therefore, we give part of our attention in this research to cover the challenges they still face as mentioned in (see Tables 4, 5, and 6).

Table 1. SA protocols

Protocol	Functions for protocols	Security features
Modbus	• It connects smart devices to powerline communication (PLC) by use of a simple master / follower concept (Drias et al. 2015). • It allows the controllers to communicate with one another and with other industrial devices. • It responds to incoming requests from other devices, detects errors, and logs them (Ma et al. 2020). • It allows the creation of a LAN connection.	• Modbus itself does not include any security specifications to provide confidentiality, authorisation, integrity, or encryption. As Parian et al. (2020) stated, "The Modbus protocol itself does not have any capability to handle these functions either"; therefore, integrating the TLS protocol with the traditional Modbus protocol adds authentication and message integrity protection features to Modbus.
DNP3	• It delivers measurement data from the client or an external station to the main server located in the control centre.	• It offers reliabilities of DNP3 due to the regular usage of cyclic redundancy check (CRC) for any exchange between master and slaves (Drias et al. 2015). • It reliably sends relatively small packets of data while ensuring that messages contained in a deterministic sequence arrive (Mohagheghi et al. 2009).
Profibus	• It facilitates communication between controllers/control systems and field sensors. • It offers quick production and cost effectiveness in operations, manufacturing, and building automation.	• It offers high levels of operational reliability and plant availability as well as high investment insurance without having any adverse impacts (Watson et al. 2017).

IEC 61850	• It maps time-sensitive messages from the application layer to the link layer directly to cut down on processing time (Lu et al. 2010). • It describes how the connection should operate between RTU-IED.	• Among the security features it implements is the use of message encryption.

Table 2. SA protocols challenges

protocol	Challenges
Modbus	• It sends messages to target devices using TCP/IP over the Internet, and suffers from vulnerabilities such as IP validation attacks and others (Shahzad et al. 2015). Therefore, Modbus TLS is not an ideal solution due to the lack of security for messages sent over the IP protocol. Also, TLS is an expensive solution.
DNP3	(Crain and Bratus 2015) discussed the challenges this protocol contains which are as follows: • The protocol is complicated because of the way the event data transfer is carried out using the server-side state. • More additional messages, such as confirmations, are required to keep things in sync.
Profibus	• There is a lack of control over authorisation and authentication. • There are concerns with protocol installation quality or failure, such as the effect of long cable issues or the lack of operational bus stations on the stability of the protocol installation (Mossin and Brandão 2012).
IEC 61850	• This standard does not recommend any particular structure and therefore does not address the problems and difficulties related to system expansion in the standard, and in the case of increased energy demand, power substations should be expanded. Therefore, issues related to the expansion of this regime must first be addressed during the planning stage (Sidhu et al. 2008).

Table 3. H/BA protocols

Protocol	Functions for protocols	Security features
SEP 2.0	• It controls the load, and responds to demand and pricing in order to inform consumers of electricity tariffs, prepare bills, and finally prepay for user payment support for services (Albano et al. 2014).	• It supports authentication (X509. Digital Certificates) and encryption (TLS and AES-128). • SEP-enabled devices use ellipsoidal curved ciphers and TLS to provide message encryption and authentication (Upreti et al. 2019; Qi et al. 2016).
BACnet	It provides real-time monitoring and controlling of building facilities while effectively managing building systems by collecting, processing and storing data about the facility (Park and Hong 2010).	• It applies encryption technology (AES256). • Event-based mechanisms are used by alarm and event services to alert subscribers to altered circumstances or alarm states (Nast et al. 2019).

Table 4. H/BA challenges

Protocol	Challenges
SEP 2.0	• Since this protocol employs encryption and authentication techniques, encryption protocols frequently require periodic updates to counter new attacks (Qi et al. 2016). • Furthermore, TLS has a long history of critical vulnerabilities due to the complexity of its protocols.
BACnet	• There is a lack of authentication because a feature called BBMD (BACnet Broadcast Management Device) makes it possible to connect to BACnet via Ethernet or IP and access subdevices, meaning BACnet devices can connect to the Internet without the need for authentication. Thus, BBMD can be enabled to control BACnet through this feature (Ciholas et al. 2019).

Table 5. DR protocols

Protocol	Functions for protocols	Security features
(OpenADR)	• It enables service providers/ consumers to exchange DR requests based on price and reliability criteria. • It transfers only the demand of the utilities' requests (McParland 2011). • Also, Carr et al. (2017) emphasized that using this protocol makes it possible to communicate price information that indicates congestion, unplanned outages, and periods of high demand to retail consumers.	• TLS is mandatory in the OpenADR transport layer. • Furthermore, OpenADR authentication depends on trusted certificate authorities (CA) (Garofalaki et al. 2022; Yassine 2016).
DRBizNet	• It has the ability to control any smart device type, including load controllers, thermostats, and power management systems (Cali et al. 2021a). • It offers effective real-time communication, lower cost, deadline monitoring, and faster operation.	• It provides its customers with automatic alerts and notifications (Cali et al. 2021a).

Table 6. DR protocols challenges

Protocol	Challenges
OpenADR	• It forces the use of TLS for client authentication, which leads to the need for public and private keys and trusted digital certificates. It pushes vendors to manage and issue certificates for each device and uses authentication and confidentiality to communicate with end devices. However, these security requirements are not used by vendors, which can expose the system to threats (Herberg et al. 2014).
DRBizNet	Engel and Hinkle (2004) and Yee (2006) discuss several challenges: • Many of the requirements of current DR software cannot be met because the data flow planning capabilities that are now available are insufficient. • Developing new generation resources and related transportation needs is costly.

2.5.2 Risks and vulnerabilities in protocols and proposed solutions

The SG depends on communication and information systems. This has led to an urgent need for a communication environment that facilitates the secure transfer of information between SG entities. However, the applicable communications protocols are still vulnerable to man-in-the-middle attacks, replay attacks, spyware, denial of service attacks, and others. The attacker takes advantage of the communication protocols by infiltrating the communication networks and tampering and falsifying the contents of the client's data, thus leading to a disturbance in the functions of the system. In some attacks, the attacker's purpose is to exploit types of data, such as data collected from sensors. For example, an attacker might tamper with the parameters of the power system located in the remote terminals. In Modbus, the lack of authentication causes servers to execute packets without authenticating them, which represents a serious threat to them because they treat the packet as if it were from an authorized client. In addition, the data is transmitted in plain text without encryption, and this leads to the risk of an attacker capturing network addresses. The fact that the protocols used in SG systems cannot support encryption technology puts them at risk of eavesdropping and sniffing attacks, which could compromise communication between one of the main and dependent smart network components (Wermann et al. 2016). The attacker can utilize the information they have obtained from sniffing and eavesdropping assaults to calculate the amount of power used by a specific section of the network, which could result in a power outage. Additionally, the majority of protocols in use lack authentication, which forces attackers to take advantage of this vulnerability by faking messages and sending them to a particular component to halt or restart it.

Since the DNP3 protocol does not yet provide authentication, an intruder can enter the conversation at the outstation to confuse or disable the connection, establish a connection to the control network, sniff DNP3 network packets, and modify them to perform replay attacks. For Profibus attacks, the lack of any authentication mechanism allows the attacker to create a false master node that can take control of the entire system network. Furthermore, the attacker is able to access the main controller, where they can write to and alter data, keep track of network connections, and intercept commands. Regarding IEC 61850, an attacker can decrypt passwords on application-level services such as protocols (Hypertext Transfer Protocol, FTP) on IEDs because the protocol lacks an encryption mechanism. Also, an attacker can run a malicious application that captures messages, alters them, and re-injects them into GOOSE because GOOSE packets are sent unencrypted in a plain-text over Ethernet and TCP/IP protocols, and this point is exploited by the attacker (Volkova et al. 2019). Also, information is distributed between devices in Ethernet frames, such as TSN, which can be easily sniffed or altered (Lázaro et al. 2021). Since BACnet usually uses LANs, an attacker can interact with BACnet devices within the network by sending messages to them and getting responses from them and so gain physical access to the control room in which the BACnet devices are located. So if a BACnet device is hacked, it will become a local network attacker (Esquivel-Vargas et al. 2017). Also, anyone can get the standard and learn how to create a device that can communicate and interact with BACnet devices on the network (Yimer et al. 2022). In SEP 2.0, an attacker can determine the total electricity usage to know whether or not consumers are at home by listening in on network traffic, performing a brute force attack, and stealing this information from the EMS to which the smart metre delivers this information. In the OpenADR protocol, the attacker launches tampering and eavesdropping attacks using network scanning tools to study the events of DR systems and to obtain private client information, for example, geographic location, device ID, and power consumption (Paranjpe 2011). Through tools like a protocol analyser, an attacker can eavesdrop on packet transmission over the network and scan packets for malicious activity, such as changing DR events, gathering source and destination information, replaying messages, or injecting phoney DR events. As for DRBizNet, it has complex relationships with energy service providers because of its open structure, which follows a policy of double service entry; this affects customers in tracking their data and making sure that the parties store and protect their data well (Subrahmanyam et al. 2005).

One of the solutions to prevent the presence of these attacks may be to add authentication or encryption mechanisms to the SG protocols. There was a necessity to implement authentication mechanisms, as it is one of the most urgent requirements in order to reduce security threats in the SG and provide a safe and reliable escort to power supply lines (Badar et al. 2021). However, although encryption mechanisms have been developed over the years, they may be difficult to add and implement in some protocols. This is because, as discussed by Reda et al. (2021), encryption techniques are subject to limited computational capabilities.

More details are available in Tables 4, 5, and 6 about each protocol and the danger or attacks that affect it, and the solutions researchers have proposed that prove their effectiveness in repelling these attacks.

Table 7. SAS protocols - attacks and security mitigation

Protocols	Attacks/threats/vulnerabilities	Solution proposed
Modbus	• A packet is authorized without being authenticated. • It transmits data packets in plain text form without an encryption (Phillips et al. 2020). • It captures network addresses. • It is subject to flooding attacks	• TLS protocol, which is "a protocol that provides communications security over the Internet" is suggested to solve this problem and ensure the confidentiality and security of data transmission (Ferst et al. 2018). • To ensure the authenticity of sent messages and to resist man-in-the-middle attacks, a Modbus TCP solution can be adopted that integrates the functionality of a Trusted Platform Module (TPM) (Tidrea et al. 2019). • An Intrusion Detection System (IDS) mechanism can be used.
DNP3	• Attacks can be replayed to confuse or disrupt the connection, establish a connection to the control network, and sniff DNP3 network packets. • Attackers can spoof normal relays due to the DNP3 protocol's lack of authentication.	Radoglou-Grammatikis et al. (2020) proposed a system called DIDEROT (Dnp3 Intrusion Detection for Ventilation System), which offers IDPS based on machine learning (ML) and is capable of identifying and preventing cyber threats . It contains two layers of threat detection: 1. intrusion detection using ML to identify DNP3 attacks, and 2. anomaly detection by determining whether the error in DNP3 was caused by an electrical disturbance or a security violation.

Profibus	- The fundamental reason for Profibus vulnerabilities is the absence of an authentication method for each connected device. A false master node can be created by an attacker and used to control the entire network.	- Isolating all segments of the protocol network can ensure that penetration of a master node in a segment of the network will not lead to penetration of the rest of the nodes or affect them (Pricop 2015). - Treytl et al. (2004) recommended using IPSec over the PROFIBUS protocol because IPSec contains two mechanisms for securing protocols, Authentication Header (AH) and Encapsulated Security Payload (ESP), which support authentication, confidentiality, and integrity.
IEC 61850	- Decrypts passwords on application-level services - Captures messages - Sniffs alters information distributed between Ethernet frames - Interoperability issues and safety issues are not considered due to its lack of authentication in communication - Message encryption lacks integrity checks and an authentication mechanism	- Early warning function in the event of detecting abnormal behaviour (Zhang 2017, Jing et al. 2015 and Hou et al. 2016). - Zhang (2017) also designed a system that detects Internet communications for smart substations by analysing the message, judging the type of message, and finally reporting anomalies if any. - Using a new kind of physical firewall called Waterfall Unidirectional Security Gateway to stop intruders from getting into the substation (Lázaro et al. 2021).

Table 8. H/BA protocols - attacks and security mitigation

Protocols	Attacks/threats/vulnerabilities	Solution proposed
BACnet	- Gains physical access to the control room in which the BACnet devices are located - Impersonates any device in BACnet	- Usage of IPSec, Kerberos, or both for authentication and encryption services.

SEP 2.0	- Listens in on network traffic, performing a brute force attack, and stealing users' consumption information	Using detection tools that monitor network traffic between the smart meter and sensor nodes to analyse and compare this traffic in order to detect normal behaviour based on system specifications and the aberration-based approach to identifying the attack (Jokar and Leung 2016).

Table 9. (DR) protocols - Attacks and security mitigation

Protocols	Attacks/threats/vulnerabilities	Solution proposed
OpenADR	Eavesdropping, data manipulation, message replay	(Yassine 2016) state: - The Transport Layer Security (TLS) protocol that OpenADR uses to send messages requires client authentication in order to perform mutual authentication. - Public/private key pairs and digital certificates issued by a trusted certificate authority (CA) are required for all nodes. - Peers must be able to use digital certificates to authenticate each other during communication.
DRBizNet	- Because it is seen as a structure, an open architecture, and a distributed communications network, this opens up problems related to privacy and security because it is necessary to understand where consumer data and records are stored. - It is also difficult to track customer data because it has complex relationships with energy service providers (Subrahmanyam et al. (2005).	In fact, there was no proposed solution to the problem of the DNP protocol, However it is possible to use blockchain technology because it helps track the flow of data and secure where its storage and prevent its tampering.

2.5.3 Development of Protocols and Related Tool

2.5.3.1 Improvements and Development of Protocols

Several researchers have published articles looking at the protocols used in SGs through analysis of the implemented protocols and making improvements to them. Majdalawieh et al. (2005) are one such research team that has enhanced the DNP3 protocol by creating a new extension to it called DNPSec. It is an authentication mechanism based on the HMAC encryption mechanism to ensure and protect messages sent between stations in a secure form by providing security features such as service availability, data origin authentication and integrity (Amoah 2016). They also discuss how DNP3-SA employs the SHA-HMAC (Secure Hash Algorithm) and AES-GMAC HMAC algorithms (Advanced Encryption Standard-Galois Message Authentication Code). The significance of this new protocol lies in its ability to address the security challenges faced by the DNP3 protocol, including issues with authentication, command integrity, and non-repudiation. In contrast, Modbus has the Encapsulated Protocol Identifier, HMAC Algorithm Identifier, HMAC Hash Length Identifier, and HMAC Hash value; these are the four parts that make up the ModbusSec security layer (Haye and El-Khatib 2013). ModbusSec, an upgraded protocol, offers a way to verify the integrity and assurance of message delivery utilising HMAC technology while enabling devices to mutually authenticate. The IEC 62351-6-part standard is created for the IEC 61850 protocol to address its cybersecurity issues and needs. Since GOOSE and SV messages transmitted via IEC 61850 carry time-critical power system messages and measurement messages respectively, researchers took great care to secure them and used the IEC 62351-6 standard to contain RSA-based digital signatures (Ustun and Hussain 2020). The proposed extension of the BACnet protocol is BACnet/SC. This new extension supports the secure transmission of messages using the IP Application protocol. It also uses IP networks without the need for a VPN. It provides a 128-bit and 256-bit elliptical curve authentication and encryption mechanism (Fisher et al. 2019). Originally, the SEP protocol was introduced as the Zigbee SE 1.x protocol, as it is simple and limited to the services it provides and the security features it supports. But SEP 2.0 is now an improvement of ZigBee SE 1.x with additional services (Cali et al. 2021). Narayan (2020) discussed how the OpenADR protocol version 1 was developed to provide scalability for demand response, and communication problem solving. The new version, OpenADR 2.0, has many advantages such as network reliability and the use of transactional semaphores using a client-server model to transfer information rather than a network-based control architecture.

Table 10 summarizes the issues addressed in this section regarding the improvements of the protocols by the additions to or recent versions of them.

Table 10. The improvements of protocols

Protocol	Improvement version	What are new adds to the protocol?
DNP3	• DNP3 Secure Authentication(DNP3-SA) and DNPSec	(Lee et al. (2014) and Volkova et al. (2019) emphasized the following elements: • Supports symmetric and asymmetric encryption • Offers complete confidentiality and authentication for multiple users in one device • Provides integrity and authentication by using SHA-2 hashing and the Challenge response HMAC. DNPSec: • It successfully offers integrity, authenticity, and confidentiality. • Security is provided by using the Triple Data Encryption Standard (3-DES) • Hash-based Message Authentication Code (HMAC) SHA-1.
Modbus	• ModbusSec by using hash-based message authentication codes (HMAC)	Hayes and El-Khatib (2013) argued that is • gives security and integrity of packets to the protocol • provides authentication mechanisms • reduces the computational burden of packets • checks the content of protocol messages without encrypting the message content
Profibus	The two versions of PROFIBUS are PROFIBUS DP and PROFIBUS PA. One of the two most widely used variations is PROFIBUS DP. Because of this, many experts define it as the industry-standard PROFIBUS.	• plug and play located in centrally, high data speed, low connection fees, and quick data transfer. • saves installation and cabling costs, as well as ensuring compatibility with devices from different manufacturers.

IEC61850	IEC 62351 Standard	• (Lazaro et al. 2021) state: • The international standardisation community worked to compile security solutions and improvements in automation systems for the power system field into IEC 62351 standard because IEC 61850 did not focus on security (Lazaro et al. 2021). • The use of digital signatures to certify data transmission is one of its additions. The TLS introduces it and specifies encryption techniques.
BACnet	BACnet Secure Connect (BACnet/SC)	• adds an encryption mechanism to protocol communications • ensures that there is authentication through certificates • unlike BACnet / IP, does not need static IP addresses
Sep 2.0	SEP 2.0, based on Zigbee Smart Energy 1.X	(Ingram et al. 2021) state : • mainly supports Wi-Fi, Bluetooth, broadband, and Ethernet • works with TCP/IP and User Datagram Protocol (UDP) protocols. • supports IPv4 and IPv6 • makes client server connections through HTTPS • addresses encryption, authentication, and authorisation requirements that some protocols lack.
OpenADR	OpenADR, version 2.0	• x.509v3 certificates for the client and server, and uses TLS 1.2 with SHA256. Also Herberg et al. (2014) discussed how it • manages peak demand by utilities, service providers and network operators, thus reducing DR cost and customer dependency.

		• avoids interoperability issues, so customers will be able to choose their devices from any vendor because the devices are certified by OpenADR, so the customer will trust any device as long as it complies with the standard. • ensures all nodes are equipped with certified and trusted digital certificates and public and private key pairs

2.5.3.2 The related tools and systems

As for the proposed tool, there are many studies that were in the same field. Fore example, Olivares et al. (2014) suggested the application of energy integration using sustainable energy sources, and this will increase energy efficiency in all sub sectors of the system by integrating advanced and smart technologies in the SG for energy control and management. In order to improve the efficiency response to the energy demand of the SG, Aladdin et al. (2020) suggested developing a multi-factor reinforcement learning model (MARLA-SG), which aims to manage smart demand so that the SG adapts to changes at all times. Their model operations are based on Q-Learning and State-Reward-State-Action (SARSA) schemes, which will lower their peak-to-average ratio (PAR) and lower their cost; this is the main goal of this type of scheme for energy in grid smart. Additionally, De Arajo et al. (2018) proposed a model that transfers data between the control centre in the power substation and the electrical equipment in SGs by using Zigbee-based WSN as a communication protocol link, since the electrical devices contain a sensor node that executes an intermediary programme that displays experiments with energy metres and obtains a history of energy consumption for the customer. This model demonstrates that interoperability is completed quickly and safely, and any new sensor can be configured. Given the security risks present due to the protocols lacking some security requirements, Kumar et al. (2019) proposed an authentication protocol based on an elliptical curve for authentication in order to manage the demand response in SG systems. Nonetheless, this proposal has several shortcomings, as confirmed by Yu et al. (2020), which show that this scheme cannot withstand various attacks, such as masquerade attacks and revealing the session key, and so it does not guarantee mutual authentication. All these reasons prompted them to propose an authentication system that preserves the privacy of users in managing the request response in smart network environments. Yu et al. (2020) asserted that their proposed protocol is more resistant to masquerading, replay, and session key disclosure attacks, as well as achieving anonymity, using XOR and hash operations. Regarding control of the user's consumption, many resources and studies proposed tools or systems for monitoring energy use. For example, Han et al. (2011) proposed an HEMS system based on comparing energy consumption with the reference energy level in the energy portal server. The idea of the proposed system is that if the consumer exceeds their consumption, the system converts the devices into an effective period of time so that the price per kilowatt is low.

2.6 Summary

Although the subject of the research is broad, the literature review has covered many aspects of the research. First, the protocols in SG systems, their functions, and the security requirements they provide, as well as the challenges that they still encounter, were discussed. Secondly, the dangers these protocols face were mentioned and there was an exploration of what solutions suggested by previous research would be effective to mitigate these risks. Third, improvements made to and new versions of the protocols are mentioned in this chapter as well. Finally, the previous systems and suggested tools were discussed.

Chapter 3: Methodology

3.1Overview

The research methodology explains the objectives of the study and identifies the requirements that fit the needs of the research. Thus, this chapter explains in detail the research methodology that was applied to achieve the objectives of the current study.

3.2Research approach

In order to plan how the project will be implemented, a methodology is needed to define the stages of project implementation. As Iacono et al. (2009) emphasized, the term 'methodology' refers to how methods are used in a research design to help distinguish between methods and outcomes. It includes clear objectives, explores ways to collect resources, identifies the constraints the research faces, and discusses the problems it will address. Therefore, in this research, a comprehensive study was conducted to understand and analyse the problem and to finally answer the research questions established earlier. A four-stage research methodology was followed, which included **understanding**, **planning**, and **analysing** to **reviewing the results**.

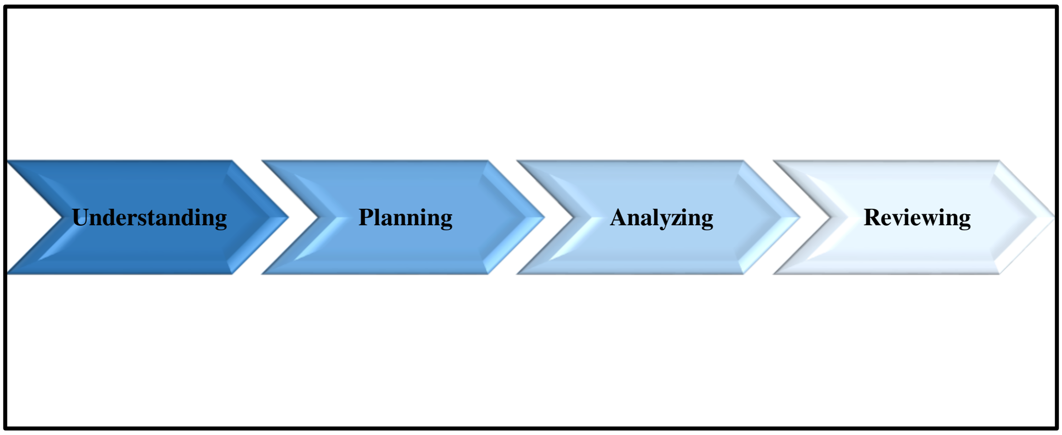


Figure 2. research stages

3.2.1 Understanding: At the beginning of the methodology, it was necessary to understand the entire project structure, and this was done by understanding the terminology related to the project, for example, "smart grid", "protocols", the structure of the SG and its seven domains, its systems and sub-systems, vulnerabilities related to protocols, security gaps, and the challenges that the protocols face. With this approach, data were collected, and aspects of the project were understood using secure digital libraries such as Cardiff University Library, IEEE Xplore, and Science Direct.

3.2.2 Planning: For the second stage, a plan was prepared by collecting the information that was sought in libraries about the field of research, drawing a model for the structure of SGs and defining the systems whose protocols would be addressed, specifically, substation automation protocols (DNP3, Modbus, PROFIBUS), Home/Building Automation Protocols (BACnet, SEP 2.0), and distributed resources and request response protocols (OpenADR, DRBizNet), and preparing tables for the important protocols to facilitate comparison among them.

3.2.3 Analysing: The third stage is the stage of **analysis** and implementation of the plan prepared in the previous stage

3.2.4 Review and verify: This stage involves reviewing and verifying what was accomplished in the protocol analysis by carefully examining what has been done in the protocols, and what has not been done in their implementation, as this makes it possible to predict the strategy that should be used to solve the future problems of SG protocols.

3.3 Waterfall development model for implementation

After completing the research element and covering all aspects of the research, the remaining task is to implement the proposed tool. To achieve this, the waterfall development model was followed to arrange the project ideas until reaching the final result.

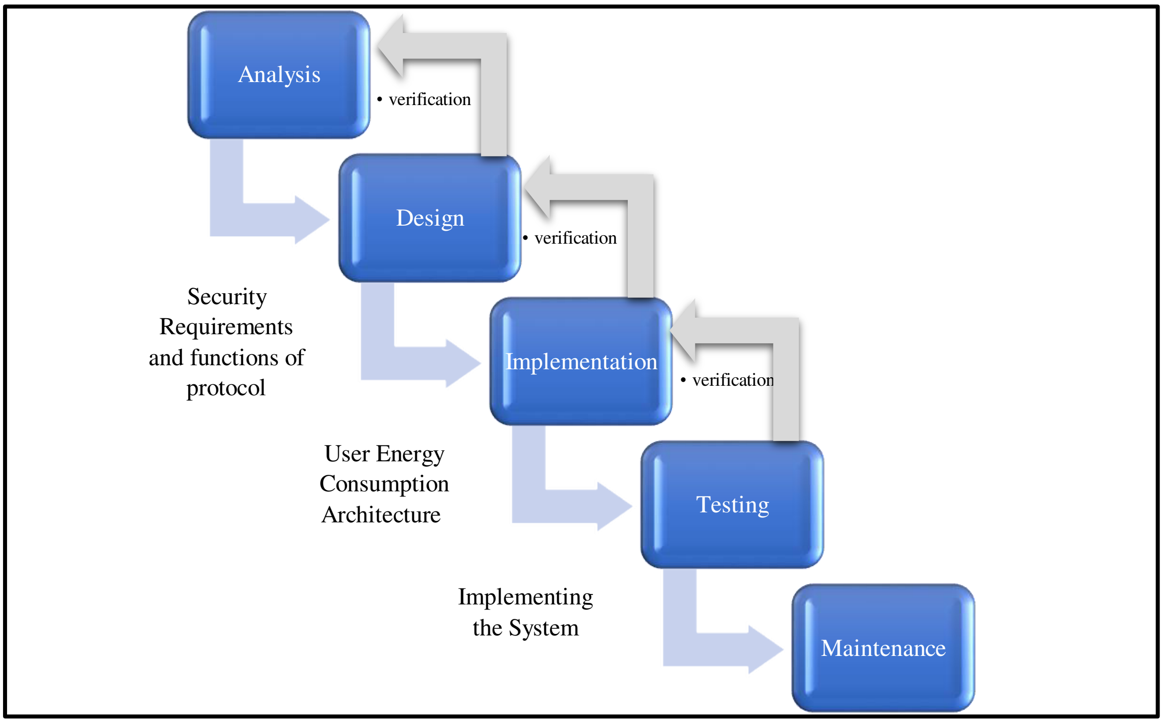


Figure 3. Waterfall development model for creating proposed tool

1. The first stage in the methodology is the **analysis** stage. In this stage, the SG protocols are analysed and their security requirements that they contain or lack are checked and recommendations made to solve the deficiencies that the protocols did not meet and to choose the best protocols from among them based on security requirements achieved (see Chapter 5).
2. In the second stage, which is the **design** stage, the design develops the concrete solution based on the functions of the protocols that were explained in Chapter 2 in addition to their requirements. This is achieved by developing a program structure that contains a plan to create a tool and plans to test the functionality of the tool. It should also contain certain standards related to the protocol functions, such as monitoring power consumption, alerting the user to exceeding the specified power limit as well as informing the user of the risks, and the possibility of choosing the appropriate action to block them.
3. Next is the **implementation** of the structure of the tool that was designed and proposed at the design stage. This is done in the specified programming language and involves the development of individual components, which contain dynamic drawings showing electricity consumption, and then verifying and merging them together to produce the proposed tool as planned.

4. **Testing** of the tool is conducted to determine whether the tool meets the previously specified requirements.
5. **Maintenance** is the last stage, in which the tool is fully equipped following success in the testing stage, and the required standards have been achieved. Thus, the proposed tool is now ready for delivery and usage.

Chapter 4: Design and Implementation

4.1 Overview

This chapter, which is divided into two parts. First, The first part describes the security requirements of protocol systems. In the second section, the suggested model-based approach is explained along with a graphical user interface for proposed tool.

4.2 Security Requirements for SAS

Inadequate **authentication** will lead to unauthorized access and the ability to damage devices and equipment. Therefore, authentication protects against forgery, unauthorized use, and spoofing (Vaidya et al. 2013). In order to access resources, a user must be **authorized,** which is a condition that is equally crucial to other security measures**.** The attacker employs password cracking to obtain access to IEDs that can subsequently execute control actions like breaking circuit breakers; this disrupts the operation of the substation and results in electric current outages (Rashid et al. 2014). The messages transmitted as GOOSE messages in these systems must include an **encryption** mechanism to prevent modification attacks on them or their capture, such as an attack by implementation of a malicious program that can capture, modify, and re-inject GOOSE messages in the network (Rashid et al. 2014)**.** The **integrity** and authenticity of messages in SAS are normally used to operate equipment. Security is of paramount importance to ensure that system information cannot be detected and tampered with SAS messages, as they are transmitted between substation devices. For example, on/off messages for circuit breakers must be strictly protected from spoofing (Lu et al. 2012). **Reliability** is a security criterion that the substation automation meets because it is intended that the component will perform the function that is expected of it within the allotted time frame without experiencing any failure. **Availability** means the systems are available for use when needed, or, as Yunus et al. (2008) suggested, as a portion of the overall time, the systems are accessible. Also, it protects against DoS attacks and ensures that those with authorized access can access the information. As Cleveland (2005) stated, **non-repudiation** is “preventing the denial of an action that took place or the claim of an action that did not take place”.

Therefore, SAS ensures that the entities that receive the data do not later refuse to receive it or claim to have received it when they did not.

4.3 Security Requirements for H/BAS

Building and home automation systems require entity **authentication** before being allowed to join a secure communication relationship. To secure the automated communications and make sure they are operational at the time of authentication, it is necessary to first authenticate and confirm the identity of the parties involved; this secures the communication channel (Granzer et al. 2009). **Authorisation** refers to, once the members of a secure communication relationship have been authenticated, it must be determined whether the joining node has the necessary access rights to attend a relationship and participation in a relationship must be denied if it has insufficient access rights (Granzer and Kastner 2010). They also confirmed that the secure channel in entities/devices in the automation uses cryptographic mechanism in order to avoid unauthorized interference of the data sent in the channel and to ensure data integrity against modification and tampering; it also ensures the confidentiality (**Encryption**) of data against the risk of interception. This prevents malicious nodes from impersonating a legitimate and trustworthy identity. The requirement of **confidentiality** is to ensure that the information and data sent in the building network is never disclosed except to those who are authorized. This is because it may provide the opponent with knowledge of the control commands of the devices and thus know the current conditions of the building or house and violate its privacy (Liu et al. 2018). **Integrity** means ensuring that all data and information provided must be validated at the time of receipt. This is because the intruder is trying to change, delay, and resend messages, which leads to them gaining control of building automation systems (Islam et al. 2012 and Liu et al. 2018). **Availability** means that BAS guarantees that data is available anytime it is required; therefore, BAS networks are able to provide data from authorized nodes (Granzer and Kastner 2010). **Reliability** is when the sensors allow real-time fault detection and isolation, which is an important factor in BAS performance requirements (Yi et al. 2011). **Non-repudiation** refers to the ability of the system to face disavowal attacks so that if the user denies doing something, the system is able to verify whether that is the case.

4.4 Security Requirements for DR

Authentication means that entities associated with DR are valid and authenticated to ensure that they do not modify or access DR's control services and only authenticated ones can issue DR event signals. For example, the lack of authentication between the smart meter and the display device enables the attacker to display energy consumption information (Paranjpe 2011). **Authorization** determines who can enter the system and access the resources because unauthorized access by the attacker gives them the opportunity to perform malicious activities that disrupt the functions of DR. Sensitive data must be **encrypted** on the network during transmission and storage in order to avoid unauthorized access to its contents. Examples of this type of data include real-time electricity usage statistics, bills, and other similar items. The system ensures that the **integrity** of the pricing signal is preserved. Most attacks affecting systems seek to manipulate customer information, electrical usage, billing information, and control signals (Paranjpe 2011). With **availability**, customers can see the performance of DR in real-time. In other words, the system provides customers with data about available energy, consumption, and operating times for loads from power utility (Vardakas et al. 2014). For **non-repudiation**, DR typically enters into service agreements with service providers, and verifiable proof must be kept in order for each participating entity to thereafter be able to dispute or challenge other entities (Mohan and Mashima 2014). **Anonymity** by protecting users' identity by masking it to prevent eavesdropping attacks. **Security mechanisms**, are the processes responsible for reporting in the event of security breaches.

4.5 The Requirements of proposed Tool

When the tool is created, prerequisites are provided that address some of the core functionality and the security requirements that must be met by the platform.

- The proposed tool should be incorporated into the SG architecture. Thus, in order to analyse the findings based on the data collected from the database, all customer information is taken from the SG database.
- The tool must contain security toolkits, such as IDS, WAF (Web Application Firewall), firewalls, and anti-malware. Besides that, it should apply situational

assessment and pattern analysis of consumption or devices behaviour analysis, and indicators of compromise (IOC).

- Each user should be provided with a unique subscription number so that their data is not mixed with others and ensures their right to deny access to their page for those who do not have the right of access.
- The data exchanged in the tool and the output must be in a machine-readable, findable, and interoperable format.
- Continuous updates are made on the actual consumption of energy, providing consumers with indicators of their current consumption and rate of consumption throughout the year in the form of graphs.
- For visibility, the tool should contain aesthetic visuals that represent information through colour coding.
- The presence of the direct display means that the tool enables consumers to see immediately what is happening in the use of energy, for example, when central heating devices are turned on, this will be noticed immediately in the change in the indicator of the room in which the heating was turned on, through a dynamic graph.
- When choosing protocols, to enable consumers to make a decision about the appropriate protocol, the tool must provide them with information about the protocols, their functions, and the security requirements they contain or lack (for example, confidentiality, integrity, availability, anonymity, authentication, authorisation, encryption, check mechanisms) to achieve credibility for consumers in choosing the appropriate protocol.
- In the event of a risk, the tool determines the degree of the risk, the damaged devices, and the history of the risk activity, in addition to enabling the consumer to choose the action they deem appropriate.

4.6 The proposed Tool

The proposed tool is designed based on the stated requirements as well as being combined with valuable features from the existing tools to appear as required and as planned. The tool displays a live picture of the user's electricity consumption and the available protocols that help them control energy use. The proposed tool stages are designed based on the waterfall development model; the analysis, design, implementation, testing, and maintenance are described in Chapter 3 (**see section 3.3**). As shown, the tool contributes to managing the demand response and provides the actual electricity consumption rates for all user devices registered in the system by the user. The existence of this proposed tool provides a seamless exchange of transmitted information between the network, consumers, and generators in buildings. The alliance of protocols and their presence in the system together provide a solution to deal quickly with overloads and excessive power consumption. This tool allows consumers to manage and control the increasing consumption; identify the reasons behind the high consumption, vulnerabilities, and risks to the system; and take the appropriate action in order to enhance energy management and enhance the SG as well.

The proposal of this tool depends on the involvement of EMSs so that each person enters their user number stored in the energy management database and can then monitor their monthly consumption since the structure of the platform allows them to verify the energy consumption of consumers and limit excessive consumption by using appropriate protocols, as DR and smart home environments have been employed to reduce such consumption. Therefore, **registration** is an important requirement to safely identify each person and their identity and not confuse user accounts or data. After the user is registered in the database, they are given a unique user number through which they can enter their consumption portal. For each consumer to set a certain limit for energy consumption is also a necessary requirement in the platform in order to **monitor and observe the person's consumption** in real time and **view the customer's consumption during the year** using the counter and not to exceed the limit that is allocated to them, so the they can **balance their electricity usage habits**. As Dolce et al. (2018) stated, the consumption is "is the total energy consumption that must be maintained below a demand limit". In the event of the person's consumption exceeding the energy, one of the necessary functional tasks provided by the system is to **inform the user** of when they are exceeding the limit. Electricity load scheduling is vital for the reliable and efficient operation of the SG because it enables customers to schedule energy use and lower electricity bills based on setting a limit to their usage (Roh and Lee 2015). If the sensor detects that the consumer's power consumption is greater than the specified limit, the consumer will be alerted by the new value being displayed on the tool platform in the consumer's counter. The consumer can ask the system to **display and monitor the rooms that have a high rate of energy usage** and **inform them of the risks or vulnerabilities** in all the devices of all the rooms in order to **choose the action** required to address them. In order to solve the problem of exceeding the permissible power limit and balancing the consumption, the system will provide the ability to **choose the appropriate protocols** for each consumer, and the selection will be made from among them based on the security requirements and functions provided by each protocol. The last operation is to **communicate with technical support** and choose the type of question the consumer wants, whether it is related to consumption, choosing a protocol, or other. The sequence diagram in Figure 4 illustrates all of these functions mentioned.

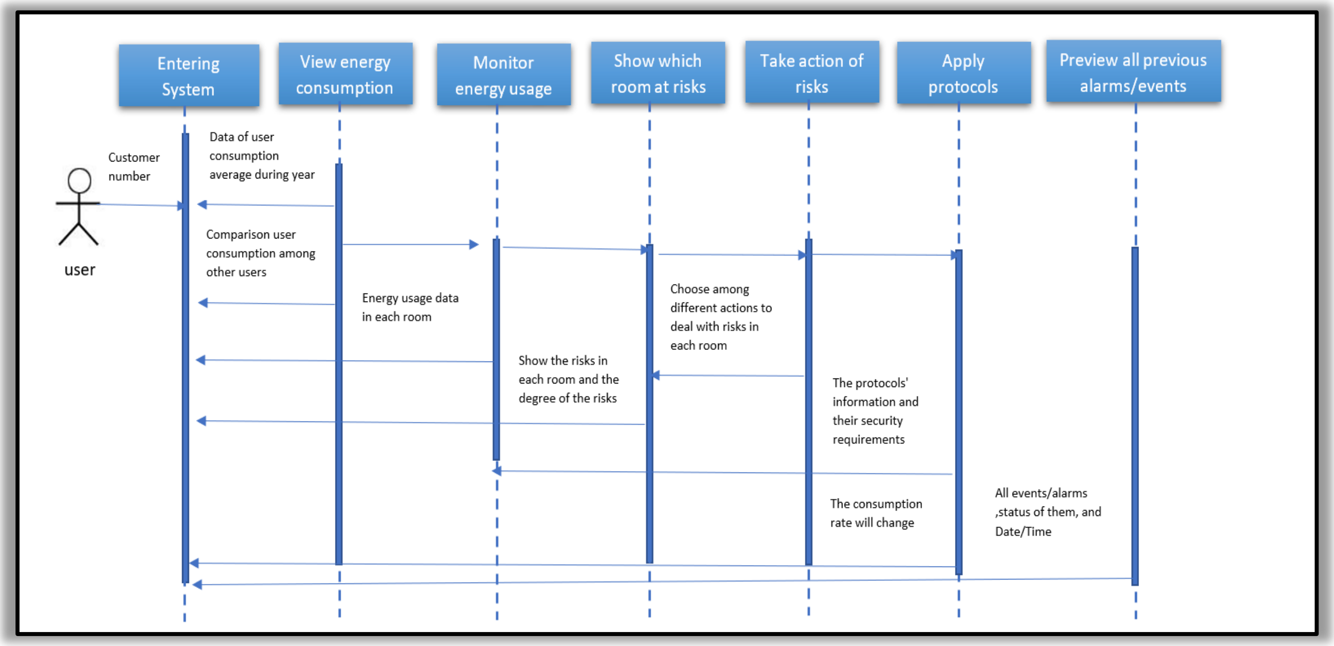

Entering System
View energy consumption
Monitor energy usage
Show which room at risks
Take action of risks
Apply protocols
Preview all previous alarms/events
user
Customer number
Data of user consumption average during year
Comparison user consumption among other users
Energy usage data in each room
Show the risks in each room and the degree of the risks
Choose among different actions to deal with risks in each room
The protocols' information and their security requirements
The consumption rate will change
All events/alarms ,status of them, and Date/Time

Figure 4. Sequence Diagram

4.7 Designing the Recommended Tool

The prototype of the recommended tool is based on the waterfall development model (**see section 3.3**). The design of the languages of the tool prototype used JavaScript, CSS, and html, and the work environment was Notepad++.

4.8 Recommended Tool GUIs

The system contains six functions: displaying the user's current energy consumption rate compared to other users, and the average consumption during the year; a live and changing picture of the consumption rate of each room registered in the system; the possibility of displaying all the risks and security holes discovered in the devices in the rooms according to which the degree of danger is determined in each room to choose the appropriate action to deal with these risks; choosing the appropriate protocol based on the requirements and functions it contains in order to adjust the user's consumption; and viewing all previous events and alerts that were displayed in the system and the status of each of them in terms of dealing with them and finally technical support. The functionality with the interface will be discussed in this section in detail. See **Figure 5** for the main interface and its components.

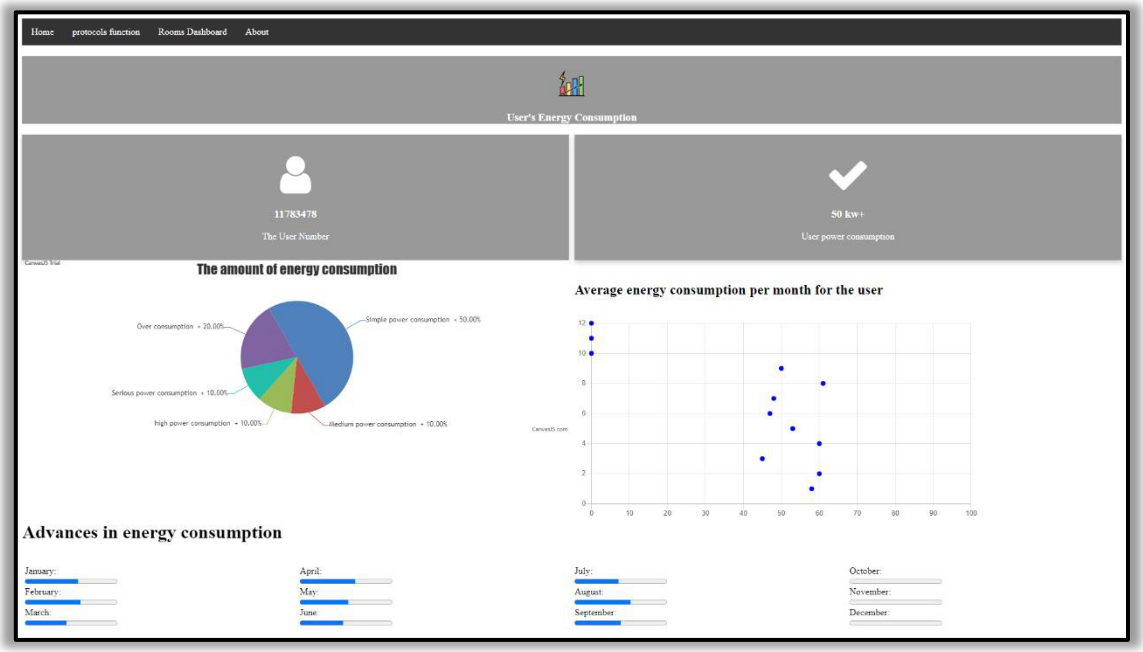

Home
protocols function
Rooms Dashboard
About
User's Energy Consumption
11783478
The User Number
50 kw+
User power consumption
CanvasJS Trial
The amount of energy consumption
Over consumption - 20.00%
Simple power consumption - 50.00%
Serious power consumption - 10.00%
high power consumption - 10.00%
Medium power consumption - 10.00%
Average energy consumption per month for the user
CanvasJS.com
12
10
8
6
4
2
0
0
10
20
30
40
50
60
70
80
90
100
Advances in energy consumption
January:
February:
March:
April:
May:
June:
July:
August:
September:
October:
November:
December:

Figure 5. The Main Interface

4.8.1 The Main Interface

The main interface page presented in **Figure 5, 6** contains colour coding in addition to the dynamic movement of the two charts each time the page is refreshed in order to clarify to the user his consumption status.

The main interface contains four parts as follows:

Description of the upper part:

1- The upper left part contains the user number. This is obtained after the user is registered in the database by filling in the required data, and then they receive a unique subscriber number to follow their consumption page and use it to log into their page.

2- Next to the subscriber's number in the upper right part, the value of their current monthly consumption in kilowatts is shown; in the figure, it is shown as 50 KW+.

The bottom part contains two graphs:

3- The lower right part shows a pie chart showing the energy consumption of the user compared to other consumers

4- A dots graph shows consumption during this year, and below, it shows the consumption by month. It is clear that the current consumption for this month (September) is 50 kilowatts, and months 10, 11, and 12 have not yet been calculated because they have not yet arrived. These charts undoubtedly will benefit the consumer by helping them to adjust their consumption habits.

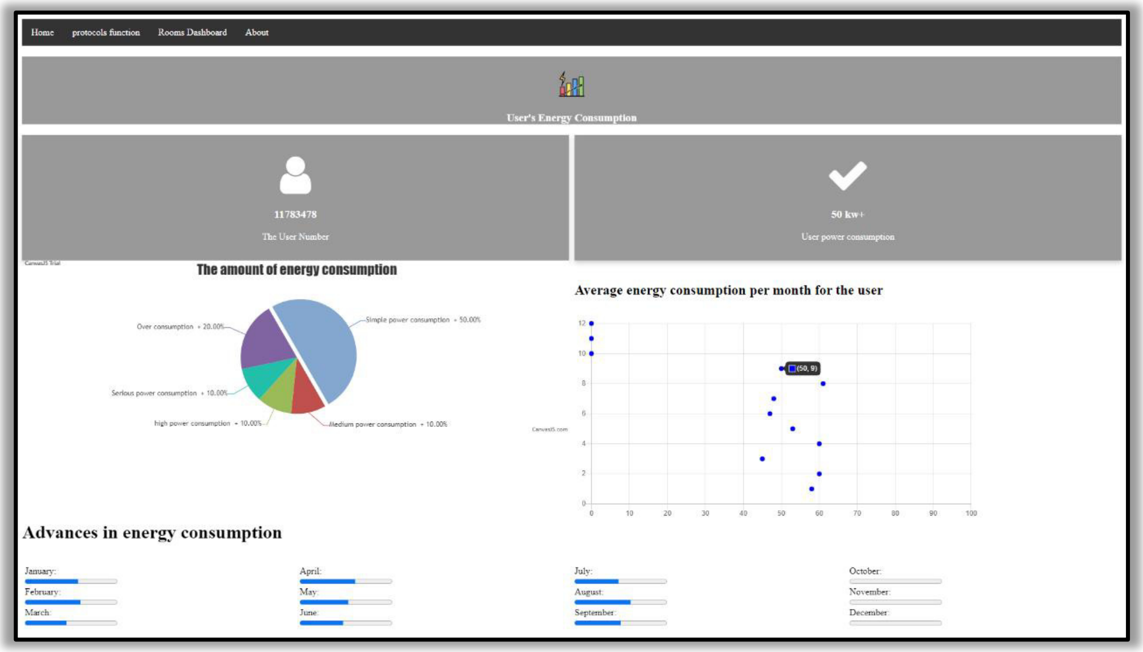
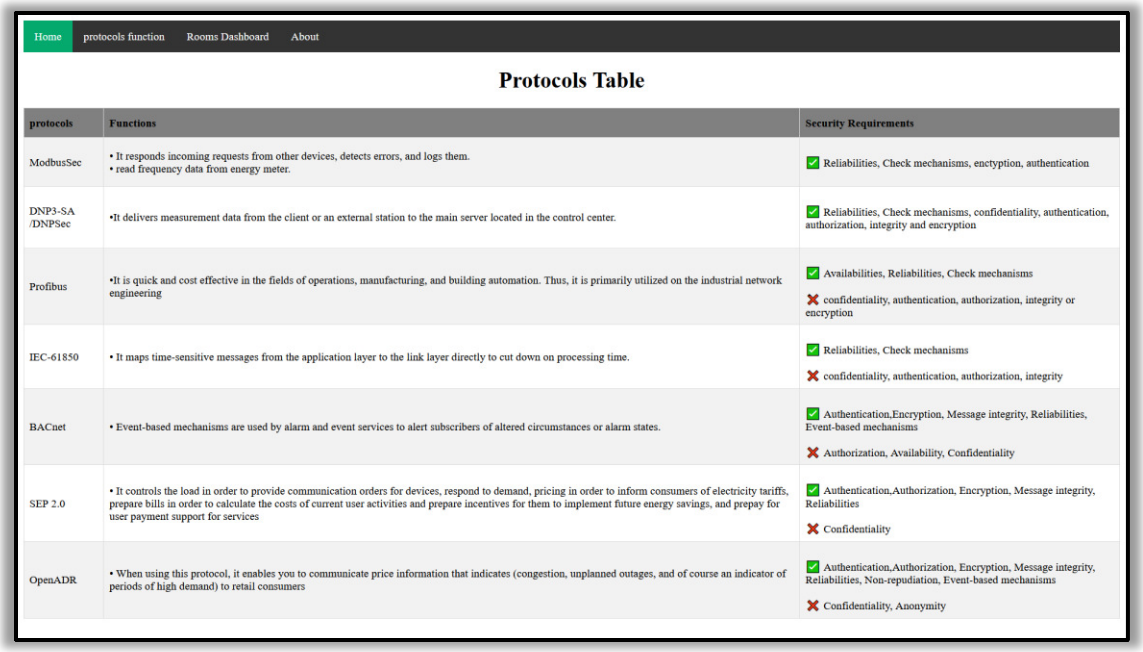

Home
protocols function
Rooms Dashboard
About
User's Energy Consumption
11783478
The User Number
50 kw+
User power consumption
CanvasJS Trial
The amount of energy consumption
Over consumption - 20.00%
Simple power consumption - 50.00%
Serious power consumption - 10.00%
high power consumption - 10.00%
Medium power consumption - 10.00%
Average energy consumption per month for the user
CanvasJS.com
(50, 9)
0
2
4
6
8
10
12
0
10
20
30
40
50
60
70
80
90
100
Advances in energy consumption
January:
February:
March:
April:
May:
June:
July:
August:
September:
October:
November:
December:

Figure 6. The four components of the main interface

4.8.2 Protocol Table Analysis Page

In the protocols table in **Figure 7**, the tool provides reliability to the user by showing all the protocols that can be applied in the consumption system along with their functions and the security features that they contain or lack; this will make it easier for the consumer to choose according to what they need to implement in the protocols.



Protocols Table

protocols	Functions	Security Requirements
ModbusSec	• It responds incoming requests from other devices, detects errors, and logs them. • read frequency data from energy meter.	✅ Reliabilities, Check mechanisms, enctyption, authentication
DNP3-SA /DNPSec	•It delivers measurement data from the client or an external station to the main server located in the control center.	✅ Reliabilities, Check mechanisms, confidentiality, authentication, authorization, integrity and encryption
Profibus	•It is quick and cost effective in the fields of operations, manufacturing, and building automation. Thus, it is primarily utilized on the industrial network engineering	✅ Availabilities, Reliabilities, Check mechanisms ❌ confidentiality, authentication, authorization, integrity or encryption
IEC-61850	• It maps time-sensitive messages from the application layer to the link layer directly to cut down on processing time.	✅ Reliabilities, Check mechanisms ❌ confidentiality, authentication, authorization, integrity
BACnet	• Event-based mechanisms are used by alarm and event services to alert subscribers of altered circumstances or alarm states.	✅ Authentication,Encryption, Message integrity, Reliabilities, Event-based mechanisms ❌ Authorization, Availability, Confidentiality
SEP 2.0	• It controls the load in order to provide communication orders for devices, respond to demand, pricing in order to inform consumers of electricity tariffs, prepare bills in order to calculate the costs of current user activities and prepare incentives for them to implement future energy savings, and prepay for user payment support for services	✅ Authentication,Authorization, Encryption, Message integrity, Reliabilities ❌ Confidentiality
OpenADR	• When using this protocol, it enables you to communicate price information that indicates (congestion, unplanned outages, and of course an indicator of periods of high demand) to retail consumers	✅ Authentication,Authorization, Encryption, Message integrity, Reliabilities, Non-repudiation, Event-based mechanisms ❌ Confidentiality, Anonymity

Figure 7. Protocols table

4.8.3 Rooms dashboard

On this page, the consumer will be able to monitor energy consumption, address risks or threats if any, track history events, and select the protocols offered by the tool .

4.8.3.1 Monitor devices usage in each room

This page shows the user the consumption of the devices in each room as stored in the system. The degree of consumption can be seen through colour coding and is divided into different categories (see **Figure 8**). The normal limit is set to be less than 170. Where the consumption is more than 200, which means it is over the limit, then the indicator shows the red colour because the room exceeds the consumption energy rate. When it is equal to 170 or a slightly higher, the indicator changes to an orange colour, so it should alert the consumer to reduce consumption. Finally, if it is less than 170, this means that the consumption of this room is in its normal state, and this is indicated by the green colour.

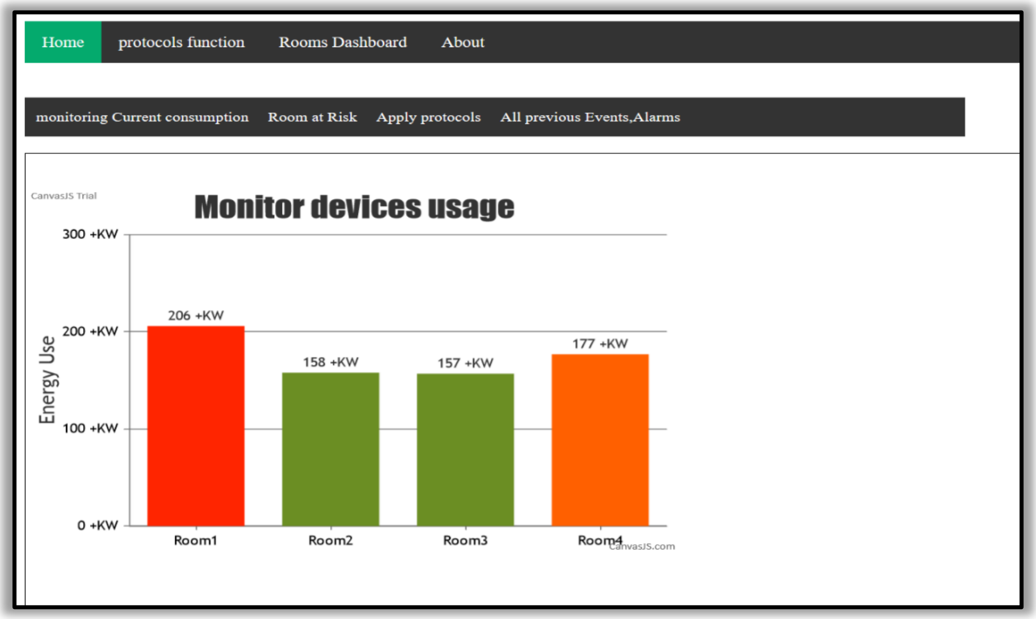
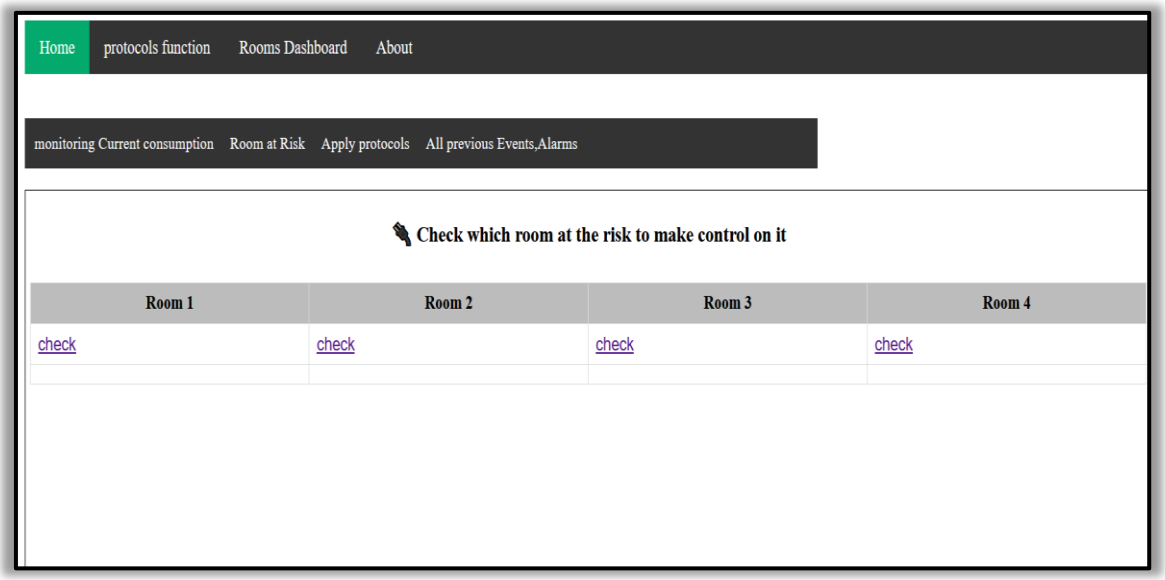


Figure 8. Devices' usage in each room

4.8.3.2 Room at Risk Page

This displays the rooms registered in the system and organizes each room and its data separately. The user can query the risks detected in these rooms and the degree of risk, and then can choose from a set of actions to solve these risks.

Figure 9 shows how the interface queries which rooms show a risk, as the data of each room is separate from that of the others.

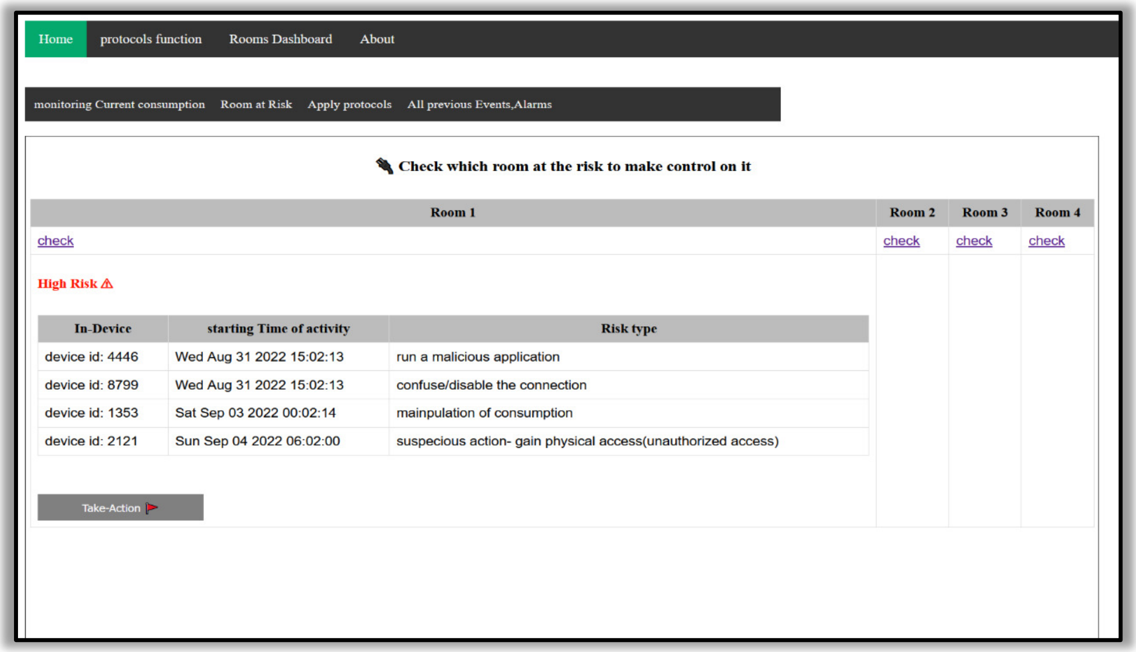


Check which room at the risk to make control on it

Room 1	Room 2	Room 3	Room 4
check	check	check	check

Figure 9. Room at risk page

Figure 10 shows that all the risks detected in the devices are presented in Room 1, and the degree of risk here is high as indicated in red. In addition, the start date of the risk activity is shown.



Check which room at the risk to make control on it

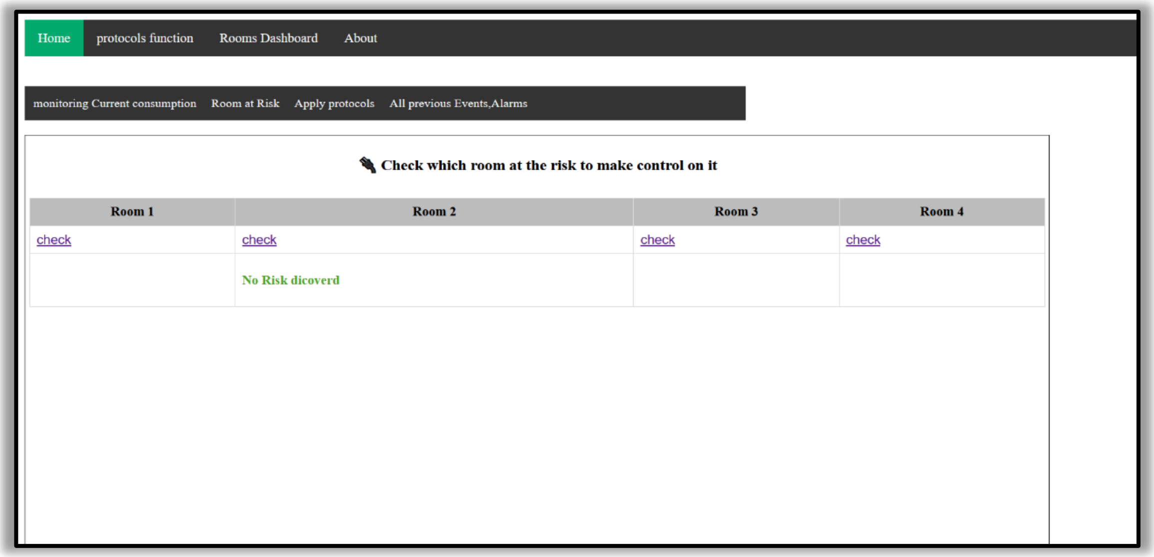
Room 1	Room 2	Room 3	Room 4
check	check	check	check

High Risk ⚠

In-Device	starting Time of activity	Risk type
device id: 4446	Wed Aug 31 2022 15:02:13	run a malicious application
device id: 8799	Wed Aug 31 2022 15:02:13	confuse/disable the connection
device id: 1353	Sat Sep 03 2022 00:02:14	mainpulation of consumption
device id: 2121	Sun Sep 04 2022 06:02:00	suspecious action- gain physical access(unauthorized access)

Figure 10. Checking Room 1 Risks/Degree

Here (**Figure 11**), it appears that Room 2 has not been detected as being in any danger, and so it is colored in green to show there is no danger.

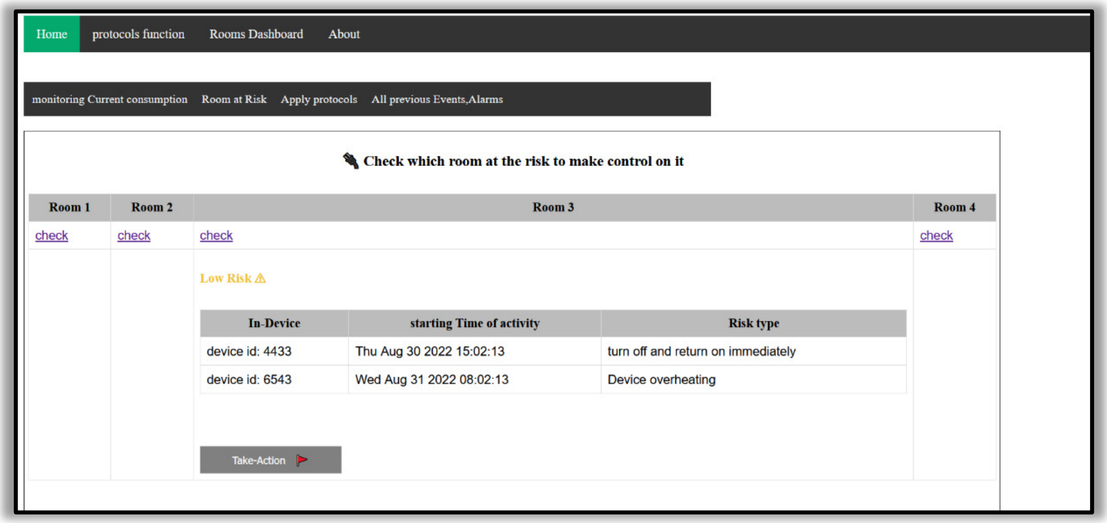


Check which room at the risk to make control on it

Room 1	Room 2	Room 3	Room 4
check	check	check	check
	No Risk dicoverd		

Figure 11. Checking Room 2 Risks/Degree

Also, Room 3 in **Figure 12** contains two detected risks, and the degree of risk detected by the two mentioned devices is low, as symbolized by the color yellow. In addition, the history of the risk's activity is provided.



Check which room at the risk to make control on it

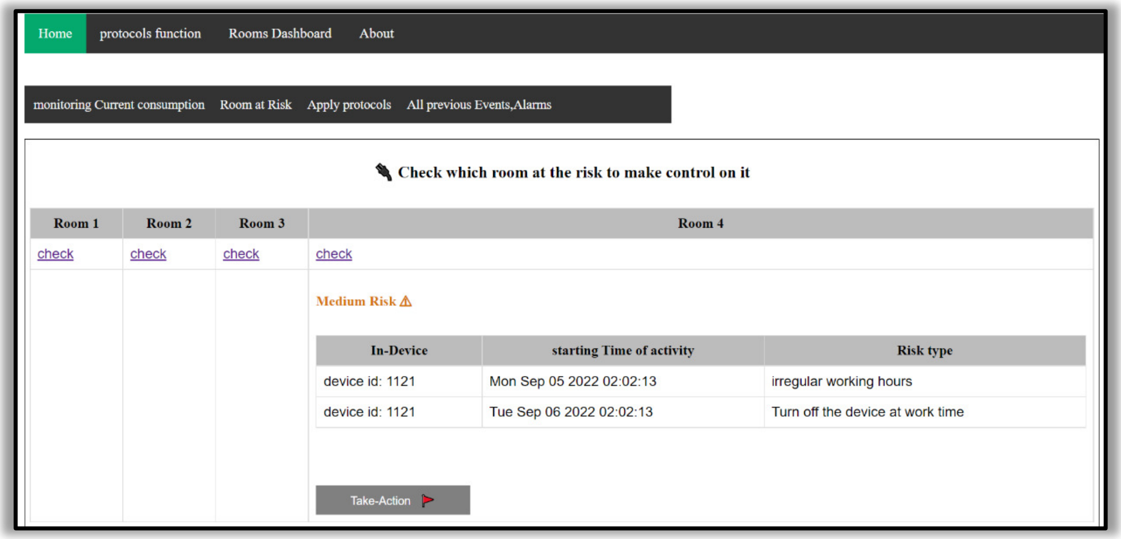
Room 1	Room 2	Room 3	Room 4
check	check	check	check

Low Risk ⚠

In-Device	starting Time of activity	Risk type
device id: 4433	Thu Aug 30 2022 15:02:13	turn off and return on immediately
device id: 6543	Wed Aug 31 2022 08:02:13	Device overheating

Figure 12. Checking Room 3 Risks/Degree

The last room registered for the consumer in the system is Room 4, and as shown in **Figure 13**, threats were discovered in its devices which meant it was at medium risk, with the degree of risk being indicated by the colour orange.



Check which room at the risk to make control on it

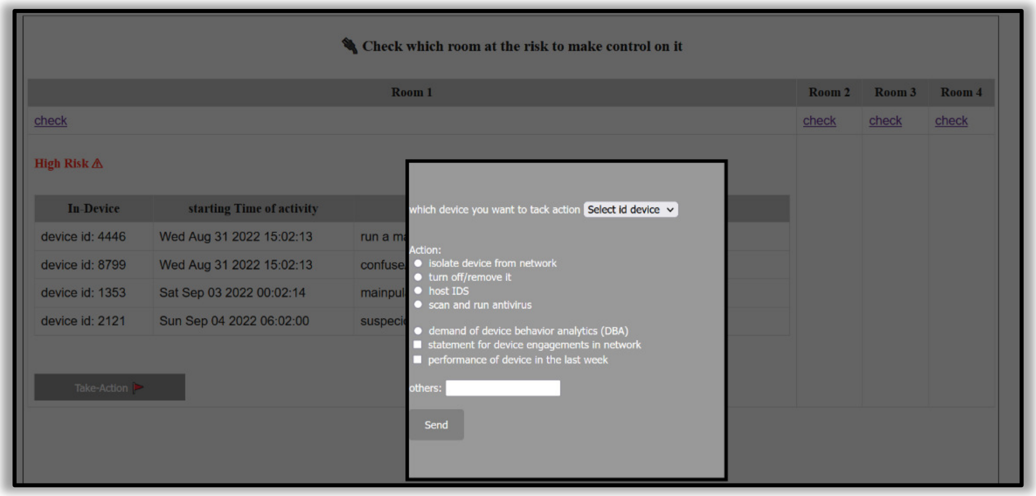
Room 1	Room 2	Room 3	Room 4
check	check	check	check

Medium Risk ⚠

In-Device	starting Time of activity	Risk type
device id: 1121	Mon Sep 05 2022 02:02:13	irregular working hours
device id: 1121	Tue Sep 06 2022 02:02:13	Turn off the device at work time

Figure 13. Checking Room 4 Risks/Degree

Here in **Figure 14**, appropriate action is taken regarding the hazards in the rooms. The consumer chooses the infected device with the ID number, or they can choose all the devices should all the devices in the room be infected. They can then choose any appropriate measure to overcome or solve these risks.



Check which room at the risk to make control on it

Room 1	Room 2	Room 3	Room 4
check	check	check	check

High Risk ⚠

In-Device	starting Time of activity	
device id: 4446	Wed Aug 31 2022 15:02:13	run a ma
device id: 8799	Wed Aug 31 2022 15:02:13	confuse
device id: 1353	Sat Sep 03 2022 00:02:14	mainpul
device id: 2121	Sun Sep 04 2022 06:02:00	suspeci

which device you want to tack action Select id device

Action:
- ● isolate device from network
- ● turn off/remove it
- ● host IDS
- ● scan and run antivirus

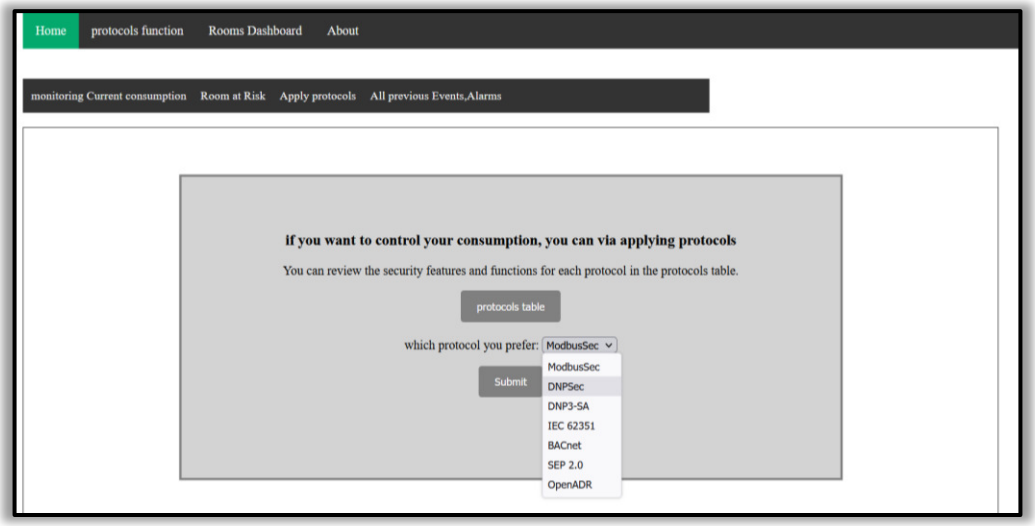
- ● demand of device behavior analytics (DBA)
- ■ statement for device engagements in network
- ■ performance of device in the last week

others:

Figure 14. Take action for risks discovered

4.8.3.3 Choose protocol

The user is given the right to review the functionality and security features of each protocol before selecting their preferred option through the protocol table button; the page for selection protocols is shown in **Figure 15**. The benefit of their choice of protocols is to control their consumption and manage it according to the functionality provided by the protocol they have chosen. After the user has decided on and selected the protocol, a page will appear for them as shown in **Figure 16** confirming the success of their choice, and they will be contacted to start installing the protocol at once. In addition, on this page, they will be redirected to the home page within 10 seconds.

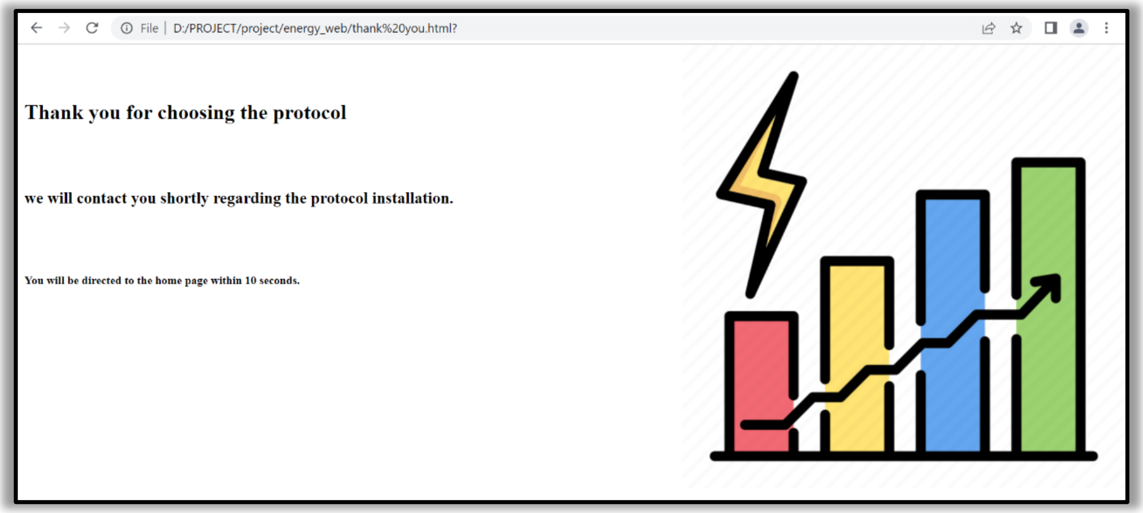


if you want to control your consumption, you can via applying protocols

You can review the security features and functions for each protocol in the protocols table.

which protocol you prefer: ModbusSec

Figure 15. Apply Protocol page



Thank you for choosing the protocol

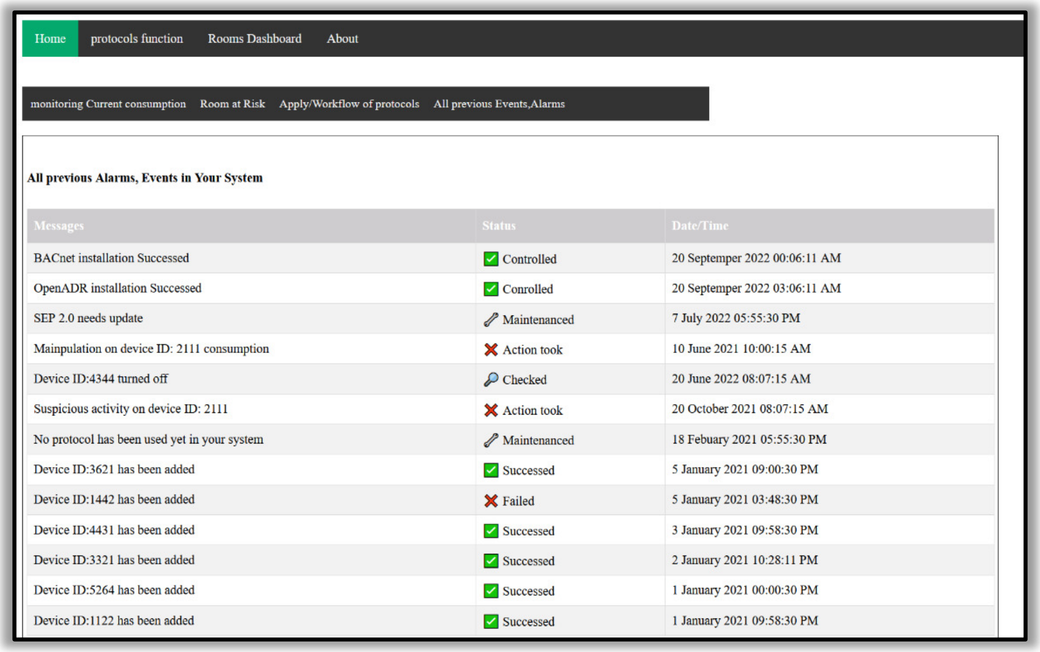
we will contact you shortly regarding the protocol installation.

You will be directed to the home page within 10 seconds.

Figure 16. Confirmation of choosing the protocol

4.8.3.4 Alarms and Events page

This page displays the history of all the alerts that reached the consumer, for example, adding new devices and connecting them in one of the rooms registered in the system, the expiration of the validity period of a protocol and the need to renew the installation, the presence of suspicious activity on the system, and informing the consumer of the successful download and installation of selected protocols and other alerts.


Home
protocols function
Rooms Dashboard
About
monitoring Current consumption
Room at Risk
Apply/Workflow of protocols
All previous Events,Alarms

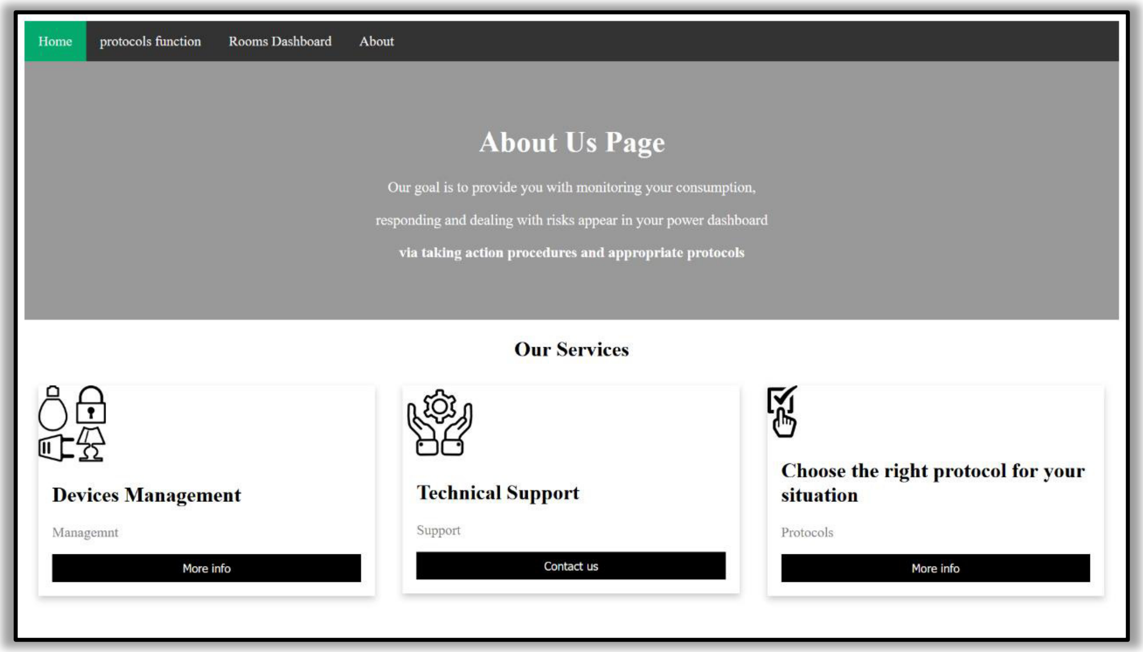
All previous Alarms, Events in Your System

Messages	Status	Date/Time
BACnet installation Successed	✓ Controlled	20 Septemper 2022 00:06:11 AM
OpenADR installation Successed	✓ Conrolled	20 Septemper 2022 03:06:11 AM
SEP 2.0 needs update	Maintenanced	7 July 2022 05:55:30 PM
Mainpulation on device ID: 2111 consumption	✗ Action took	10 June 2021 10:00:15 AM
Device ID:4344 turned off	Checked	20 June 2022 08:07:15 AM
Suspicious activity on device ID: 2111	✗ Action took	20 October 2021 08:07:15 AM
No protocol has been used yet in your system	Maintenanced	18 Febuary 2021 05:55:30 PM
Device ID:3621 has been added	✓ Successed	5 January 2021 09:00:30 PM
Device ID:1442 has been added	✗ Failed	5 January 2021 03:48:30 PM
Device ID:4431 has been added	✓ Successed	3 January 2021 09:58:30 PM
Device ID:3321 has been added	✓ Successed	2 January 2021 10:28:11 PM
Device ID:5264 has been added	✓ Successed	1 January 2021 00:00:30 PM
Device ID:1122 has been added	✓ Successed	1 January 2021 09:58:30 PM

Figure 17. Alarms/ Events page

4.8.3.5 The services provided by the tool

The page shown in **Figure 18** explains the services provided by the proposed tool. In addition, it will provide technical support in the event of a problem with the installation of the protocol or in the event of consumption or any problem facing the consumer by selecting the ‘Contact us’ box, whereupon, the consumer will be directed to the support page as seen in **Figure 19**.



About Us Page

Our goal is to provide you with monitoring your consumption,

responding and dealing with risks appear in your power dashboard

via taking action procedures and appropriate protocols

Our Services

Devices Management

Managemnt

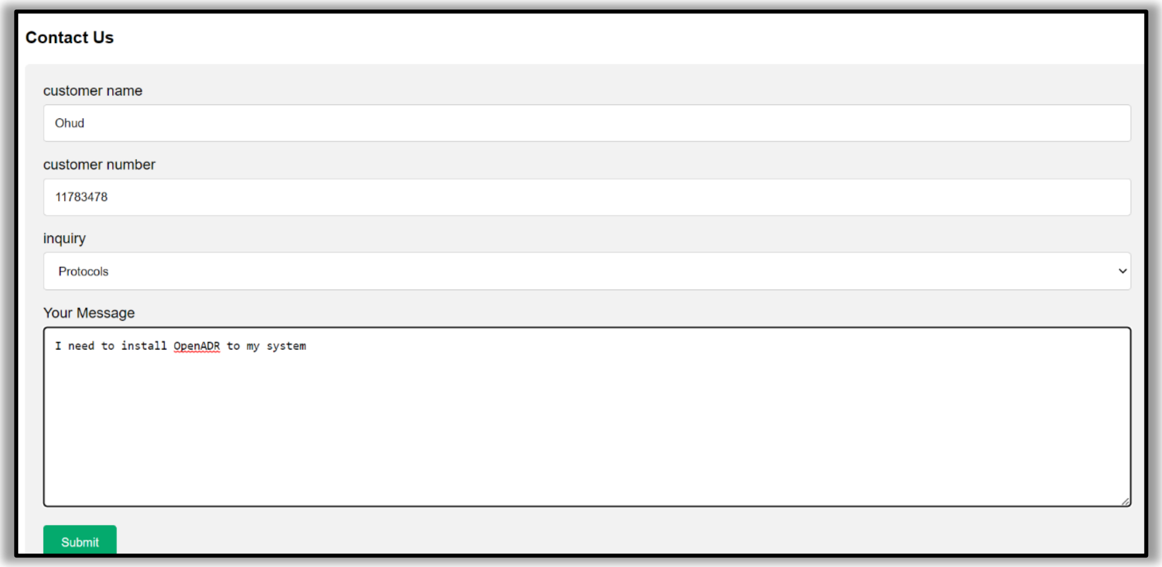
Technical Support

Support

Choose the right protocol for your situation

Protocols

Figure 18. Our Services page



Contact Us

customer name

Ohud

customer number

11783478

inquiry

Protocols

Your Message

```
I need to install OpenADR to my system
```

Figure 19. Contact Us page

Chapter 5: Results and Evaluation

5.1 Overview

In this chapter, results are presented for the study and the analysis of the protocols in SA protocols, H/BA Protocols, and DR protocols. Choosing the best protocols from among them according to the security requirements provided by the protocol are discussed in addition to the protocol's effective functions. According to what was analysed and discussed in Chapter 2 about some of the security requirements that SG protocols contain and which ones they lack, in this section, more information are given to all security requirements in order to choose the best among them and give the recommendations.

5.2 Security requirements for SA protocols

The security requirements that the automation protocols (DNP3, Modbus, Profibus, IEC-61850) meet and what they do not are provided and assessed in this section to help in the selection of the best protocol according to whether it fulfils most requirements, and suggestions will be provided for the requirements it lacks.

Table 11. SA protocols security requirements

Security requirements	DNP3	Modbus	Profibus	IEC61850
Authentication	✗	✗	✗	✓
Authorisation	✗	✗	✗	✗
Encryption	✗	✗	✗	✓
Message/Data integrity	✗	✗	✗	✓
Availability	✗	✗	✓	✗
Reliability	✓	✓	✗	✓
Non-repudiation	✗	✗	✗	✗

5.2.1 Analysis of SA protocols' security requirements table

There are no built-in procedures for **authentication** provided by all of these protocols to confirm the identities of master and slave devices except IEC 61850. Since the DNP3 protocol does not use authentication, authorisation, or encryption, therefore, a hacker with access to the network may easily spoof the messages (Pandey and Misra 2016). Modbus does not have authentication, and it was stated by Fovino et al. (2009) that since Modbus TCP does not authenticate master and slave machines, a compromised device can pretend to be the master and send commands to the slaves. Also, for Profibus, Abouzakhar (2013) stresses that non-authentication is one of the main limitations it faces, as it leads to unauthorized control of its functionality, which disables it or injects code into slave nodes. However, the IEC 61850 protocol primarily uses authentication by using Message Authentication Codes (MAC) and Secure Hash Algorithm to secure GOOSE messages in order to guarantee the integrity of the data and the reliability of its source (Moreira et al. 2016). Even though IEC 61850 deals with authentication during data transfer using digital signatures, it is missing the authorization that is crucial for maintaining the integrity and secrecy of the data (Lee et al. 2014). For **authorisation**, none of these procedures offer protection from unauthorized access. Modbus has no security mechanism to prevent unauthorized access (Pandey and Misra 2016); therefore, attackers reuse the legitimate messages for Modbus transmitted to or from slave devices. Regarding the third requirement (**encryption**), among all of these protocols, IEC 61850 is the one which uses message encryption. The Modbus protocol does not provide itself with any security techniques, and all its messages are sent in clear and plain text without any encryption of the message (Byres et al. 2004). For **integrity**, all these protocols lack message integrity since neither the master nor the slave can confirm the authenticity of the messages they have received except for DNP3, which adds additional integrity checks at the application layer as well as the transport layer (Hayes and El-Khatib 2013). In Modbus, due to lack of message integrity checks, an attacker may modify or fabricate legitimate messages and send them to slave devices in the protocol (Fovino et al. 2009). For IEC 61850 **,** it fulfills this requirement and Moreira et al. (2016) prove that. Moving to **availabilities**, none of these protocols fulfils this requirement except Profibus and DNP3. External devices lose their primary functionality, or communications with the master are disrupted as a result of availability attacks (East et al. 2009). Also, it is confirmed by Kanabar and Sidhu (2009) that he mentions availability improvements in the design of stations based on IEC 61850 is the most challenging problem. For **reliability** in communication, because there is a need for this requirement to be implemented in the SG, all protocols have been adopted due to the reliability of the data. The DNP3 protocol has reliability as well as Modbus due to its regular use of cyclic redundancy checks for any exchange between master and slave. The high-speed communication process based on Ethernet with authorized access makes IEC 61850 a reliable protocol (Elgargouri et al. 2015). However, the Profibus protocol does not provide reliability; as Huang et al. (2021) argued, the lack of this protocol in the reliability of control systems is due to problems in installation and equipment. Regarding the last requirement (**non-repudiation**) , DNP3 does not fulfill non-repudiation and that confirmed by (Majdalawieh et al. 2005). It is clear that the Modbus also does not fulfill this requirement, because The fact that the new extension to Modbus put out by Fovino et al. (2009) supports non-repudiation since the original Modbus did not comply with this criteria. Also, Profibus and IEC-61850 Sami et al. (2013) confirm that.

5.2.2 Security evaluation of chosen SA protocol and its recommendations

Although most of the protocols do not meet the security requirements, the **IEC61850** protocol is considered the best among them to achieve 3 out of 6 requirements. Also, a set of recommendations has been developed for the security requirements that IEC-61850 lack of to increase its efficiency and effectiveness.

Table 12. recommendations for IEC-61850

Security requirements	IEC-61850
Authentication	✓
Authorization	✗ Recommendation in section 5.2.2.1
Encryption	✗ Recommendation in section 5.2.2.2

Message/Data integrity	✓
Availability	✗ Recommendation in section 5.2.2.3
Reliability	✓
Non-repudiation	✗ Recommendation in section 5.2.2.4

5.2.2.1 Attribute Certificate (AC)

It is a successful method to safeguard data, demonstrate its authenticity, and ensure that non-repudiation through the use of digital signatures. Also, I recommend the existence of a certificate that serves to authorize its holder. there is a Suggestion by (Vaidya et al. 2013) is an attribute certificate AC that stores attributes known by users, and a digital ID signed and contains certain attributes for authorization.

5.2.2.2 Encryption Scheme

using the methodology that proposed by Hussain et al. (2020) which is “Authenticated Encryption with Associated Data (AEAD) algorithms, which is based on three phases: Encrypt-then-MAC (EtM), Encrypt-and-MAC (E&M) and MAC-then-Encrypt (MtE)”.

5.2.2.3 Multi-Replica Data Possession (MR-PDP) for availability

I recommend that there should be a number of data replicas. As (Rusitschka et al. 2010) suggest copying the data and having a number of copies inside the data centers allows for quick recovery of data from the data cloud in the event that data was not available . Also, using MR-PDP, which is methodology proposed by (Curtumola et al. 2008); it guarantees the availability and reliability of the data by allowing users to store multiple replicas of a single file across various distributed servers, allowing them to access the original file from any server even in the event that one of them fail.

5.2.2.4 recommendations for non-repudiation scheme

Non-repudiation can be handled using the AC and digital signature specified in (section 5.2.2.1) above.

5.3 Improvements for SA protocols security requirements

Since **Table 11** shows that the majority of automation protocols lack significant security requirements, the enhanced protocols with security additions will be highlighted here and **Table 10** in Chapter 2.

Table 13. Adds security features for new version of SA protocols

Protocol	Authentication mechanisms			Encryption mechanism	
	Hash Message Authentication Code (HMAC)	Challenge And Response	X.509 certificates	3-DES	TLS encryption
DNPSec	✓	✗	✓	✓	✗
DNP3-SA	✓	✓	✓	✓	✗
ModbusSec	✓	✗	✗	✗	✓
Profinet	✓	✗	✗	✓	✗
IEC 62351	✗	✗	✓	✗	✓

5.3.1 Analysis of enhanced SA protocols' security requirements

Taking into account the new versions of the protocols and the efforts that have been made to add new features to them, the security features of some protocols have not been completed **see chapter 2 table 10**. Fortunately, all of the upgraded protocols satisfy the first prerequisite, which is authentication, specifically, HMAC authentication; all protocols except IEC 62351 apply. For X.509 certificates, only DNPSec, DNP3-SA, and IEC 62351 are used. For Challenge and Response, only DNP3-SA is used (Lee et al. 2014 and Volkova et al. 2019).

Regarding encryption security requirements, the DNP3-SA and DNPSec protocols release contributes to adding encryption requirements for the DNP3 protocol. DNPSec applies the Triple Data Encryption Standard (3-DES), while DNP3-SA uses asymmetric and symmetric encryption (Lee et al. 2014 and Volkova et al. 2019). Regarding ModbusSec, as Abou el Kalam (2021) discussed, ModbusSec is a type of Modbus encapsulation in a TLS layer, so it uses TLS encryption to secure communications. Profinet uses the same mechanism as DNP3-SA uses, which is both 3-DES (Müller and Doran 2018). Regarding IEC 62351, it defines the security features for IEC 61850 communications, and therefore, TLS encryption is used. As Moreira et al. (2016) emphasized, it uses comprehensive authentication by using TLS version 1.0 and uses SHA to authenticate messages.

5.3.2 Security evaluation of improvements SA protocols

As analysed in Table 12, two protocols, DNP3-SA and DNPSec, are preferred because of their application of more than one authentication mechanism, but DNP3-SA was chosen due to its use of three authentication mechanisms and 3-DES encryption method.

5.4 H/BA protocols' security requirements

In this section, Home/Building Automation protocols (SEP 2.0, BACnet) are examined by highlighting the most crucial security requirements regarding what they have and what they lack, thus making it possible to select the best protocols from the group.

Table 14. H/BAS protocols security requirements

Security requirements	BACnet	SEP 2.0
Authentication	✓	✓
Authorization	✗	✓
Encryption	✓	✓
Integrity	✗	✓

Availability	✗	✗
Reliability	✓	✓
Non-repudiation	-	-
Event-based mechanisms	✓	✓

5.4.1 Analysis of H/BA protocols' security requirements

Regarding the **authentication** and **authorisation** requirements, The SEP 2.0 protocol uses TLS to ensure client authentication and to provide an X509 digital certificate (Upreti et al. 2019; Qi et al. 2016). Many of the authentication and authorisation criteria missing from other protocols are addressed in the SEP 2.0 standard (Ingram et al. 2021), while BACnet is authenticated by implementing device authentication (Johnstone et al. 2015) (see Table 3 in Chapter 2). All of these protocols fulfil **encryption**, but there are differences according to the mechanism used. SEP 2.0 uses TLS and AES-128, and it enables devices to use ellipsoidal curved ciphers (Upreti et al. 2019; Qi et al. 2016). Moving on to message integrity, it has been observed that the SEP 2.0 protocol uses TLS for message exchange and that guarantees this requirement; however, BACnet unfortunately lacks all of these features. For **integrity**, BACnet proved that it lacked integrity since a hacker can craft any packet and send it to the BACnet system, and there is no verification check (Yimer et al. 2022). **Availability**, SEP 2.0 doesn’t guarantee this requirement If there is insufficient protection from the firewall, the hacker will be able to enter and therefore, this will disable the protocol's functionality and data cannot be accessed and device information or signals cannot be retrieved (Levy et al. 2011). Regarding **reliability**, all of these protocols guarantee this requirement since the BACnet application layer is responsible for managing the user's application program interface and ensuring reliability (Yimer et al. 2022). For **non-repudiation**, there is no proof found for this requirement applied in both protocols. Regarding **event-based mechanisms**, the BACnet protocol makes it possible to check frequently for the particular values of the devices and to notify about the damage as soon as the device's state changes since some devices can report the state of a change in a given value but cannot send alarm messages. However, there is no evidence of SEP 2.0 being able to apply event-based mechanisms.

5.4.2 Security evaluation of chosen H/BA protocol and its recommendations

It is also clear that the SEP 2.0 protocol is the best compared to the other to achieve 6 out of 8 requirements, so proposed solutions will be mentioned for the security requirements that it lacks to increase its security and effectiveness.

Table 15. Recommendations for SEP 2.0

Security requirements	SEP 2.0
Authentication	✓
Authorization	✓
Encryption	✓
integrity	✓
Availability	✗ Recommendation in section 5.4.2.1
Reliability	✓
Non-repudiation	- Recommendation in section 5.4.2.2
Event-based mechanisms	✓

5.4.2.1 Scheme for Availability Requirements

The recommendation for availability is mentioned above in section 5.2.2.3

5.4.2.2 Scheme for Non-repudiation Requirement

The AC, and digital signature mentioned above in (section 5.2.2.1) can be used to address non-repudiation if it is lacking in the protocol.

5.5 DR Protocols' Security Requirements

This section lists and evaluates the security requirements that the DR protocols meet and providing solutions for the requirements that the chosen protocol lacks.

Table 16. DR protocols security requirements

Security requirements	DRBizNet	OpenADR
Authentication	✓	✓
Authorization	-	✓
Encryption	✓	✓
Message integrity	✓	✓
Availability	✓	✗
Reliability	✓	✓
Non-repudiation	-	✓
security mechanisms	✓	✓
Anonymity	-	✗

5.4.1 Analysis of DR protocols' security requirements

Regarding the **authentication** requirement in OpenADR, communicating entities are authenticated using TLS and mutual authentication (Yassine 2016). DRBizNet uses so-called "intelligent agents (IA)" which confirm requests for authenticity using DR exchange (DRX), and DRX verifies IA's authentication using PKI (Vojdani 2008). **Authorization,** for the OpenADR, it uses the CA to allow authorized access, while no proof was found for the DRBizNet protocol regarding this requirement. Regarding **encryption,** both protocols follow this requirement depending on the approach used. As for the DRBizNet, there is no explicitly for the encryption methodology used, but Yee (2006b) confirmed that this protocol ensures that there is no visibility for those who load enrolled programs, and this confirms confidentiality. In the OpenADR protocol, each message is encrypted with individual digital signatures. Regarding

message integrity, I have found no evidence to indicate DRBizNet supports this requirement, but it has been shown that IA acts as a key to support DRBizNet messages and give them security mechanisms (Vojdani 2008). Meanwhile OpenADR uses TLS, which provides it with safe exchange messages and ensures communication integrity protection. Regarding **availability**, there was no evidence that proof of OpenADR guarantees its availability; this was confirmed by Basmadjian (2021). The access, availability, and usability of system resources on demand cannot be guaranteed because DoS attacks pose a threat to them whereas the DRBizNet protocol ensures that responsive products are available within 10-20 minutes or less, and resource and response time are also rapid (Yee 2006a). For **reliability**, DRBizNet achieves powerful operations that are highly fault tolerant. Yee (2006b) also argued that it ensures an unbalanced and regulated power supply, as it gives a minimum of issues and problems for network operators. Regarding the **security mechanism**, the OpenADR protocol contains event properties and flags, event duration, and event start time whereas DRBizNet has notification for the start and end of its events in addition to using appropriate firewalls and controlling access to and use of data (Engel and Hinkle 2004). However, the OpenADR protocol does not guarantee the **anonymity** of consumer data from aggregators because some of the individuals running the pools are able to identify nodes based on load signatures, as confirmed by Upreti et al. (2019), while in DRBizNet, there was no evidence for it either having or lacking anonymity.

5.5.2 Security evaluation of chosen DR protocol and its recommendations

As shown in **Table 16**, both protocols are somewhat similar in meeting security requirements, but what makes me choose OpenADR over DRBizNet is that there are no reliable sources for its application of Authorization, non- repudiation or Anonymity requirements. In **Table 17**, recommendations are presented in order to address the security vulnerabilities, and threats faced by the OpenADR.

Table 17. Recommendations for OpenADR

Security requirements	OpenADR
Authentication	✓
Authorization	✓
Encryption	✓
Message integrity	✓
Availability	✗ Recommendation in section 5.4.3.1
Reliabilities	✓
Non-repudiation	✓
Anonymity	✗ Recommendation in section 5.4.3.2
Event-based mechanisms	✓

5.5.2.1 Scheme for ensure availability

The recommendation for availability is mentioned in section 5.2.2.3

5.5.2.2 Anonymous scheme

The scheme that refers to the anonymous, is called blind signature with anonymous authentication and privacy preservation of the SG. It is recommended by (Kong et al. 2020). The unique feature of a blind signature is that neither the issuing signatory nor the data owner's identity are made public. Their scheme contain three components, first, the control center, which is responsible for creating system parameters and validating data. Second, the user-interactive smart substation that establishes a blind signature and uses it to confirm the user's identification. A smart meter, the third component, captures data in real time. In the event that the signature's authenticity is not confirmed, the user's identity can be concealed through a blind signature.

Chapter 6: Conclusion

6.1 Conclusion

The current study sought an insight into the SG and its associated protocols in their systems, and provided an analysis of a group of its protocols by studying their functions, challenges, risks, proposed solutions and improvements added to them. Three systems were selected to discuss the most prominent protocols used in them, SAS, including protocols (DNP3, Modbus, Profibus and IEC- 61850), B/HAS (SEP 2.0 and BACnet) and DR (OpenADR and DRBizNet). Then, the best protocols in each system were identified based on a security analysis of the requirements it meets, and recommendations for the missing requirements in order to address the weaknesses and threats it faces. The IEC-61850 protocol was identified as the best protocol in SAS that met most security requirements, and recommendations were made to address a requirements that it lacks. These recommendations include: Using an Attribute Certificate (AC) and digital signature to address non-repudiation and authorization. In the encryption requirement it is recommended to use Authenticated Encryption with Associated Data (AEAD) algorithms that has 3 stages: (EtM), (E&M) and (MtE). For availability requirement MR-PDP is recommended. The SEP 2.0 protocol in H/BAS has been identified as the best protocol compared to BACnet, and the proposed recommendations to address what it lacks in requirements: the recommendation of both availability and non-repudiation mentioned in the protocol (IEC-61850). Finally, OpenADR was chosen as the best protocol in DR. As for the recommendations that have been made to address what is lacking of the security requirements, it is the availability mentioned in the IEC-61850, and the blind signature with anonymous authentication and privacy preservation recommendation to address anonymity.

Also, we proposed tool to track the energy consumption of a user's page and provide protocols to choose from to control its consumption and to choose preventive measures in case the consumer encounters a threat. The need for this work is increasing due to the need for energy management and smart grid application management.

6.2 Future work

In the future, there will be a physical connection to the user database taken from SG to make this tool more realistic and interactive. Moreover, another set of smart network protocols will be integrated into the proposed tool and enable the user to integrate 3 or more protocols into his consumption page to take the strengths of each protocol and thus secure his page through the embedded protocols. Also, have the tool integrate with other utility applications such as electric vehicle charging applications to make the platform fulfill the purpose of monitoring electricity consumption in all aspects of a consumer's life.

6.3 Reflection of my learning

This study greatly improved my understanding of the smart grid infrastructure and the protocols used between its systems. The one of the first challenge I faced it was Researching in protocols because the field of smart grid is very deep and contains many protocols in every system and part of the system, so I chose to talk about the platforms in smart grid and their protocols. Of course, the journey of searching for each protocol and its advantages and features took a lot of time, because most of the time I do not find enough sources for the same idea that I am looking for. Determining the issue of risks and challenges facing each protocol is no less difficult than the other challenges, because it is necessary to take into account the risks and what are the proposed solutions to solve them. Also, addressing the functions of each protocol and its security features with the challenges that still hinder it despite its advantages is undoubtedly one of the challenges Which I encountered because I had to make them fit with each other and relate to each other.

Also in the field of implementation, I was confused because I want a platform that integrates protocols with other applications that benefit the consumer in energy, and I was looking for how to deliver my idea on the ground. I think I was able to communicate the idea of my proposal as it was planned.

My belief in myself always motivates me to learn and grow in the sea of knowledge. As for what I learned from this experience, time is gold and every day is calculated in achievement. It helped me to plan well and divide the tasks of the writing my dissertation. I learned to think outside the box and to follow the strategy of critical analysis of everything I write in order to communicate the content of the research without the complexity in ideas presented.

References

Abou el Kalam, A., 2021. Securing SCADA and critical industrial systems: From needs to security mechanisms. International Journal of Critical Infrastructure Protection, 32, p.100394.

Abouzakhar, N., 2013. Critical infrastructure cybersecurity: a review of recent threats and violations.

Aladdin, S., El-Tantawy, S., Fouda, M.M. and Eldien, A.S.T., 2020. MARLA-SG: Multi-agent reinforcement learning algorithm for efficient demand response in smart grid. IEEE access, 8, pp.210626-210639.

Albano, M., Ferreira, L.L. and Pinho, L.M., 2014. Convergence of Smart Grid ICT architectures for the last mile. IEEE Transactions on Industrial Informatics, 11(1), pp.187-197.

Amoah, R., 2016. Formal security analysis of the DNP3-Secure Authentication Protocol (Doctoral dissertation, Queensland University of Technology).

Badar, H.M.S., Qadri, S., Shamshad, S., Ayub, M.F., Mahmood, K. and Kumar, N., 2021. An identity based authentication protocol for smart grid environment using physical uncloneable function. IEEE Transactions on Smart Grid, 12(5), pp.4426-4434.

Barenghi, A., Breveglieri, L., Fugini, M. and Pelosi, G., 2012 Smart Power Grids Security: Smart Meters and Home Gateway Scenarios.

Basmadjian, R. (2021). Communication Vulnerabilities in Electric Mobility HCP Systems: A Semi-Quantitative Analysis. Smart Cities, 4(1), pp.405–428. doi:10.3390/smartcities4010023.

Byres, E.J., Franz, M. and Miller, D., 2004, December. The use of attack trees in assessing vulnerabilities in SCADA systems. In Proceedings of the international infrastructure survivability workshop (pp. 3-10). Citeseer.

Cali, U., Kuzlu, M., Pipattanasomporn, M., Kempf, J. and Bai, L. (2021). Smart Grid Standards and Protocols. Digitalization of Power Markets and Systems Using Energy Informatics, pp.39–58. doi:10.1007/978-3-030-83301-5_3.

Carr, J., Brissette, A., Ragaini, E. and Omati, L., 2017. Managing smart grids using price responsive smart buildings. Energy Procedia, 134, pp.21-28.

carter sullivan (2020). An Introduction To The UK Smart Grid. [online] Carter Sullivan. Available at: https://www.cartersullivan.co.uk/blog/an-introduction-to-the-uk-smart-grid/#:~:text=Described%20as%20the%20%E2%80%98internet%20of%20energy%E2%80%99%2C%20the%20UK. [Accessed 7 Sep. 2022].

Chang, S.F., Chen, C.F., Wen, J.H., Liu, J.H., Weng, J.H. and Dong, J.L., 2015. Application and development of ZigBee technology for smart grid environment. Journal of Power and Energy Engineering, 3(4), pp.356-361.

Ciholas, P., Lennie, A., Sadigova, P. and Such, J.M., 2019. The security of smart buildings: a systematic literature review. arXiv preprint arXiv:1901.05837.

Cintuglu, M.H., Mohammed, O.A., Akkaya, K. and Uluagac, A.S., 2016. A survey on smart grid cyber-physical system testbeds. IEEE Communications Surveys & Tutorials, 19(1), pp.446-464.

Cleveland, F., 2005, October. IEC TC57 security standards for the power system's information infrastructure–beyond simple encryption. In Transmission and Distribution Conference and Exhibition (Vol. 2006, pp. 1079-1087).

Crain, J.A. and Bratus, S., 2015. Bolt-on security extensions for industrial control system protocols: A case study of dnp3 sav5. IEEE Security & Privacy, 13(3), pp.74-79.

Dolce, V., Jackson, C., Silvestri, S., Baker, D. and De Paola, A., 2018, June. Social-behavioral aware optimization of energy consumption in smart homes. In 2018 14th

International Conference on Distributed Computing in Sensor Systems (DCOSS) (pp. 163-172). IEEE.

Drias, Z., Serhrouchni, A. and Vogel, O., 2015, July. Taxonomy of attacks on industrial control protocols. In 2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS) (pp. 1-6). IEEE.

East, S., Butts, J., Papa, M. and Shenoi, S. (2009). A Taxonomy of Attacks on the DNP3 Protocol. IFIP Advances in Information and Communication Technology, pp.67–81. doi:10.1007/978-3-642-04798-5_5.

Ebeid, E., Rotger-Griful, S., Mikkelsen, S.A. and Jacobsen, R.H., 2015, June. A methodology to evaluate demand response communication protocols for the Smart Grid. In 2015 IEEE International Conference on Communication Workshop (ICCW) (pp. 2012-2017). IEEE.

Elgargouri, A., Virrankoski, R. and Elmusrati, M., 2015, March. IEC 61850 based smart grid security. In 2015 IEEE International Conference on Industrial Technology (ICIT) (pp. 2461-2465). IEEE.

Engel, D. and Hinkle, R. (2004). *DRBizNet Project: From Today's World Boldly into* the Future. [online] Available at: https://uc-ciee.org/ciee-old/downloads/ws1004_today_future.pdf [Accessed 9 Sep. 2022].

Esquivel-Vargas, H., Caselli, M. and Peter, A., 2017, November. Automatic deployment of specification-based intrusion detection in the BACnet protocol. In Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy (pp. 25-36).

Ferst, M.K., de Figueiredo, H.F., Denardin, G. and Lopes, J., 2018, November. Implementation of secure communication with modbus and transport layer security protocols. In 2018 13th IEEE International Conference on Industry Applications (INDUSCON) (pp. 155-162). IEEE.

Fisher, D., Isler, B. and Osborne, M. (2019). BACnet Secure Connect A Secure Infrastructure for Building Automation. [online] Available at:

https://cdn.chipkin.com/assets/uploads/2022/Feb/BACnet-SC-Whitepaper-v10_Final_20180710_21-17-31-26.pdf [Accessed 14 Aug. 2022].

Fovino, I.N., Carcano, A., Masera, M. and Trombetta, A. (2009). Design and Implementation of a Secure Modbus Protocol. IFIP Advances in Information and Communication Technology, [online] pp.83–96. doi:10.1007/978-3-642-04798-5_6.

Garofalaki, Z., Kosmanos, D., Moschoyiannis, S., Kallergis, D. and Douligeris, C., 2022. Electric Vehicle Charging: a Survey on the Security Issues and Challenges of the Open Charge Point Protocol (OCPP). IEEE Communications Surveys & Tutorials.

Granzer, W. and Kastner, W., 2010, July. Communication services for secure building automation networks. In 2010 IEEE International Symposium on Industrial Electronics (pp. 3380-3385). IEEE.

Granzer, W., Praus, F. and Kastner, W., 2009. Security in building automation systems. IEEE Transactions on Industrial Electronics, 57(11), pp.3622-3630.

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), pp.847-855.

Han, J., Choi, C.S., Park, W.K. and Lee, I., 2011, June. Green home energy management system through comparison of energy usage between the same kinds of home appliances. In 2011 IEEE 15th International Symposium on Consumer Electronics (ISCE) (pp. 1-4). IEEE.

Hayes, G. and El-Khatib, K., 2013, June. Securing modbus transactions using hash-based message authentication codes and stream transmission control protocol. In 2013 third international conference on communications and information technology (ICCIT) (pp. 179-184). IEEE.

Herberg, U., Mashima, D., Jetcheva, J.G. and Mirzazad-Barijough, S., 2014, November. OpenADR 2.0 deployment architectures: Options and implications. In 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm) (pp. 782-787). IEEE.

Hong, S.H., Kim, S.H., Kim, G.M. and Kim, H.L. (2014). Experimental evaluation of BZ-GW (BACnet-ZigBee smart grid gateway) for demand response in buildings. Energy, 65, pp.62–70. doi:10.1016/j.energy.2013.12.008.

Hou, L., Zhang, J., Jin, N., et al. (2016) Design of Network Attack Detection and Forensics for Substation Process Layer and SMV Security Transmission. Power System Automation, 40, 87-92+155.

Huang, X. - N., Li, H., Chen, X.-S. and Liu, X.-Y. (2021). Research on Reliability Design of PROFIBUS Fieldbus System in Conventional Island of Nuclear Power Plant. Lecture Notes in Electrical Engineering, pp.332–340. doi:10.1007/978-981-16-3456-7_32.

Hussain, S.S., Farooq, S.M. and Ustun, T.S., 2020. A method for achieving confidentiality and integrity in IEC 61850 GOOSE messages. IEEE transactions on Power Delivery, 35(5), pp.2565-2567.

Iacono, J., Brown, A. and Holtham, C. (2009) Research Methods—A Case Example of Participant Observation. The Electronic Journal of Business Research Methods, 7, 39-46.

Ingram, M., Mahmud, R. and Narang, D. (2021). Informative Background on the Interoperability Requirements in IEEE Std 1547-2018. [online] Available at: https://www.nrel.gov/docs/fy21osti/77959.pdf [Accessed 13 Aug. 2022].

Islam, K., Shen, W. and Wang, X., 2012, May. Security and privacy considerations for wireless sensor networks in smart home environments. In Proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design (CSCWD) (pp. 626-633). IEEE.

Jing, K., Dong, L. and Sun, Y. (2015) Research and Application of Intelligent Substation Monitoring and Early Warning System. Electric Power Information and Communication Technology, 13, 153-157.

Johnstone, M.N., Peacock, M. and den Hartog, J.I., 2015. Timing attack detection on BACnet via a machine learning approach.

Jokar, P. and Leung, V.C., 2016. Intrusion detection and prevention for ZigBee-based home area networks in smart grids. IEEE Transactions on Smart Grid, 9(3), pp.1800-1811.

Kanabar, M.G. and Sidhu, T.S., 2009, July. Reliability and availability analysis of IEC 61850 based substation communication architectures. In 2009 IEEE Power & Energy Society General Meeting (pp. 1-8). IEEE.

Kong, W., Shen, J., Vijayakumar, P., Cho, Y. and Chang, V., 2020. A practical group blind signature scheme for privacy protection in smart grid. Journal of Parallel and Distributed Computing, 136, pp.29-39.

Kumar, N., Aujla, G.S., Das, A.K. and Conti, M., 2019. ECCAuth: A secure authentication protocol for demand response management in a smart grid system. IEEE Transactions on Industrial Informatics, 15(12), pp.6572-6582.

Lauss, G.F., Faruque, M.O., Schoder, K., Dufour, C., Viehweider, A. and Langston, J., 2015. Characteristics and design of power hardware-in-the-loop simulations for electrical power systems. IEEE Transactions on Industrial Electronics, 63(1), pp.406-417.

Lázaro, J., Astarloa, A., Rodríguez, M., Bidarte, U. and Jiménez, J., 2021. A Survey on Vulnerabilities and Countermeasures in the Communications of the Smart Grid. Electronics, 10(16), p.1881

Lee, B., Kim, D.-K., Yang, H. and Jang, H. (2015). Role-based access control for substation automation systems using XACML. Information Systems, 53, pp.237–249. doi:10.1016/j.is.2015.01.007.

Lee, D., Kim, H., Kim, K. and Yoo, P.D., 2014, January. Simulated attack on dnp3 protocol in scada system. In Proceedings of the 31th Symposium on Cryptography and Information Security, Kagoshima, Japan (pp. 21-24).

Levy, R., Herter, K. and Hofmann, R., 2011. Technical Options to Address Cyber Security, Interoperability and Other Issues with ZigBee SEP.

Liu, Y., Pang, Z., Dán, G., Lan, D. and Gong, S., 2018. A taxonomy for the security assessment of IP-based building automation systems: The case of thread. IEEE Transactions on Industrial Informatics, 14(9), pp.4113-4123.

Lu, X., Wang, W. and Ma, J. (2012). Authentication and Integrity in the Smart Grid: An Empirical Study in Substation Automation Systems. International Journal of Distributed Sensor Networks, 8(6), p.175262. doi:10.1155/2012/175262.

Ma, Q., Wang, W., Guan, T., Liu, Y. and Lin, L., 2020. Modbus Protocol Based on the Characteristics of the Transmission of Industrial Data Packet Forgery Tampering and Industrial Security Products Testing. In Advances in Intelligent Information Hiding and Multimedia Signal Processing (pp. 335-344). Springer, Singapore

Majdalawieh, M., Parisi-Presicce, F. and Wijesekera, D., 2005, December. Distributed network protocol security (DNPSec) security framework. In Proceedings of the 21st Annual Computer Security Applications Conference, Tucson, Arizona.

McParland, C., 2011, July. OpenADR open source toolkit: Developing open source software for the Smart Grid. In 2011 IEEE Power and Energy Society General Meeting (pp. 1-7). IEEE.

Mohagheghi, S., Stoupis, J. and Wang, Z., 2009, March. Communication protocols and networks for power systems-current status and future trends. In 2009 IEEE/PES Power Systems Conference and Exposition (pp. 1-9). IEEE.

Mohan, A. and Mashima, D., 2014, May. Towards secure demand-response systems on the cloud. In 2014 IEEE International Conference on Distributed Computing in Sensor Systems (pp. 361-366). IEEE.

Moreira, N., Molina, E., Lázaro, J., Jacob, E. and Astarloa, A., 2016. Cyber-security in substation automation systems. Renewable and Sustainable Energy Reviews, 54, pp.1552-1562.

Mossin, E.A. and Brandão, D., 2012, March. Intelligent diagnostic for PROFIBUS DP networks. In 2012 IEEE International Conference on Industrial Technology (pp. 772-777). IEEE.

Müller, T. and Doran, H.D., 2018, June. Protecting PROFINET cyclic real-time traffic: A performance evaluation and verification platform. In 2018 14th IEEE International Workshop on Factory Communication Systems (WFCS) (pp. 1-4). IEEE.

Narayan, A. (2020). Demand Response Optimization and Management System for Real-TIme (DROMS-RT). AutoGrid Systems, Inc., Redwood City, CA (United States). doi:10.2172/1595092.

Nast, M., Butzin, B., Golatowski, F. and Timmermann, D., 2019, May. Performance analysis of a secured bacnet/ip network. In 2019 15th IEEE International Workshop on Factory Communication Systems (WFCS) (pp. 1-8). IEEE.

Olivares, D.E., Mehrizi-Sani, A., Etemadi, A.H., Cañizares, C.A., Iravani, R., Kazerani, M., Hajimiragha, A.H., Gomis-Bellmunt, O., Saeedifard, M., Palma-Behnke, R. and Jiménez-Estévez, G.A., 2014. Trends in microgrid control. IEEE Transactions on smart grid, 5(4), pp.1905-1919.

Pandey, R.K. and Misra, M., 2016, December. Cyber security threats—Smart grid infrastructure. In 2016 National power systems conference (NPSC) (pp. 1-6). IEEE.

Paranjpe, M., 2011. Security and privacy in demand response systems in smart grid.

Parian, C., Guldimann, T. and Bhatia, S., 2020. Fooling the master: Exploiting weaknesses in the Modbus protocol. Procedia Computer Science, 171, pp.2453-2458.

Park, T. and Hong, S.H., 2010, July. A new proposal of network management system for BACnet and its reference model. In 2010 8th IEEE International Conference on Industrial Informatics (pp. 28-33). IEEE.

Phillips, B., Gamess, E. and Krishnaprasad, S., 2020, April. An evaluation of machine learning-based anomaly detection in a SCADA system using the modbus protocol. In Proceedings of the 2020 ACM Southeast Conference (pp. 188-196).

Pricop, E., 2015. Security of industrial control systems-an emerging issue in romania national defense. Scientific Bulletin" Mircea Cel Batran" Naval Academy, 18(2), p.142.

Qi, J., Hahn, A., Lu, X., Wang, J. and Liu, C.-C. (2016). Cybersecurity for distributed energy resources and smart inverters. IET Cyber-Physical Systems: Theory & Applications, 1(1), pp.28–39. doi:10.1049/iet-cps.2016.0018.

Radoglou-Grammatikis, P., Sarigiannidis, P., Efstathopoulos, G., Karypidis, P.A. and Sarigiannidis, A., 2020, August. DIDEROT: An intrusion detection and prevention system for DNP3-based SCADA systems. In Proceedings of the 15th International Conference on Availability, Reliability and Security (pp. 1-8).

Rashid, M.T.A., Yussof, S., Yusoff, Y. and Ismail, R., 2014, November. A review of security attacks on IEC61850 substation automation system network. In Proceedings of the 6th International Conference on Information Technology and Multimedia (pp. 5-10). IEEE.

Reda, H.T., Anwar, A., Mahmood, A.N. and Tari, Z., 2021. A taxonomy of cyber defence strategies against false data attacks in smart grid. arXiv preprint arXiv:2103.16085.

Roh, H.T. and Lee, J.W., 2015. Residential demand response scheduling with multiclass appliances in the smart grid. IEEE Transactions on Smart Grid, 7(1), pp.94-104.

Rusitschka, S., Eger, K. and Gerdes, C., 2010, October. Smart grid data cloud: A model for utilizing cloud computing in the smart grid domain. In 2010 First IEEE international conference on smart grid communications (pp. 483-488). IEEE.

Sami, A., Abdullah, K., Davanian, A. and Azimi, M., 2013. Era of Insecure Industrial Control Systems and Calamities to Come. Journal of Electronic Systems Volume, 3(4), p.155.

Shahzad, A., Lee, M., Lee, Y.-K., Kim, S., Xiong, N., Choi, J.-Y. and Cho, Y. (2015). Real Time MODBUS Transmissions and Cryptography Security Designs and Enhancements of Protocol Sensitive Information. Symmetry, 7(3), pp.1176–1210. doi:10.3390/sym7031176.

Sidhu, T.S., Kanabar, M.G. and Parikh, P.P., 2008, December. Implementation issues with IEC 61850 based substation automation systems. In Fifteenth National Power Systems Conference (NPSC), IIT Bombay.

Subrahmanyam, P.A., Wagner, D., Mulligan, D., Jones, E., Shankar, U. and Lerner, J., 2005. Network security architecture for demand response/sensor networks.

Tariq, M., Zhou, Z., Wu, J., Macuha, M. and Sato, T., 2012, October. Smart grid standards for home and building automation. In 2012 IEEE International Conference on Power System Technology (POWERCON) (pp. 1-6). IEEE.

Tawde, R., Nivangune, A. and Sankhe, M., 2015, March. Cyber security in smart grid SCADA automation systems. In 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS) (pp. 1-5). IEEE.

Tidrea, A., Korodi, A. and Silea, I., 2019. Cryptographic considerations for automation and SCADA systems using trusted platform modules. Sensors, 19(19), p.4191.

Treytl, A., Sauter, T. and Schwaiger, C., 2004, September. Security measures for industrial fieldbus systems-state of the art and solutions for ip-based approaches. In IEEE International Workshop on Factory Communication Systems, 2004. Proceedings. (pp. 201-209). IEEE.

Upreti, A., Cardell, J. and Thiebaut, D., 2019. Data Privacy in the Smart Grid: A Decentralized Approach.

Ustun, T.S. and Hussain, S.S., 2020. IEC 62351-4 security implementations for IEC 61850 MMS messages. IEEE Access, 8, pp.123979-123985.

Vaidya, B., Makrakis, D. and Mouftah, H.T., 2013. Authentication and authorization mechanisms for substation automation in smart grid network. IEEE Network, 27(1), pp.5-11.

Vardakas, J.S., Zorba, N. and Verikoukis, C.V., 2014. A survey on demand response programs in smart grids: Pricing methods and optimization algorithms. IEEE Communications Surveys & Tutorials, 17(1), pp.152-178.

Vojdani, A. (2008). Energy Use in Buildings Enabling Technologies Title California Demand Response Business Network (DRIbiznet). [online] Available at: https://escholarship.org/content/qt2p65m9cj/qt2p65m9cj.pdf?t=qzy2jx [Accessed 9 Sep. 2022].

Volkova, A., Niedermeier, M., Basmadjian, R. and de Meer, H. (2019). Security Challenges in Control Network Protocols: A Survey. IEEE Communications Surveys & Tutorials, 21(1), pp.619–639. doi:10.1109/comst.2018.2872114.

Wang, W. and Lu, Z. (2013). Cyber security in the Smart Grid: Survey and challenges. Computer Networks, [online] 57(5), pp.1344–1371. doi:10.1016/j.comnet.2012.12.017.

Watson, V., Lou, X. and Gao, Y. (2017). A Review of PROFIBUS Protocol Vulnerabilities - Considerations for Implementing Authentication and Authorization Controls. Proceedings of the 14th International Joint Conference on e-Business and Telecommunications. doi:10.5220/0006426504440449.

Wermann, A.G., Bortolozzo, M.C., da Silva, E.G., Schaeffer-Filho, A., Gaspary, L.P. and Barcellos, M., 2016, April. ASTORIA: A framework for attack simulation and evaluation in smart grids. In NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium (pp. 273-280). IEEE.

Yardley, T., Berthier, R., Nicol, D. and Sanders, W.H., 2013, February. Smart grid protocol testing through cyber-physical testbeds. In 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT) (pp. 1-6). IEEE.

Yassine, A., 2016, July. Implementation challenges of automatic demand response for households in smart grids. In 2016 3rd International Conference on Renewable Energies for Developing Countries (REDEC) (pp. 1-6). IEEE.

Yee, G. (2006a). California Demand Response Business Network (DRBizNet) Field Simulation Workshop. escholarship.org. [online] Available at: https://escholarship.org/uc/item/08h732xz [Accessed 9 Sep. 2022].

Yee, G. (2006b). Energy Use in Buildings Enabling Technologies Title California Demand Response Business Network (DRBizNet) Field Simulation Workshop. [online] Available at: https://escholarship.org/content/qt08h732xz/qt08h732xz.pdf?t=qzy2jv [Accessed 9 Sep. 2022].

Yi, P., Iwayemi, A. and Zhou, C. (2011). Building Automation Networks for Smart Grids. International Journal of Digital Multimedia Broadcasting, 2011, pp.1–12. doi:10.1155/2011/926363.

Yimer, T., Smith, E., Harvey, P., Tienteu, M. and Kornegay, K., 2022, June. Error Correction Attacks on BACnet MS/TP. In 2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST) (pp. 77-80). IEEE.

Yu, S., Park, K., Lee, J., Park, Y., Park, Y., Lee, S. and Chung, B., 2020. Privacy-preserving lightweight authentication protocol for demand response management in smart grid environment. Applied Sciences, 10(5), p.1758.

Yunus, B., Musa, A., Ong, H.S., Khalid, A.R. and Hashim, H., 2008, December. Reliability and availability study on substation automation system based on IEC 61850. In 2008 IEEE 2nd International Power and Energy Conference (pp. 148-152). IEEE.

Zhang, Y. (2017) Intelligent Substation Network Communication Online Monitoring System. Nanjing University of Science and Technology, Nanjing.

Zhou, X., Ma, Y., Gao, Z. and Wang, H., 2017, August. Summary of smart metering and smart grid communication. In 2017 IEEE International Conference on Mechatronics and Automation (ICMA) (pp. 300-304). IEEE.