

Enhancement of Cyber Security in Substation Projects

Filip Bengs

Degree Thesis for Bachelor of Engineering

Degree Programme in Electrical Engineering and Automation

Vaasa 2023

DEGREE THESIS

Author: Filip Bengs

Degree Programme and place of study: Electrical Engineering and Automation, Vaasa

Specialisation: Information Technology

Supervisor(s): Jan Berglund, Mats Warg

Title: Enhancement of Cyber Security in Substation Projects

Date: 24.5.2023 Number of pages: 57 Appendices: 0

Abstract

This bachelor's thesis was conducted for the Automation department at VEO Oy. The research was performed to better understand and be able to reduce the cyber security risks in VEO's substation projects. The purpose of the thesis was to identify cyber security risks of the IEC 60870-5-104 communication between RTUs and SCADA systems and to find a cost-efficient and well-supported solution for mitigating these risks.

The theoretical part examines topics such as the OSI model, TCP/IP, and the IEC 60870-5-101/104 protocols. Additionally, it addresses topics such as the various phases of a cyber-attack, specific types of cyber-attacks, and mitigation solutions such as IEC 62351 and VPNs.

The first part of the empirical section describes the test environment that was set up for this thesis. The cyber-attacks presented in the theoretical part were then performed in the test environment. Having examined the attacks and their implications, a solution was presented and tested to assess its ability to effectively prevent these attacks.

The result of this thesis was an improved understanding of the cyber security risks of the IEC 60870-5-104 communication between RTUs and SCADA systems in VEO's substation projects. A suitable solution to mitigate these risks was found in the IPsec VPN protocol.

Language: English

Key Words: IEC 60870-5-104, Cyber Security, Cyber Attack, RTU, SCADA

EXAMENSARBETE

Författare: Filip Bengs

Utbildning och ort: El- och automationsteknik, Vasa

Inriktning: Informationsteknik

Handledare: Jan Berglund, Mats Warg

Titel: Förbättring av cybersäkerhet i elstationsprojekt

Datum: 24.5.2023 Sidantal: 57

Bilagor: 0

Abstrakt

Examensarbetet har utförts för automationsavdelningen på VEO Oy. Undersökningen genomfördes för att bättre förstå och kunna minska cybersäkerhetsriskerna i VEO:s elstationsprojekt. Syftet med arbetet var att identifiera cybersäkerhetsriskerna med den IEC 60870-5-104-baserade kommunikationen mellan RTU-enheter och SCADA-system, samt att hitta en kostnadseffektiv och väletablerad lösning för att minska dessa risker.

Den teoretiska delen behandlar ämnen som OSI-modellen, TCP/IP och IEC 60870-5-101/104-protokollen. Därutöver behandlas ämnen som de olika skedena av en cyberattack, specifika typer av cyberattacker samt lösningar för att motverka dessa attacker, såsom IEC 62351 och VPN.

Empiriska delen inleds med en beskrivning av den testmiljö som byggdes upp för detta arbete. De cyberattacker som presenterades i den teoretiska delen genomfördes sedan i testmiljön. Efter att ha undersökt attackerna och deras konsekvenser presenterades och testades en lösning för att bedöma dess förmåga att effektivt motverka dessa attacker.

Resultatet av detta arbete var en förbättrad förståelse för cybersäkerhetsriskerna med den IEC 60870-5-104-baserade kommunikationen mellan RTU-enheter och SCADA-system i VEO:s elstationsprojekt. En lämplig lösning för att motverka dessa risker hittades i IPsec VPN-protokollet.

Språk: engelska

Nyckelord: IEC 60870-5-104, Cybersäkerhet, Cyberattack, RTU, SCADA

OPINNÄYTETYÖ

Tekijä: Filip Bengs

Koulutusohjelma ja paikka: Sähkö- ja automaatiotekniikka, Vaasa

Suuntautumisvaihtoehto: Tietotekniikka

Ohjaajat : Jan Berglund, Mats Warg

Nimike: Kyberturvallisuuden parantaminen sähköasemissa

Päivämäärä: 24.5.2023

Sivumäärä: 57

Liitteet: 0

Tiivistelmä

Opinnäytetyö on suoritettu VEO Oy:n automaatio-osastolle. Tutkimus toteutettiin paremman ymmärryksen saavuttamiseksi ja kyberturvallisuusriskien vähentämiseksi VEO:n sähköasemaprojekteissa. Työn tarkoituksena oli tunnistaa IEC 60870-5-104-pohjaisen viestinnän RTU-laitteiden ja SCADA-järjestelmien väliset kyberturvallisuusriskit sekä löytää kustannustehokkaan ja vakiintuneen ratkaisun näiden riskien vähentämiseksi.

Työn teoreettinen osa käsittelee aiheita kuten OSI-malli, TCP/IP ja IEC 60870-5-101/104-protokollat. Lisäksi käsitellään kyberhyökkäyksien eri vaiheita, tiettyjä kyberhyökkäystyyppisiä ja eri ratkaisuja näiden hyökkäysten torjumiseksi, kuten IEC 62351 ja VPN.

Työn empiirinen osa alkaa kuvaamalla tätä työtä varten luotua testiympäristöä. Teoreettisessa osassa esitellyt kyberhyökkäykset suoritettiin tämän jälkeen testiympäristössä. Hyökkäysten ja niiden seurausten tutkimisen jälkeen esitettiin ratkaisu sekä testattiin ratkaisun kykyä estää hyökkäyksiä tehokkaasti.

Tämän työn tuloksena saavutettiin parempi ymmärrys IEC 60870-5-104-pohjaisen viestinnän RTU-laitteiden ja SCADA-järjestelmien välisistä kyberturvallisuusriskeistä VEO:n sähköasemaprojekteissa. Sopiva ratkaisu näiden riskien torjumiseksi löytyi IPsec VPN-protokollasta.

Kieli: Englanti

Avainsanoja: IEC 60870-5-104, Kyberturvallisuus, Kyberhyökkäys, RTU, SCADA

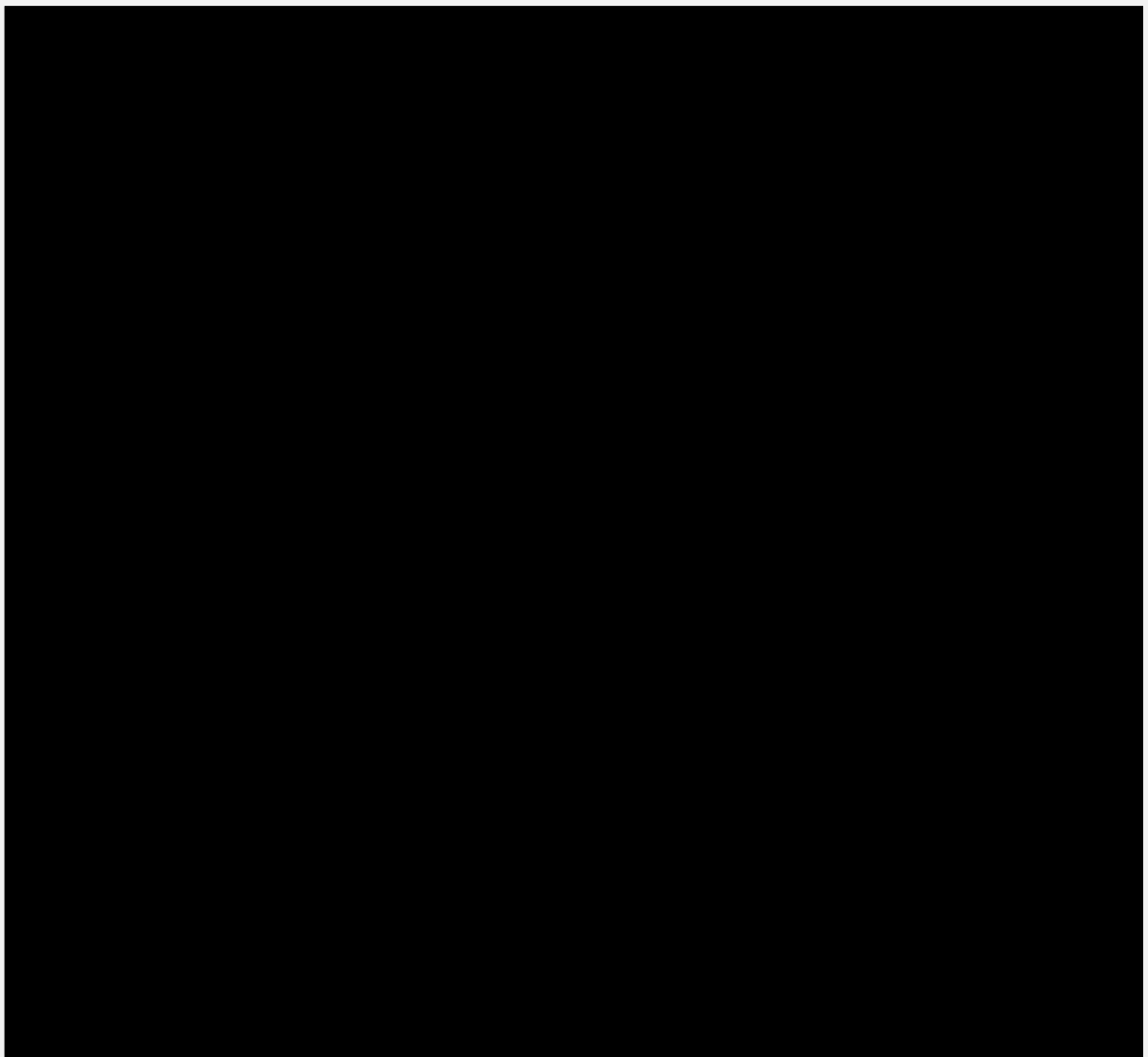
Table of Contents

1	Introduction.....	1
1.1	Purpose.....	2
1.2	Limitations.....	2
1.3	VEO Oy.....	2
2	Theory.....	4
2.1	Substations.....	4
2.2	RTU.....	4
2.3	SCADA.....	5
2.4	OSI model.....	5
2.4.1	Physical layer (Layer 1).....	7
2.4.2	Data Link Layer (Layer 2).....	8
2.4.3	Network Layer (Layer 3).....	9
2.4.4	Transport Layer (Layer 4).....	10
2.5	TCP/IP.....	11
2.5.1	Network Interface Layer.....	13
2.5.2	Internet Layer.....	14
2.5.3	Transport Layer.....	14
2.5.4	Application layer.....	14
2.5.5	TCP Three-way handshake.....	15
2.6	IEC 60870-5-101.....	16
2.6.1	History.....	16
2.6.2	Architecture.....	17
2.6.3	Communication modes.....	18
2.6.4	Application Service Data Unit.....	18
2.6.5	Information Objects.....	19
2.6.6	Frame formats.....	20
2.7	IEC 60870-5-104.....	21
2.7.1	Architecture.....	21
2.7.2	Application Protocol Data Unit.....	22
2.7.3	Security issues with IEC 104.....	23
2.8	Cyber-attacks against IEC 104-based ICS systems.....	23
2.8.1	Detection phase.....	24
2.8.2	Capture phase.....	24
2.8.3	Attack phase.....	25
2.8.4	Replay attack.....	25

2.8.5	Injection attack	26
2.9	Solutions to increase security	26
2.9.1	IEC 62351-3 & IEC 62351-5.....	27
2.9.2	VPN	27
2.10	IPsec.....	28
2.10.1	IKE phase 1	29
2.10.2	IKE phase 2	30
2.10.3	Encapsulation mode	30
2.10.4	IPsec Protocol.....	31
3	Test environment	33
3.1	Technologies used	33
3.1.1	VMware Workstation Pro 16.....	33
3.1.2	DemoWinPP104.....	33
3.1.3	Qttester104.....	34
3.1.4	pfSense	34
3.1.5	Kali Linux.....	34
3.1.6	Wireshark.....	34
3.1.7	Ettercap	35
3.2	1 st Test network	35
3.3	2 nd Test network	36
4	Attacking the test environment	37
4.1	Identifying IEC 104 traffic.....	37
4.2	Becoming Man-in-the-Middle	37
4.3	Dropping packets	37
4.4	Replay attack.....	37
4.5	Injection attack	37
5	Testing the IPsec solution.....	38
5.1	Identifying encrypted IEC 104 traffic	38
5.2	Dropping encrypted IEC 104 packets.....	38
5.3	Conclusion of IPsec testing	38
6	Discussion	39
7	References	40

List of Figures

Figure 1. Significant cyber incidents worldwide, 2006-2019 [1]	1
Figure 2. VEO's key figures from the 2021 Annual Report [3]	2
Figure 3. Data encapsulation in the OSI model [10].....	6
Figure 4. Comparing the OSI and TCP/IP Models [11].....	12
Figure 5 TCP Sequence Number Synchronization [13].....	16
Figure 6. Comparing OSI Model and EPA [14]	17
Figure 7 The ASDU format [15].....	18
Figure 8 The format of an information object [15]	20
Figure 9 IEC 101 frame format [15]	21
Figure 10 APDU structure in IEC 104 [15].....	23
Figure 11 IPsec Phase 1 and 2 tunnels [18]	30
Figure 12 IPsec Transport mode [18]	31
Figure 13 IPsec tunnel mode [18].....	31
Figure 14 IP packet with AH header [18].....	32
Figure 15 IP packet with ESP header and trailer [18]	32
Figure 16 1 st Test network and devices	35
Figure 17 2nd Test network and devices.....	36



List of Tables

Table 1. The OSI model.....	7
Table 2. Comparison of IEC 101 & IEC 104	22
Table 3. Most common RTUs and SCADA systems in VEO's substation projects (hidden for secrecy).....	28

List of Abbreviations

AH	Authentication Header
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
CAM	Content Addressable Memory
CoT	Cause of Transmission
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial-of-Service
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
GSM	Global System for Mobile communication
HTTP	Hypertext Transfer Protocol
I/O	Input/Output
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IMAP	Internet Message Access Protocol
IPS	Intrusion Prevention System
IPSec	IP Security
LAN	Local Area Network
MAC	Media Access Control
MAN	Metropolitan Area Network
NFS	Network File System
OSI	Open Systems Interconnection
PLC	Programmable Logic Controller
PPP	Point-to-Point Protocol
RIP	Routing Information Protocol
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

List of Definitions

IEC 101 & IEC 104	For simplicity's sake, the term IEC 101 will be used in place of IEC 60870-5-101, and IEC 104 in place of IEC 60870-5-104 during this thesis.
Bit	A bit, short for <i>binary digit</i> is the smallest unit of digital information that a computer can understand. At the lowest level of computing, all types of data in a computer system are represented as bits. Since a bit is binary it can only have one of two values, either 0 or 1.
Protocol	A protocol can be thought of as a set of rules for messages and procedures that allow machines and/or applications to exchange information. For the receiver to understand the sender's messages, both machines must follow the common rules defined by the particular protocol in use.
Message	A message refers to a unit of data, such as a forum post or a chat message, that is transmitted between network devices. A message typically consists of the data itself, also known as the payload, and so-called header and footer fields, which e.g., provide information about the message and its destination.
Internetwork	The word internetwork simply means a (large) network consisting of multiple smaller networks. The most common internetwork is the global public network that is accessible to anyone, the so-called Internet.

Telecontrol	Telecontrol enables the remote monitoring and management of industrial processes, such as substations, without the need for physical intervention on-site. In this thesis, telecontrol will be discussed in the context of communication between SCADA systems and RTUs.
Control Station	Also known as a master station, a central facility that oversees and controls an industrial system. In the context of this thesis, a control station refers to a SCADA system.
Remote Station	A location where RTUs are installed. The remote station collects data from sensors, performs local control functions, and communicates with the control station. In the context of this thesis remote stations refer to RTUs.
MitM Attack	A so-called Man-in-the-Middle attack is where an attacker intercepts and relays communication between two network devices, without their knowledge. By being positioned between the two devices, the attacker can listen in on the communication and even potentially modify the data in-transit.
Hashing	Hashing refers to the process of applying a mathematical algorithm to input data to generate a fixed-size output called the <i>hash value</i> . This is useful for a wide array of tasks, such as verifying data integrity and digital signatures.

1 Introduction

Electrical substations play an integral part in the transmission and distribution of electricity in the modern power grid. Substations are one of the essential components without which power grids would be unable to operate effectively.

With cyber-attacks against critical infrastructure becoming more common [1], substations and other critical parts of the power grid are at ever-growing risk of being attacked. To mitigate these risks, the need to continuously stay up to date and make sure that this critical infrastructure is secured is higher than ever before.

Figure 1 depicts how the amount of significant cyber incidents worldwide has increased over the years. Even though electricity-related incidents have so far been relatively low, it is very important to secure these systems, as cyber-attacks can be expensive and dangerous, both to humans and the environment.

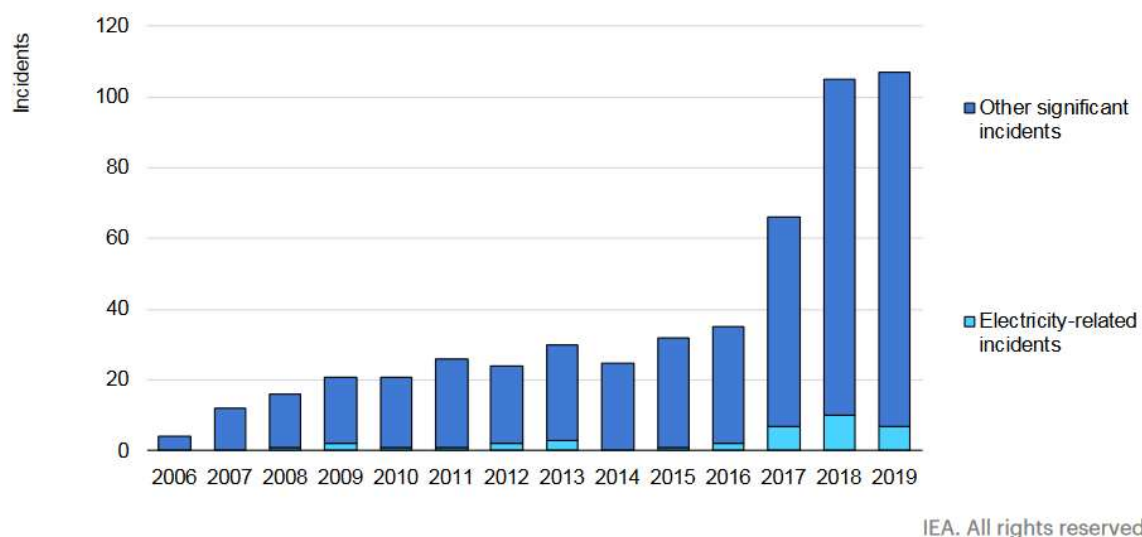


Figure 1. Significant cyber incidents worldwide, 2006-2019 [1]

This thesis is conducted for the *Automation* department at VEO Oy. It focuses on improving the cyber security of IEC 104 communication between RTUs and SCADA systems in VEO's substation projects.

1.1 Purpose

This thesis investigates the risks of unencrypted and unauthenticated telecontrol messages between SCADA systems and RTUs using the IEC 104 protocol and aims to find ways of mitigating them. The purpose of the thesis is to find a solution to secure this communication so that it can be implemented in both operational and upcoming substation projects.

1.2 Limitations

With the goal of improving Cyber Security, there is an endless number of solutions one could choose to implement. To keep the scope of this thesis concise, the focus will be specifically on improving the security of IEC 104 communication between SCADA systems and RTUs.

In the future, further work could be done to improve the security of other aspects of these projects.

1.3 VEO Oy

Vaasa Engineering Oy was founded in 1989 by Harri Niemelä and Mauri Holma. The company formally changed its name to VEO in 2012. [2] *Figure 2* shows VEO's key figures from its 2021 Annual report.

VEO'S 2021 IN NUMBERS	
Turnover 124.8 M€	Operating Margin (EBITDA) 4.6 M€
Operating Profit (EBIT) 2.3 M€	Orders 103.2 M€
Net Profit 1.4 M€	Net Cash Flow 1.0 M€

Figure 2. VEO's key figures from the 2021 Annual Report [3]

Taken from VEO's website, the company introduces itself as follows:

“VEO is an energy expert offering electrification and automation solutions for its customers. More than half of the company's revenue comes from renewable energy solutions. VEO's headquarter is located in Vaasa, Finland and the company also has subsidiaries in Sweden, Norway, and the UK. VEO Group employs 500 persons and had a turnover of EUR 124.8 million in 2021.” [4]

2 Theory

This chapter contains the theory on which the thesis is based upon.

2.1 Substations

Substations are an essential part of the power grid and are used for electrical transmission and distribution. A substation is a junction (node) in the power grid that safely connects and routes incoming and outgoing electricity. [5]

There are multiple types of substations, depending on the station's purpose and its equipment. The most common types are transformer and switching substations. [5]

Transformer and *Switching substations* both distribute electrical energy in the grid. What differentiates these two is that transformer substations transform the voltage between different levels while switching substations operate at a single voltage level. [5]

2.2 RTU

RTU, short for *Remote Terminal Unit*, is a hardware device used to communicate between the central SCADA system and physical control and protection units, e.g., PLCs or relays. An RTU may include I/Os for measuring and sending both digital and analog signals, such as power and voltage measurements. This data is interpreted and encoded into a digital format and sent to the SCADA system's monitoring equipment. [6]

In SCADA systems, RTUs and PLCs perform most of the on-site control. So, what differentiates these two devices? The usage of RTUs focuses on remote monitoring and communication, with higher demand for application communications and protocol availability. On the other hand, PLC usage focuses on fast, localized control of discrete variables, taking in analog or digital input and executing a logical program loop based on these inputs. [7]

To provide a reliable communication link between the SCADA system and on-site RTUs, RTU manufacturers include multiple communication media that can be used. Some examples of communication media are dial-up phone lines, GSM, satellite, IEEE 802.3 (Ethernet), and IEEE 802.11 (WLAN). [7]

Usual communication protocols used between SCADA and RTUs are DNP3, Modbus, IEC 61850, IEC 101, and IEC 104. The main protocol that VEO uses in substation projects for SCADA-RTU communication is IEC 104, which will be discussed in greater detail in section 2.7.

RTU-to-RTU and RTU-to-PLC communication can also be performed with multiple communication protocols. Usual protocols for this use-case are IEC 61850 and IEC 101/IEC 104.

2.3 SCADA

SCADA, short for Supervisory Control and Data Acquisition, is a computer system used for remote control and supervision of machines and processes. SCADA systems are used for many different industrial applications, such as power plants, water distribution plants, controlling transport of gas and oil in pipelines, etc. [8] In the context of VEOs substation projects, the SCADA system usually communicates with an RTU to monitor and control a substation.

In most VEO substation projects, the SCADA system is installed and operated by the customer or another third party. This can result in the customer choosing a SCADA system that doesn't support encrypted IEC 104 communication. To account for this, the encryption and authentication of IEC 104 traffic will most likely have to be handled by another piece of hardware, such as an additional router creating a VPN tunnel to secure the communication.

2.4 OSI model

Many protocols are built upon the 7-layered OSI (Open Systems Interconnection) model. The model provides a reference for how to build up messages to be sent across a network. The model is designed so that the data is processed through at least some, if not all of the 7 layers, before being sent across the network. To successfully send a message across a network, a minimum of three OSI layers must be used. These are the Physical (layer 1), the Data Link (layer 2), and the Network (layer 3) layers. [6]

When sending a message, the data goes through the OSI model from top to bottom, i.e., from the highest (layer 7) to the lowest (layer 1). Each layer adds to or modifies the message to be sent, by encapsulating the data, also known as the *payload*, with so-called *header* and *footer* fields. These header and footer fields contain protocol-specific data, such as the source and destination IP addresses (layer 3), what TLS cipher to use (layer 6), and information about what application is being used (layer 7). [9] This encapsulation can occur multiple times as data is passed down to lower levels of the OSI model, as illustrated in *Figure 3*.

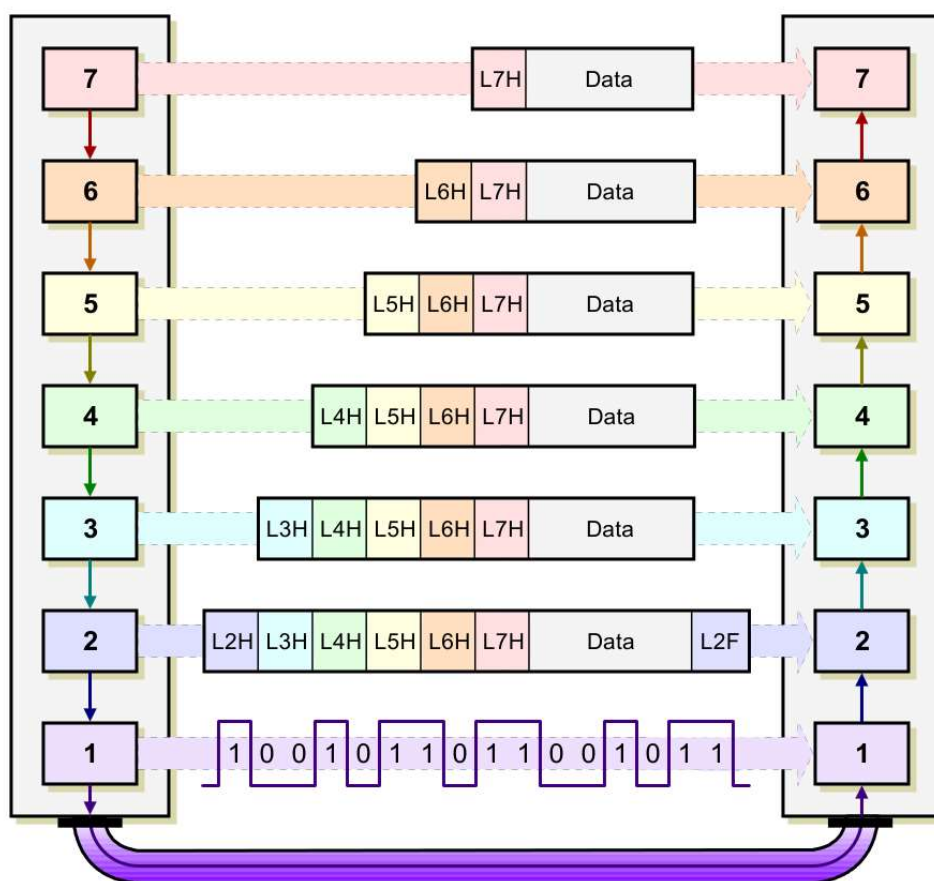


Figure 3. Data encapsulation in the OSI model [10]

As illustrated in *Figure 3*, the process is reversed when the message reaches the receiving machine. Having been received, the message gets processed through the OSI model layers from lowest to highest, stripping away all the headers and footers. When this

process is finished, the data retakes its original form so that the end application can display it to the user. [9]

The hierarchy of the OSI model and some examples of protocols, standards, and functions is illustrated in Table 1. Layers 1 to 4 of the OSI model will be discussed in further detail during the remainder of this section. The upper three layers will not be further examined, as they are not relevant to the contents of this thesis.

Table 1. The OSI model

#	Layer Name	Content	Examples of standards & protocols	Function
7	Application	User data	HTTP, FTP, SSH, DNS, Websocket, SNMP	Application data
6	Presentation	Encoded user data	SSL, TLS, IMAP, FTP, MPEG, JPEG	Presentation of application data, encryption
5	Session	Sessions	APIs, Sockets, NetBIOS	Sessions between local and remote devices
4	Transport	Datagram/Segment	TCP, UDP	Broker communication between lower (layer 1-3)
3	Network	Datagram/Packet	IP, IPv6, ICMP, ARP, IPSec, IGMP, BGP	Messages between local and remote devices
2	Data Link	Frames	IEEE 802.3 (Ethernet), IEEE 802.11 (WLAN), PPP	Low-level data between local devices
1	Physical	Bits	IEEE 802.3 (Ethernet), IEEE 802.11 (WLAN) DSL, CAN bus, USB, Bluetooth	Physical signals between local devices

2.4.1 Physical layer (Layer 1)

Out of all the layers in the OSI model, the physical layer is unique. What differentiates this layer from the others in the OSI model is that it is the only one where physical data is moved across a network interface. The other 6 layers of the model perform various useful functions, but they all rely on the physical layer to send data across the network. [9]

The physical layer has the following main functions: [9]

- *Defining hardware specifications:* Details regarding specifications for cables, network interface cards, wireless transceivers, and other devices are defined at the physical layer. These specifications include properties such as the physical layout of cables and connectors, transmission frequency, transmission voltage, and other low-level parameters.
- *Encoding and Signaling:* Data is transformed from bits to electrical or optical signals that can be transmitted across the network.
- *Data Transmission and Reception:* Data is transmitted and received over the physical network connection. Even though there is not always a physical cable connecting devices, this applies both to wired and wireless networks.

- *Topology and network design*: The network design and network topologies are defined at the physical layer. Examples of some topologies are LAN, WAN, and MAN.

In some cases, the physical layer can also perform functions that are normally associated with the Data Link Layer (Layer 2). Examples of this are bit-level repackaging of Data Link Layer frames and error detection and correction. [9]

2.4.2 Data Link Layer (Layer 2)

The data link layer, or DLL for short, serves as the main operational layer for various wired and wireless LAN technologies, such as IEEE 802.3 (Ethernet), IEEE 802.11 (WLAN), IEEE 802.5 (Token Ring) and Point-to-Point protocol (PPP). The data link layer is only concerned with getting data from one device to another if they are on the same local network. [9]

To improve the interoperability of different network technologies, the data link layer is often divided into two conceptual sublayers: the Logical Link Control (LLC) and Media Access Control (MAC) layers. [9]

The data link layer has the following main functions: [9]

- *Logical Link Control (LLC)*: Establishes and controls logical links between local network devices. It provides a uniform interface to the Network Layer (layer 3) and hides unnecessary details about the Data Link Layer to allow seamless integration with higher layers. Most LAN networks use the IEEE 802.2 (LLC) protocol to define these functions.
- *Media Access Control (MAC)*: Controls access to the network medium. Since many networks and devices can share a single physical medium, such as a single network cable or wireless signal, it is necessary to set and enforce rules to avoid conflicts over this medium. Media Access Control addresses, more commonly known as MAC addresses, are used to uniquely identify network devices in the data link layer.
- *Data Framing*: Final encapsulation of messages from higher levels of the OSI model. This step encapsulates the messages into so-called *frames*, which are then sent over the network at the physical layer (Layer 1).

- *Addressing:* This step adds information about the destination location to the message. Here MAC addresses are used to ensure that the data is properly delivered to the intended receiving machine.
- *Error Detection and Handling:* The data link layer handles errors that happen at the network stack's lower levels. An example of this is using a *cyclic redundancy check* (CRC) field to allow the receiver of the data to determine if it was received correctly.

The data link layer (layer 2) and the physical layer (layer 1) are closely related. The requirements for the physical layer of a network are often decided by what data link layer technology is being used. An example of this is the Ethernet standard (IEEE 802.3). This standard defines both the hardware specifications of the physical layer and how Ethernet works at the data link layer. [9]

2.4.3 Network Layer (Layer 3)

The network layer is similar to the data link layer (layer 2) in many ways: they both deal with addressing, encapsulation, and error handling. But unlike the data link layer, which only works on local networks, the network layer is tasked with getting data from one device to another even if they are not on the same network. [9]

The network layer has the following main functions: [9]

- *Logical Addressing:* Every device communicating over a network has at least one logical address associated with it. Unlike the addressing at the data link layer (layer 2), which is bound to physical hardware, logical addresses are independent of particular hardware. The most common protocol for logical addressing is IP (Internet Protocol), where every machine has one or multiple so-called IP addresses. An IP address looks like this: *192.168.1.10*. The value of each *octet*, which are the numbers separated by the dots, can be between 0-255.
- *Routing:* Hardware devices and software running at the network layer handles incoming packets from various sources, figures out their final destination, and then determines where they need to be sent to reach the destination.
- *Datagram Encapsulation:* Messages are placed into datagrams with a network layer header.

- *Fragmentation and Reassembly:* Depending on the data link layer (layer 2) technology being used, there may be restrictions on the size of the packets that can be sent over the data link layer. If the network layer packet to be sent is too large, the network layer splits up the packet into multiple parts and sends each part to the data link layer. When the packets arrive at the network layer of the destination machine, the parts are reassembled to form the original message.

The most common protocol used at the network layer is the Internet Protocol (IP). The Internet Protocol is a so-called connectionless protocol, which means that network devices do not establish any type of connection before sending data to each other. Connectionless protocols have multiple drawbacks compared to connection-oriented protocols, such as lack of reliability, congestion control, flow control, error correction, sequencing, and acknowledgment. To make up for these drawbacks, connection-oriented services are often provided by the transport layer (layer 4). An example of this is TCP/IP, where the TCP protocol handles the connection-oriented services at the transport layer. [9] TCP/IP will be discussed further in section 2.5.

2.4.4 Transport Layer (Layer 4)

As previously discussed, layers 1 through 3 are concerned with the packaging, addressing, routing, and delivery of data. The transport layer is different, it isn't directly concerned with moving data, that part is already handled by the three lower layers. The transport layer acts as a kind of broker between the abstract applications of the higher layers (layers 5-7), and the concrete operations of the lower layers (layers 1-3). [9]

The transport layer has the following main functions: [9]

- *Process-Level Addressing:* The transport layer uses addressing to differentiate between programs on a single device. This enables multiple programs on one device to use a network layer protocol at the same time and can be used with both TCP and UDP. This addressing is made possible by using TCP and UDP *ports*. Each port within a particular IP identifies a specific software process.
- *Multiplexing and Demultiplexing:* Transport layer protocols use the previously mentioned addressing to *multiplex* the data received from different programs for

transport. What this means is that the data is combined into a single stream before being sent. When the destination machine's transport layer receives the multiplexed stream, it gets *demultiplexed* and each package of data can be directed to the appropriate application process.

- *Segmentation, Packaging, and Reassembly:* Depending on the technologies used at the underlying network layer (layer 3), data is segmented into smaller pieces on the source machine to be sent over the network layer. This process is reversed on the receiving machine to retrieve the data that was sent.
- *Connection Establishment, Management, and Termination:* Connection-oriented protocols like TCP are responsible for establishing, maintaining, and terminating connections.
- *Acknowledgments and Retransmissions:* Many protocols implement protocols that guarantee reliable data delivery at the transport layer. This is usually accomplished by using acknowledgments and retransmissions. Whenever data is sent, the sender waits for an acknowledgment from the recipient that the data was successfully received. If no acknowledgment is received within a specified time, the data is retransmitted, to hopefully be properly received.
- *Flow Control:* Mismatches in speed between a sender and receiver can result in one of them receiving more data than it can handle. To prevent this, flow control features are often implemented, meaning that one device can tell another one it is communicating with to throttle the rate at which it sends data.

2.5 TCP/IP

Having discussed the OSI model and its 4 lowest layers, the TCP/IP model can now be examined. The TCP/IP model consists of four layers, which logically span the upper six layers of the OSI model. The only OSI layer that is not involved in the TCP/IP model is layer 1, the physical layer. [9] *Figure 4* illustrates how the TCP/IP model relates to the OSI model.

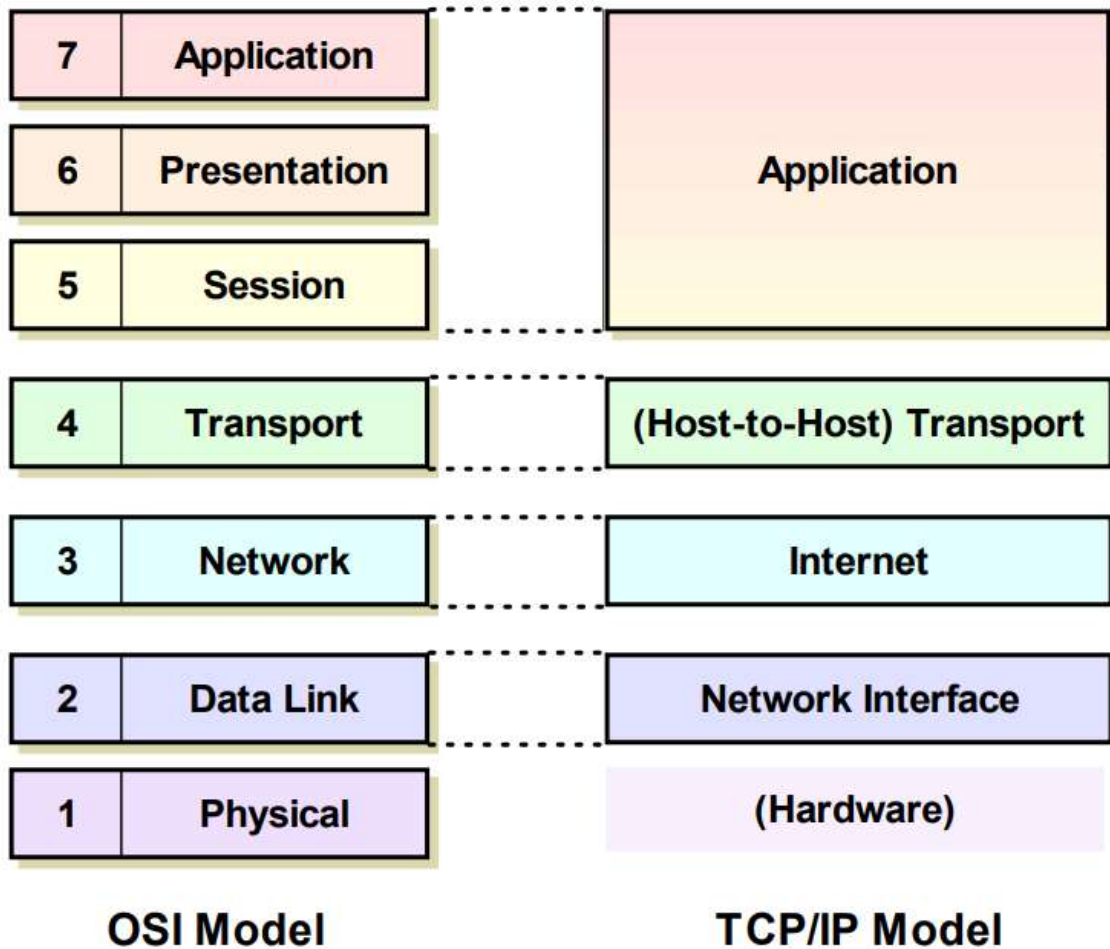


Figure 4. Comparing the OSI and TCP/IP Models [11]

As in the OSI model, data is added to the message at each layer of the model in the form of headers when sent from an application program to a receiver. When the receiver receives the message it goes through the layers in reverse, stripping off corresponding header information, ending up with usable data. [12] *Figure 5* depicts the flow of information in the TCP/IP protocol, moving in both sender and receiver direction.

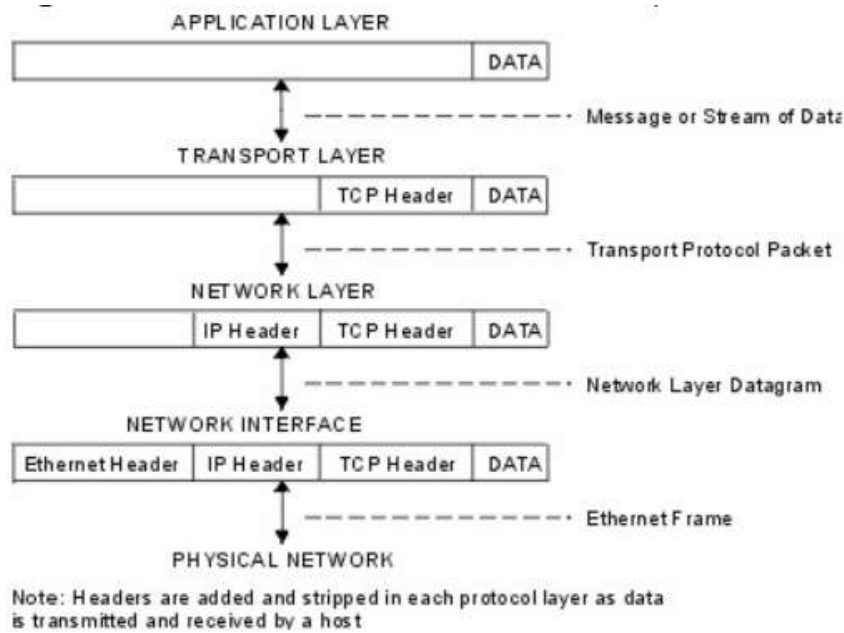


Figure 5. TCP/IP data transmission and reception [12]

Although it is often referred to as a protocol, TCP/IP is a *protocol suite*, consisting of dozens of different protocols, of which TCP and IP are the most notable ones. Other notable protocols in the TCP/IP protocol suite are, e.g., PPP, ARP, IPsec, ICMP, UDP, DNS, DHCP, SNMP, FTP, NFS, SMTP, IMAP, and HTTP. [9]

TCP/IP primarily operates under the *client/server* structural model. This refers to a system where a small number of powerful *servers* provide services to a large number of *clients*. The client, usually an end-user using some client software such as a web browser or email client, initiates the communication by sending a request for data or other resources to a server. The server responds to the client, either by directly giving the client what it requested or by informing the client where the requested resource can be found or responding with some kind of error message. [9] The four layers of the TCP/IP model will be discussed in further detail during the remainder of this section.

2.5.1 Network Interface Layer

The network interface layer is where the higher-level protocols of the TCP/IP suite interface with the local network. This layer is equivalent to the data link layer (layer 2) of the OSI model. [9]

Neither TCP nor IP runs at this layer, so data link and physical layer functions are often handled by and dictated by the network medium being used. Some common examples of this are running TCP/IP over IEEE 802.3 (Ethernet) or IEEE 802.11 (WLAN). The TCP/IP protocol suite does, however, contain protocols that implement their own data link layer functions. Examples of this are Serial Line Internet Protocol (SLIP) and Point-to-Point Protocol (PPP). [9]

2.5.2 Internet Layer

The internet layer is equivalent to the OSI model's network layer (layer 3). This layer handles typical layer three tasks, such as routing, logical device addressing, and data packaging. The Internet Protocol (IP) works at this layer, in conjunction with support protocols such as ICMP and routing protocols such as BGP and RIP. Although not yet widely adopted, IP version 6, or IPv6 for short, also operates at the internet layer. [9]

2.5.3 Transport Layer

The TCP/IP model's transport layer is equivalent to the OSI model's transport layer (layer 4). The main function of this layer is to enable end-to-end communication over an internetwork. The transport layer enables devices to make logical connections to send data to each other. As in the OSI transport layer, this is where the identification of source and destination processes is accomplished. [9]

The most commonly used protocols in the transport layer of the TCP/IP protocol suite are, of course, TCP but also UDP. One could mistakenly assume that only TCP can be used at the transport layer in the TCP/IP protocol suite, but that is not the case. The protocol suite is simply called TCP/IP because they are the two most important and most commonly used protocols. [9]

2.5.4 Application layer

The topmost layer in the TCP/IP model, the application layer, spans layers 5-7 of the OSI model. This layer is considered to be somewhat ambiguous since it covers the three upper layers of the OSI model, which themselves are inherently abstract. It is often

difficult to specify at which of the upper 3 layers a specific technology works, as it can often span more than one of them. [9]

Several protocols operate at the application layer of the TCP/IP protocol suite. Some of the more common protocols are HTTP, SMTP, FTP for end-user services, and administrative protocols such as DHCP, DNS, and SNMP. [9]

2.5.5 TCP Three-way handshake

As previously mentioned, TCP is a so-called connection-based protocol. This means that to be able to transmit data between devices, a connection must first be established. During the connection establishment, the devices exchange so-called *initial sequence numbers*, ISN for short, and various other parameters that dictate how the connection should operate. [9]

TCP uses control messages to manage the connection process. To indicate whether a TCP segment is used for control purposes or data transfer, a set of control flags are set in the TCP header. Two specific control flags are used to establish a TCP connection: [9]

- *SYN*: The SYN-flag, short for *synchronize*, indicates that a connection is being initialized.
- *ACK*: The ACK-flag, short for *acknowledgment*, indicates that a message has been successfully received.

Figure 5 illustrates the three-way handshake between a client and a server. The process can be broken down into three steps: [9]

1. First, the client chooses a random initial sequence number (ISN), in this example 4567. The client then sends a segment with the SYN-flag with the *sequence number* field set to 4567.
2. Having received the SYN message, the server chooses its own random ISN, which is 12998 in this example. It then responds with a SYN+ACK message, with an *acknowledgment number* field of 4568, which is just the client's ISN + 1, and a sequence number field of 12998.

- Seeing that the server has correctly received and acknowledged the SYN message, the client responds with a final ACK message, this time with the sequence number of the server's ISN + 1.

A TCP connection has now been established, allowing the devices to start sending segments of data between each other. The first segment that the client sends to the server will have the sequence number 4568 and the server's next sequence number will be 12999. [9]

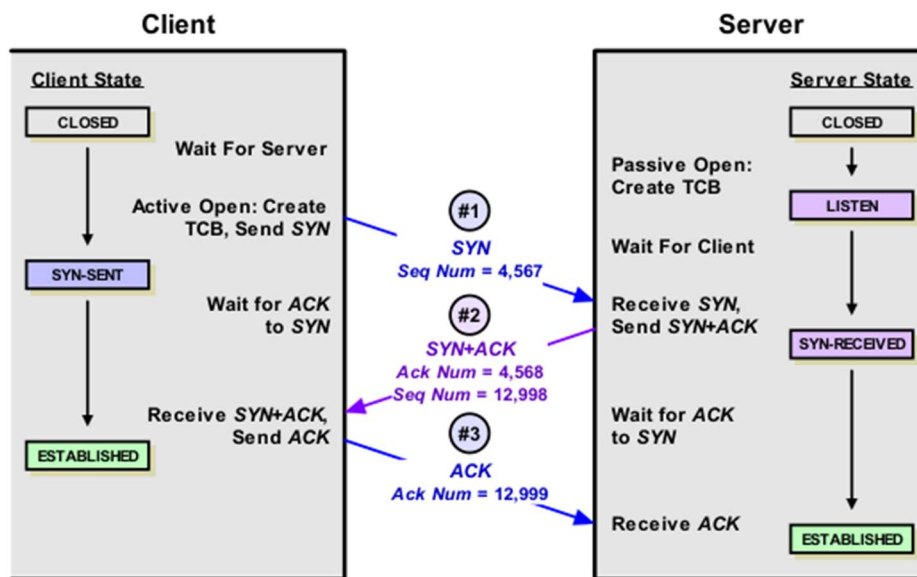


Figure 5 TCP Sequence Number Synchronization [13]

2.6 IEC 60870-5-101

Although this thesis will focus on the IEC 104 protocol, the fundamental concepts of IEC 101 first have to be explained. This section will explain the history of the IEC 60870-5 set of standards and some basic functionality of IEC 101.

2.6.1 History

In the 1980s, as manufacturers kept introducing more proprietary and patented networking and automation solutions to the market, the need for an international standard kept growing. Since these systems were built upon patented communications protocols, they were not easily integrated with protocols and devices created by other manufacturers. This led to the buyers of these systems having to purchase complete

systems from the same manufacturer. This was problematic since these patented systems were often very expensive, and the buyer now had to rely on the manufacturer for continued support. If, for example, the manufacturer went bankrupt or simply stopped supporting a specific product line, the buyer was out of luck. [14]

To address this problem, European manufacturers started co-operating through the IEC, short for International Electrotechnical Commission. In 1988, the IEC 60870-5 set of standards was introduced, which provided a telecontrol protocol specifically designed for electric power control with SCADA applications. In 1995, the IEC 60870-5-101 (IEC 101) protocol was introduced, which provided this telecontrol over a serial-based connection. In 2000, the IEC 60870-5-104 (IEC 104) protocol was introduced, which uses the application layer of IEC 101, and the TCP/IP protocol suite for networking. [14]

2.6.2 Architecture

The IEC 101 protocol is described by a 3-layer model, the so-called *Enhanced Performance Architecture*, or EPA for short. Comparing it to the 7-layered OSI model, the EPA model is only concerned with the physical (layer 1), data link (layer 2), and application (layer 7) layers. *Figure 6* compares the OSI model and the EPA model. [14]

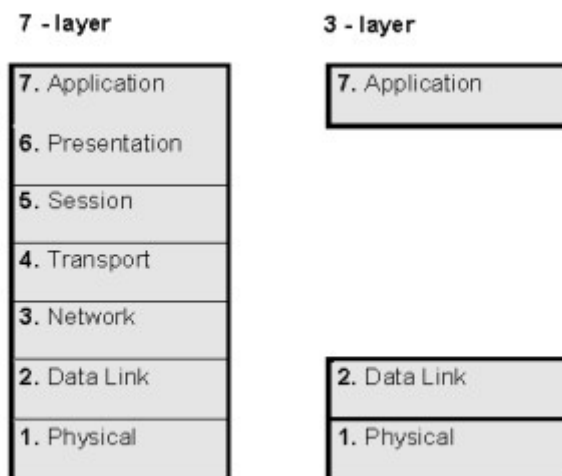


Figure 6. Comparing OSI Model and EPA [14]

2.6.3 Communication modes

There are 2 communication modes available in IEC 101: balanced and unbalanced mode. *Balanced mode* is used when a dedicated point-to-point communication channel is established between the control station (SCADA) and the remote station (RTU). In balanced mode the communication is *full duplex*, meaning that simultaneous transmission and reception of data in both directions is possible. In this mode, the remote station can transmit data without waiting for a request from the control station. [15]

The other communication mode is *unbalanced mode*. This is used when a point-to-multipoint communication channel is set up between control and remote stations. In this mode the communication is *half-duplex*, meaning that data transmission in both directions is allowed, but not simultaneously. In this mode the control station has to send data requests to a specific remote station by referring to its specific *data link layer address*, to be able to get information from it. [15]

2.6.4 Application Service Data Unit

Application Service Data Unit, ASDU for short, is a data structure used for exchanging information between devices in the IEC 101 protocol. ASDUs operate at the application layer (layer 7). ASDUs contain the actual data being transmitted between control and remote stations, such as sensor values and status indications. [15]

When sending ASDUs, there are two possible directions of communication: [15]

- *Control direction*: A message from the control station to the remote station.
- *Monitor direction*: A message from the remote station to the control station.

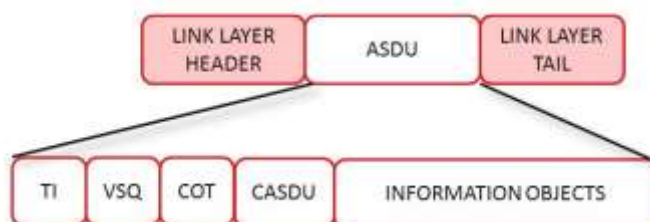


Figure 7 The ASDU format [15]

ASDUs consist of an ASDU header and information objects. The ASDU header contains control and addressing information and the information objects contain the actual data. One ASDU can contain a maximum of 64 information objects. [15]

The ASDU header consists of: [15]

- *TI*: Type Identification, a number that identifies the ASDU, its format, and its content.
- *VSQ*: Variable Structure Qualifier, describes how information objects are organized.
- *COT*: Cause of Transmission, describes the reason for sending the ASDU.
- *CASDU*: Common Address of ASDU, an address used to identify the data in the system. Usually, one RTU has one CASDU.

As seen in *Figure 7*, the ASDU is also encapsulated by a link layer header and a link layer tail. The *link layer header* typically includes fields such as source and destination addresses, length information, and control bits. These details are necessary for the proper routing and identification of the ASDU within the communication network. The *link layer tail* acts as a *delimiter*, it indicates the end of the ASDU, allowing the receiving device to identify the boundaries of the received frame. [15]

The ASDU contains the most critical data for both IEC 101 and IEC 104 systems. This is most likely what adversaries will focus on accessing and/or modifying when trying to attack the system. [16]

2.6.5 Information Objects

Information objects are the individual data points or parameters contained within an ASDU. Some examples of information objects are analog values such as voltage or temperature measurements and binary values indicating the status of switches or alarms. [15]

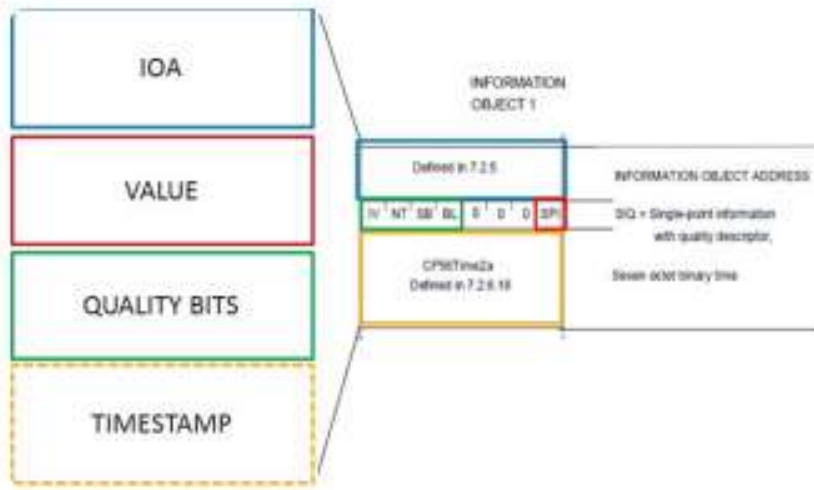


Figure 8 The format of an information object [15]

As seen in *Figure 8*, the information object consists of four different fields: [15]

- *IOA*: Information Object Address, every information object within an ASDU is assigned a unique IOA, allowing other devices to properly reference and interpret the different information objects within the ASDU. Any data point in an IEC 101 system can be identified by combining these two addresses: the common address of ASDU (CASDU) and the information object address (IOA).
- *Value*: The actual value of the object.
- *Quality bits*: Indicates if the value is valid or invalid.
- *Timestamp*: This field is optional. It provides the time when the information object's value was obtained.

2.6.6 Frame formats

In IEC 101, a *frame* is a structured message format that encapsulates the control messages or ASDUs, enabling the exchange of information within the communication link between the control and remote stations. The frames operate at the data link layer (layer 2), and they are usually transmitted over serial communication links, such as RS-232 or RS-485. [15]

The maximum size of a frame is 255 bytes. Depending on the size of the data being sent, one frame can contain multiple ASDUs. [15]

There are two different frame formats defined in IEC 101, the *fixed length* frame, and the *variable length* frame. The fixed length frame is used for control messages while the variable length frame is used to transport ASDUs. [15] The *DATA* field seen in the variable length frame in *Figure 9* consists of the ASDU.

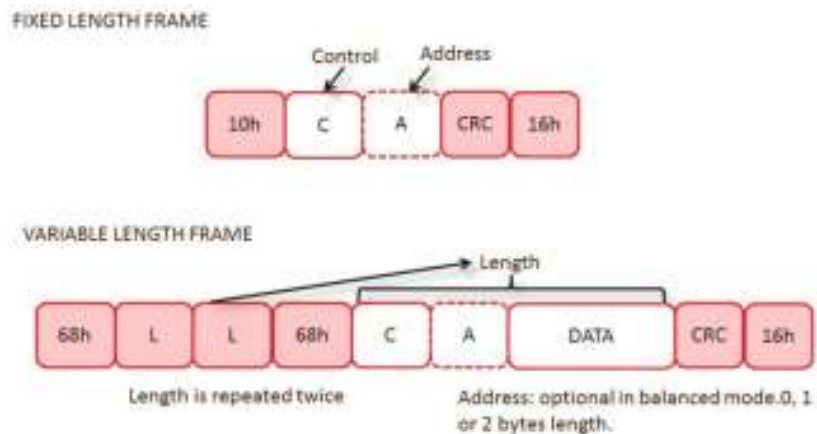


Figure 9 IEC 101 frame format [15]

2.7 IEC 60870-5-104

With knowledge of the fundamentals of IEC 101, IEC 104 can now be examined. IEC 104 is the protocol used for telecontrol in VEO substation projects.

2.7.1 Architecture

IEC 104 operates at 5 layers of the OSI model and only shares parts of the implementation of the application layer with IEC 101. IEC 104 uses the TCP/IP protocol suite at layers 1-4 for network communication. This results in all communication being full duplex, allowing devices to communicate simultaneously in both directions over a common communication media, such as IEEE 802.3 (Ethernet) and IEEE 802.11 (WLAN). [14]

IEC 104 does not use the communication modes defined in the IEC 101 protocol, but its full-duplex communication can be likened to the balanced mode in IEC 101. Table 2 shows

how the IEC 101 and IEC 104 protocols compare to each other and what layers of the OSI model they operate at. [14]

Table 2. Comparison of IEC 101 & IEC 104

#	OSI Layer	IEC 101	IEC 104	Comment
7	Application	x	x	Both use application layer as defined in IEC 101
6	Presentation			
5	Session			
4	Transport		x	IEC 104 uses TCP at the transport layer
3	Network		x	IEC 104 uses IP at the Network layer
2	Data Link	x	x	Dependant upon what physical layer technology is used
1	Physical	x	x	IEC 101: RS-232, RS-485; IEC 104: Ethernet, optical fiber

Since IEC 104 mostly builds upon the application layer implementation of IEC 101 and uses TCP/IP for networking, there aren't many new concepts that need to be explained for IEC 104. Previous sections have explained the workings of both TCP/IP and IEC 101. There is however one important differentiator between IEC 101 and IEC 104, at the application layer, which will be explained in the next subsection.

2.7.2 Application Protocol Data Unit

Application Protocol Data Unit, or APDU for short, is a data structure defined in the IEC 104 protocol. The APDU consists of a header called *Application Protocol Control Information* (APCI) and an ASDU as defined in IEC 101. The APCI header replaces the serial header used in IEC 101, and it operates at the data link layer (layer 2). The APCI header contains information used for proper framing, sequencing, acknowledgment, and synchronization of data communication between the control and remote stations. [15] *Figure 10* shows the structure of an APDU.

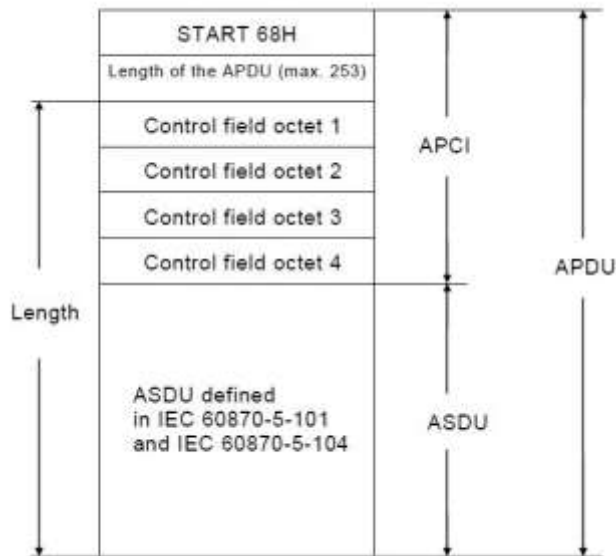


Figure 10 APDU structure in IEC 104 [15]

2.7.3 Security issues with IEC 104

As previously stated, this thesis aims to increase the security of IEC 104 communication between SCADA systems and RTUs. To be able to secure this communication and protect against cyber-attacks, it is important to understand the vulnerabilities present in the IEC 104 protocol.

In the base IEC 104 protocol specification, no real security measures are defined. None of the basic security features such as *access passwords*, *authentication*, and *encryption* are included, which makes it necessary to find other methods of securing the IEC 104 communication. [15] Possible methods for securing this communication will be presented in section 2.9.

2.8 Cyber-attacks against IEC 104-based ICS systems

This section will go through the various phases of a cyber-attack against an IEC 104-based ICS system, such as the ones in use in VEO's substation projects. Specific types of attacks that can be utilized against an IEC 104 system will also be covered.

2.8.1 Detection phase

Most attacks begin with a *detection phase*, which aims to detect and identify network devices and their possible vulnerabilities. There are two methods of detecting IEC 104 devices on a TCP/IP network: active and passive. [16]

Passive detection uses a network interface set to promiscuous mode, which receives and passes on all packets passing through it. These packets can then be monitored using tools such as *Wireshark* or *tcpdump* to identify IEC 104 traffic and devices. This data can then be used in future attacks against the system. [16]

Active detection is where an attacker sends packets to other network devices in the hope of receiving a response from an IEC 104 device, revealing information about it that is useful to the attacker. There are, for example, pre-written scripts that can take a list of IP addresses as input, probe those devices, and return the IEC 104 common addresses of the targets. This type of detection is more likely to be picked up by an IDS or IPS than the passive detection method. [16]

2.8.2 Capture phase

The second phase of the attack, the *capture phase*, aims at capturing data that can later be used to attack targets identified during the detection phase. [16]

One way of capturing data is by gaining access to a *span port*, often referred to as *port mirroring*. Port mirroring replicates and sends a copy of all network traffic to a designated port, where it can be used to monitor and analyze the network traffic. Port mirroring capabilities are most commonly implemented in network switches but can also be found in some routers/firewalls. Port mirroring is commonly used for legitimate purposes, like intrusion detection and prevention on a network. [16]

If, however, an attacker gets access to a switch or router/firewall that has an available span port, they can monitor and capture any traffic on the network. If no span port is available to the attacker, there are methods that exploit vulnerable switches or routers/firewalls, that can give the attacker access to all of the network traffic. One example of this is a *CAM table overflow attack*, which overflows the memory of a switch,

and makes it function like a network hub, resulting in all incoming traffic being forwarded to all ports. [16]

2.8.3 Attack phase

This is the final phase, where the attacker puts the information they have learned about the system into use. Two main attack methods will be discussed, *replay attacks* and *injection attacks*.

2.8.4 Replay attack

In a replay attack, the attacker captures legitimate packets that are transmitted between IEC 104 devices. The attacker can then *replay* the packet at a later time, meaning that the same packet is transmitted again. Unlike an injection attack, which will be discussed in the next sub-section, a replay attack can be performed without acting as a Man-in-the-Middle. [16]

Being fairly easy to execute, replay attacks are often performed by inexperienced attackers or attackers who don't fully grasp how the specific IEC 104 system is working. Not grasping how the IEC 104 system works can be a result of the attacker not having enough domain knowledge, or not having had enough time to capture data and analyze how the specific system works. [16]

Replay attacks are one of the reasons why encryption in itself is not sufficient to secure IEC 104 communication. Even though encryption of the telecontrol data prevents an attacker from reading it, the attacker can still cause problems by replaying the encrypted packet. This is why both encryption and authentication have to be implemented.

Replay attacks can disrupt the control system and even cause physical damage and hazardous situations. If the control system relies on real-time data or commands, it can be disrupted by replaying old transmissions or by replaying the same transmission multiple times. Another risk of replay attacks is replaying commands that, for example, increase the speed of an engine multiple times. If no fail-safes are implemented, this could lead to physical damage and hazardous situations if the engine goes beyond its intended limits. Another safety hazard is if, for example, a safety shutdown system is

instructed to remain inactive during an emergency, which could cause damage to equipment, personnel, and the environment. [16]

2.8.5 Injection attack

In an injection attack, the attacker performs a MitM attack, intercepting the packets between two IEC 104 devices. The attacker then modifies, and re-transmits the packets in real-time to the recipient, without being detected. The MitM attack can be performed in many different ways, such as DNS spoofing and ARP spoofing. [16]

The famous *Stuxnet* attack, which exploited vulnerabilities in SCADA to PLC communications within Iran's nuclear program, was an injection attack. In that attack, control commands issued to the PLCs controlling the centrifuges, which were used to create weapons-grade uranium, were modified, ultimately causing physical damage to the centrifuges. [17]

An injection attack is often more dangerous than a replay attack, as it is being performed in real-time, is harder to detect, and allows the attacker to modify parts of the IEC 104 commands or ASDUs.

Compared to a replay attack, the injection attack requires great knowledge about the specific IEC 104 system one wants to attack, making it very difficult to perform. Because of its difficulty, it will most likely be performed by a very advanced attacker, such as a nation-state or other professional cybercriminals. [16]

2.9 Solutions to increase security

Having discussed the security flaws of the IEC 104 protocol and some common attacks, different solutions can now be considered. Based on the information presented in sections 2.7 and 2.8, it is evident that both encryption and authentication of the IEC 104 communication is necessary. The possible solutions will be presented in this section, with their respective benefits and drawbacks.

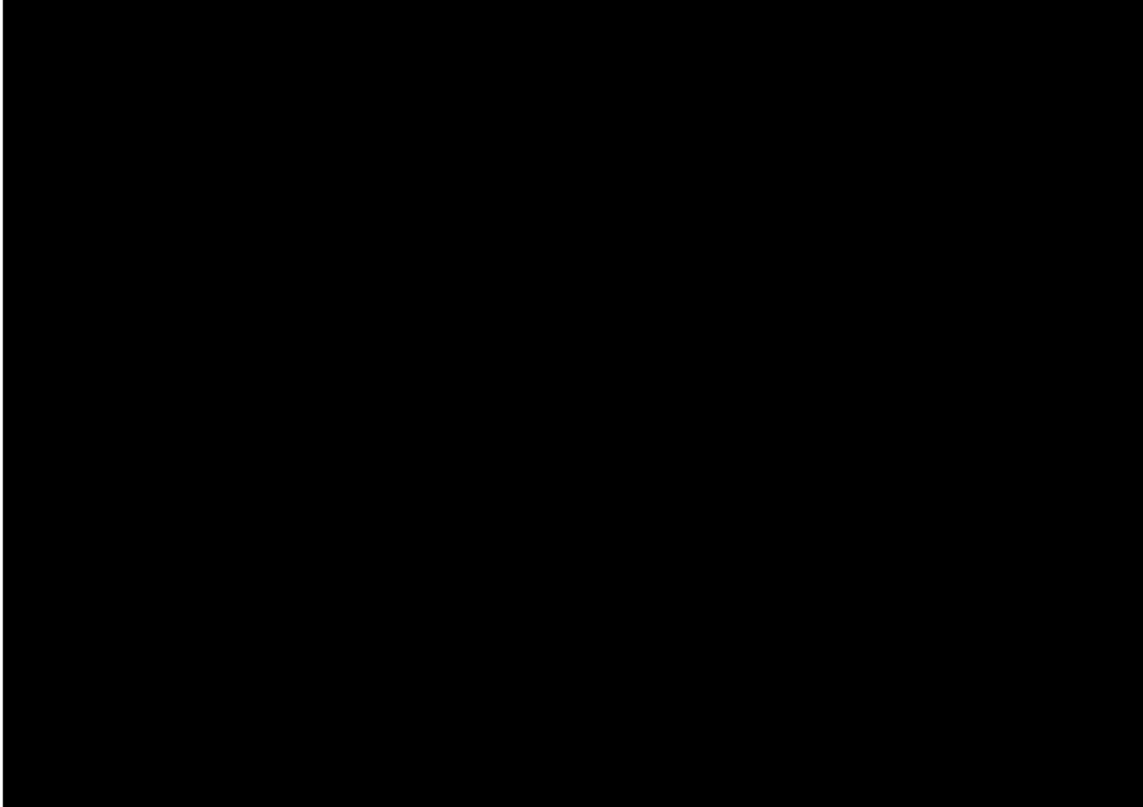
2.9.1 IEC 62351-3 & IEC 62351-5

One solution could be using implementations of either the IEC 62351-3 or IEC 62351-5 standards, which both provide authentication and encryption for IEC 104. There are, however, multiple problems with using this solution. The first problem is that not all RTUs and SCADA systems used in VEO projects implement these standards. The second problem is that these standards only provide guidelines and recommendations for how they should be implemented. This results in manufacturers implementing the standards in different ways, which leads to incompatibility and configuration problems when using products from different manufacturers. Since VEO substation projects often use RTUs and SCADA systems from different manufacturers, this would be very difficult to implement and maintain.

2.9.2 VPN

Another interesting solution is to implement a VPN protocol to secure this communication. Broadly adopted VPN protocols, such as IPsec and OpenVPN, also provide the encryption and authentication that is needed. This solution would likely be much easier to implement and maintain, as both IPsec and OpenVPN are standard protocols that almost every modern system supports.

Table 3 shows the most common RTUs and SCADA systems used in VEO substation projects, and what protocols and standards they support. Seeing that the IPsec VPN protocol is the most well-supported of the options, it is the protocol that will be analyzed and tested in this thesis.

Table 3. Most common RTUs and SCADA systems in VEO's substation projects (hidden for secrecy)

2.10 IPsec

IPsec is a tunneling protocol, commonly used for creating Virtual Private Networks, VPNs. It was designed to provide security features that the IP protocol itself lacks. IPsec encrypts IP packets and works at OSI layer 3, the network layer. Here are some of the main ways IPsec can protect communications: [18]

- *Confidentiality:* As data is *encrypted*, only the sender and receiver will be able to read the messages being sent. As will be seen in chapter 4, sending unencrypted messages over a network can be very dangerous if there is an attacker or compromised device listening on the network.
- *Integrity:* Using cryptography, the integrity of messages can be validated by the sender and receiver. This means that if somehow the message was modified during transit, the receiver would notice that it has been changed.
- *Authentication:* Aside from verifying the integrity of the messages being sent and received, the sender and receiver can also authenticate each other, to verify that they are communicating with the correct peer.

- *Anti-replay*: Like TCP, IPsec also uses sequence numbers, but for different reasons. While TCP sequence numbers ensure reliable data transmission and ordering, IPsec sequence numbers focus on detecting and preventing replay attacks. As explained in sub-section 2.8.4, even if a packet is encrypted, an attacker could try capturing the packet and replaying it later, but in IPsec, this is prevented by the use of sequence numbers.

Before IPsec can be used to protect IP packets between two peers, they first have to build an IPsec tunnel. This is done in two phases, *IKE phase 1 and IKE phase 2*. IKE stands for Internet Key Exchange. These phases will be examined in the coming sub-sections. [18]

2.10.1 IKE phase 1

In the first phase, the two peers will negotiate to find security parameters, such as *authentication, encryption, and hashing* algorithms/methods that are supported by both peers. If the peers cannot find parameters that they both support, the IPsec tunnel cannot be established. [18]

Here is an example of a usual set of algorithms and methods the peers might decide to use: [18]

- Encryption algorithm: AES-128 or AES-256
- Hash algorithm: SHA-1 or SHA-256
- Authentication method: MD5 or HMAC-SHA-1
- Diffie-Hellman group: DH Group 2 (1024-bit) or DH Group 14 (2048-bit)
- IKE version: IKEv1 or IKEv2

During this phase, an *ISAKMP* (Internet Security Association and Key Management Protocol) session is established. This is usually referred to as the ISAKMP tunnel or IKE phase 1 tunnel. This phase 1 tunnel is only used for *management traffic*, it is used as a secure method to establish the phase 2 tunnel over an unsecured network. [18]

2.10.2 IKE phase 2

Having completed the phase 1 tunnel, the phase 2 tunnel can now be built inside the phase 1 tunnel, as can be seen in *Figure 11*. As in phase 1, the peers once again have to negotiate about several parameters that will be used to establish the phase 2 tunnel. The same principle applies here as in phase 1, if the peers can't find parameters that they both support, no phase 2 tunnel can be established. [18]

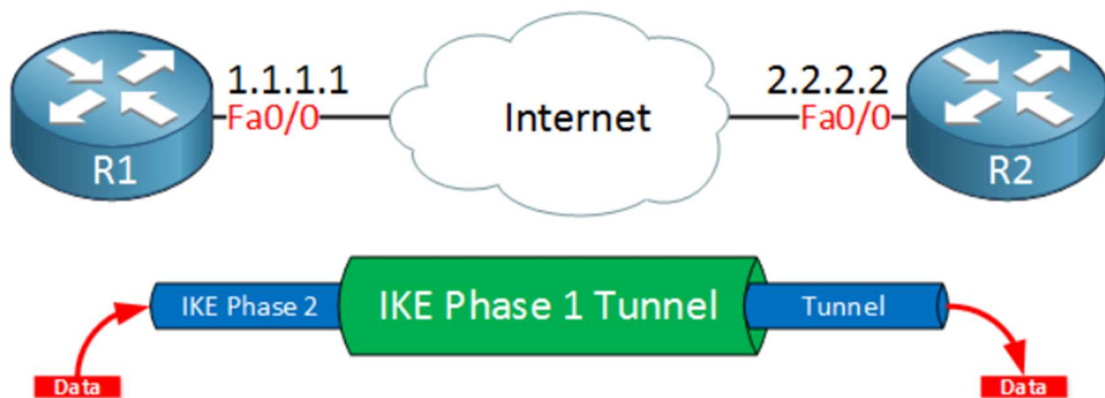


Figure 11 IPsec Phase 1 and 2 tunnels [18]

In this phase, two very important parameters have to be decided on, the *Encapsulation mode* and what *IPsec protocol* to use. These two parameters will be examined in the coming sub-sections.

2.10.3 Encapsulation mode

There are two encapsulation modes to choose between, *Transport mode* and *Tunnel mode*. The main difference between these two modes is that the transport mode simply protects the payload of the original IP packet, while tunnel mode encapsulates the whole IP packet within a new IP packet. The difference between the two modes is illustrated in *Figures 12 and 13*. [18]

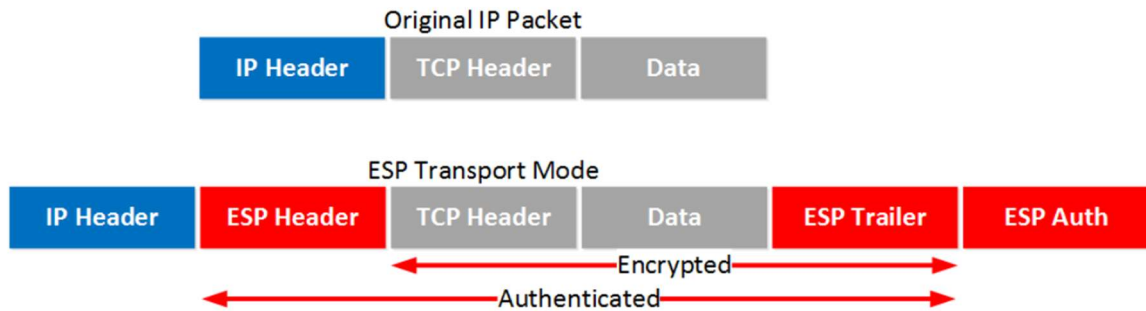


Figure 12 IPsec Transport mode [18]

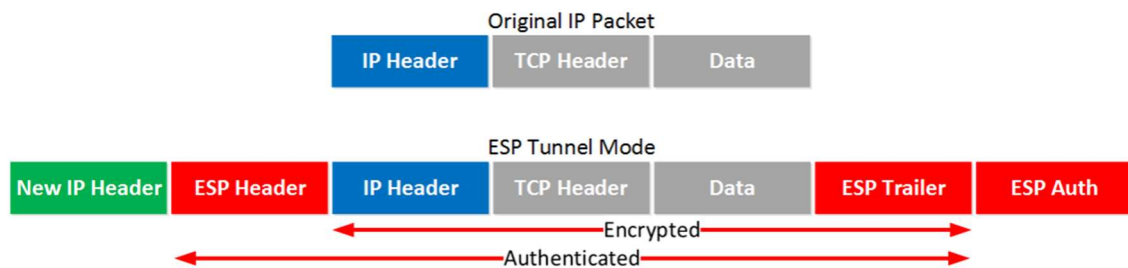


Figure 13 IPsec tunnel mode [18]

2.10.4 IPsec Protocol

This is the parameter that decides how the data being transmitted through the tunnel will be protected. Two protocols can be chosen between, *AH* (Authentication Header) and *ESP* (Encapsulating Security Payload). [18]

The *AH* protocol simply offers authentication and integrity of IP packets, it does not provide encryption. This is done by calculating a hash value over most parts of the IP header, which can then be verified by the receiver, to validate that the packet is authentic and has not been tampered with. [18] *Figure 14* shows an IP packet with an *AH* header attached to provide authentication of the packet.

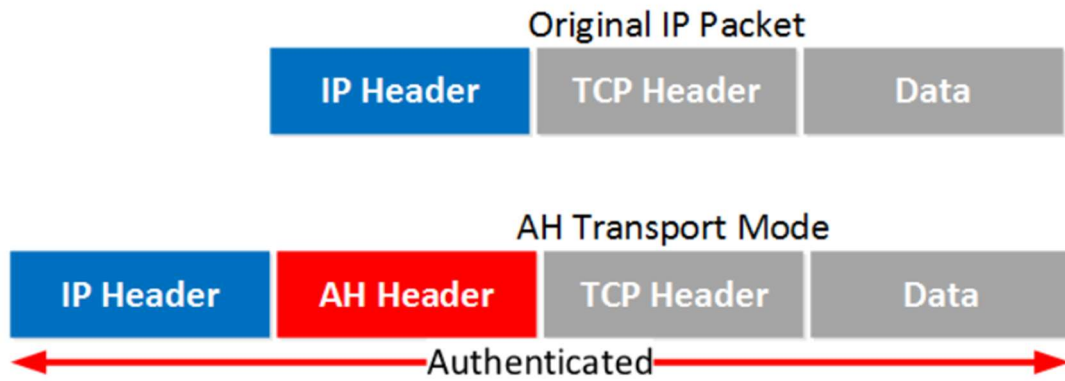


Figure 14 IP packet with AH header [18]

The other protocol, which is the one that will be used in this thesis, is ESP. ESP provides both authentication and encryption, which makes it the more popular choice between the two IPsec protocols. ESP adds a header and trailer around the TCP header and the payload, as can be seen in *Figure 15*. [18]

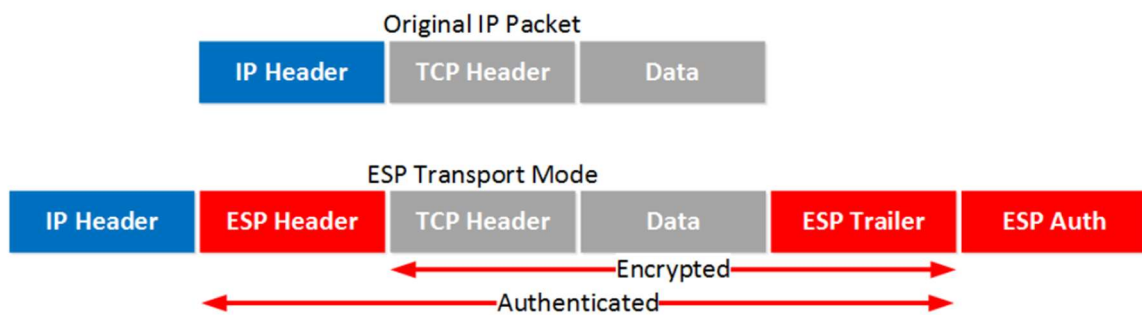


Figure 15 IP packet with ESP header and trailer [18]

3 Test environment

To better understand the threats that were examined in section 2.9, and to be able to test how the presented solution could mitigate those threats, a test environment had to be set up. This chapter explains how the environment was set up and the various systems and software that were utilized for testing.

3.1 Technologies used

These are the technologies that were utilized to perform the testing.

3.1.1 VMware Workstation Pro 16

VMware Workstation Pro 16 is a Type 2 Hypervisor, that allows the user to run multiple virtual machines, VMs for short, on a single computer. It handles the emulation of computer hardware, enabling the installation and operation of a wide range of operating systems. It also provides powerful networking capabilities, which is very helpful when setting up networks in test environments. [19]

VMware Workstation Pro 16 was installed on a Windows 10 Pro computer. All other virtual machines that are mentioned in this thesis were hosted on this instance of VMware Workstation Pro 16.

3.1.2 DemoWinPP104

DemoWinPP104 was used to simulate the RTU, acting as an IEC 104 server. The program simulates IEC 104 traffic and communicates with any compatible IEC 104 client simulator. It logs messages received and sent and it allows manual sending of messages, which is helpful for testing. It also allows the user to modify the default behavior of different messages, allowing the user to, e.g., automatically send a single-point information message every 10th second. [20]

DemoWinPP104 was installed on a Windows 10 Pro virtual machine.

3.1.3 Qtester104

Qtester104 is an open-source IEC 104 client simulator and was used to simulate a SCADA system. It can both send and receive IEC 104 commands, which makes testing easy. It also logs both messages it sends and receives, making it easy to see the IEC 104 traffic in real-time. [21]

Qtester104 was installed on a Windows 10 Pro virtual machine.

3.1.4 pfSense

pfSense is an open-source FreeBSD-based firewall/routing platform, that was used mainly as a VPN server. It offers a feature-rich set of tools and functionalities with a user-friendly web interface.

pfSense was chosen since it requires very low resources, has great documentation, and supports all technologies that were required for this test setup. [22]

3.1.5 Kali Linux

Kali Linux is an open-source Debian-based distribution, that is specifically designed for penetration testing, ethical hacking, and digital forensics. It comes pre-installed with a vast number of tools and utilities specifically tailored for penetration testing and hacking, making it easy to quickly set up and start using. [23]

This virtual machine acted as the attacker during the testing phase.

3.1.6 Wireshark

Wireshark is an open-source network protocol analyzer. It is widely used for network troubleshooting, analysis, and packet capturing. Wireshark lets the user decide which network interface they want to capture traffic on and allows for easy filtering of the traffic. [24]

Wireshark was installed on the Kali Linux machine used to emulate the attacker.

3.1.7 Ettercap

Ettercap is an open-source network security tool that is specifically designed to perform Man-in-the-Middle attacks. It allows the user to intercept, manipulate, log, and analyze network traffic. [25]

Ettercap also supports so-called *filters*, which enhance its functionality and allows for customized network analysis and manipulation. Filters provide a way to selectively capture and manipulate network traffic based on user-specified criteria. Ettercap filters can quite easily be written by anyone who has the slightest experience in any programming language. Ettercap filters that were used during testing will be examined in section 4. [25]

Ettercap was installed on the Kali Linux machine that was used to emulate the attacker.

3.2 1st Test network

This testing network was very simple. It consisted of one VMware *Host-only* virtual network that all virtual machines were connected to. This configuration can be likened to connecting all of these machines to an unmanaged switch. Any message sent to another machine on the network can be seen by all of the other virtual machines. This network has a level of security that matches the usual network that the RTU and SCADA systems communicate via. It is highly insecure since if an attacker manages to get access to this network, there are no limitations to what the attacker can do on the network, as will be shown in the next chapter.

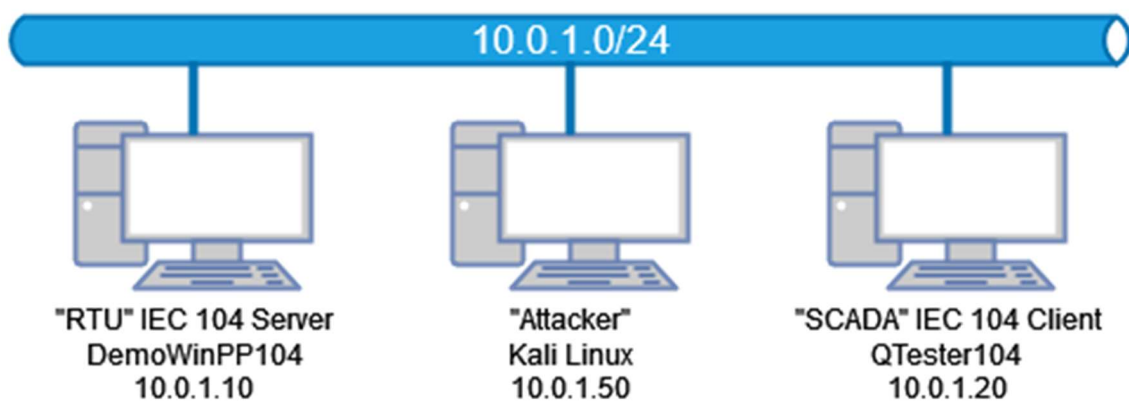


Figure 16 1st Test network and devices

3.3 2nd Test network

Based on the theoretical chapters and the testing of different attacks in chapter 4, the second test network was built to be able to prevent these attacks and properly secure the IEC 104 communication. It is very similar to the 1st test network; the only difference is that now a pfSense-based router has been added to the network.

The pfSense router acts as an IPsec VPN server, to which both the RTU and SCADA simulators have been connected. The IPsec server uses two-factor authentication in the form of requiring both a valid digital certificate and a valid username and password.

The virtual network has a subnet mask of 30, meaning that it can only contain two hosts, the RTU, and the SCADA system. The RTU and SCADA system are then reconfigured to send all of their IEC 104 communication over the VPN tunnel. As will be proven in chapter 5, this simple network change protects against all of the cyber-attacks that have been examined in this thesis.

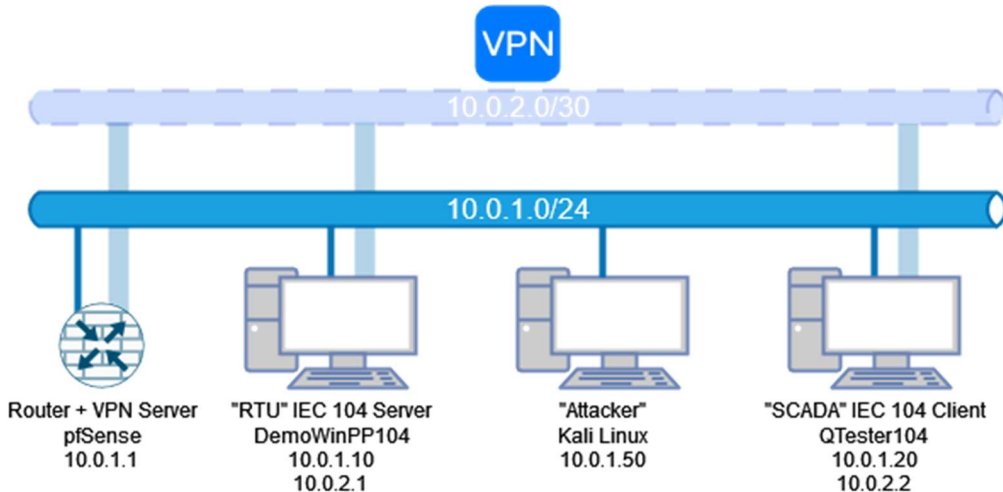


Figure 17 2nd Test network and devices

Installing a router at the substation that acts as an IPsec VPN server would be a highly cost-effective and simple solution to implement. Depending on the customer, they could either connect to the IPsec server directly with the SCADA system, or a site-to-site VPN tunnel could be set up between the substation VPN router and another router on the customer's end.

4 Attacking the test environment

This chapter covers the attempts at performing the various attacks described in section 2.9. The content of this chapter has been hidden as it contains confidential information.

4.1 Identifying IEC 104 traffic

4.2 Becoming Man-in-the-Middle

4.3 Dropping packets

4.4 Replay attack

4.5 Injection attack

5 Testing the IPsec solution

Having examined both theoretically and practically what kind of risks and attacks need to be protected against, the implementation of the IPsec VPN solution can now be tested. Parts of this chapter have been hidden as they contain confidential information.

5.1 Identifying encrypted IEC 104 traffic

5.2 Dropping encrypted IEC 104 packets

5.3 Conclusion of IPsec testing

Having attempted some of the attacks that were successful pre-IPsec now that all IEC 104 communication was going through the IPsec VPN, it can be concluded that the IPsec VPN solution stops all of these attacks.

The final injection attack was not tested, since it is clear that if the MitM and packet-dropping attacks didn't work, neither would the injection attack. The injection attack would be even more difficult to perform, as all of the IEC 104 communication is now encrypted, so the attacker has no idea what parts of the packet to change, or even what packets to target.

6 Discussion

With the ever-increasing threats of cyber-attacks against critical infrastructure, it is now more important than ever to stay ahead of attackers and provide secure communications. The findings of this thesis provide a part of the solution, but it does not provide an extensive solution to all problems. Combining the findings of this thesis with a wide array of other solutions can help provide a more secure way of using the IEC 104 protocol for ICS.

This research has proven both theoretically and practically some of the major threats to the IEC 104 protocol and its communication. Understanding these threats is the first step toward being able to implement a solution.

As the purpose of this thesis was to identify and learn more about the cyber security risks of IEC 104 communication between RTUs and SCADA systems, and to find ways of mitigating these risks, the goal has successfully been achieved. Having taken into consideration the specifics of VEO's substation projects, the solution to these risks is implementing an IPsec VPN server at the substation, that the RTU and SCADA system connects to. This secures all IEC 104 communication against attackers and other insecure or infected systems.

The solution provided is not a one-size-fits-all, using IPsec makes the most sense in VEO's substation projects. For other companies and individuals, it may be more suitable to implement IEC 62351-3 or IEC 62351-5, or some other VPN solution such as OpenVPN. What this thesis does provide is a clear message: IEC 104, and other vulnerable ICS communication protocols, need to be protected by both encryption and authentication. One of the many ways of achieving this is by using a VPN tunnel for this communication, e.g., IPsec.

Future research could build upon the contents of this thesis, e.g., by examining how this solution could be implemented in both VEO's existing and upcoming substation projects. As this thesis was limited to the IPsec VPN protocol, future research could investigate the possible performance gains of using more modern VPN protocols such as OpenVPN or WireGuard.

7 References

- [1] K. Everhart et al., "Power systems in transition - Challenges and opportunities ahead for electricity security," October 2020. [Online]. Available: https://iea.blob.core.windows.net/assets/cd69028a-da78-4b47-b1bf-7520cdb20d70/Power_systems_in_transition.pdf. [Accessed 12 April 2023].
- [2] Harri Sippola, VEO:n tarina, Vaasa: VEO Oy, 2017.
- [3] "Front Page - Annual Report 2021," VEO Oy, 2021. [Online]. Available: <https://ar.veo.fi/2021>. [Accessed 2 March 2023].
- [4] "Company - VEO Oy," [Online]. Available: <https://veo.fi/about-us/company/>. [Accessed 2 March 2023].
- [5] T. Råholm, "Beräkningsverktyg för installationer i elstationer," Yrkeshögskolan Novia, Vasa: Examensarbete för ingenjörsexamen inom elektroteknik, 2016.
- [6] J. Ainasoja, "RTU 560 with IEC 61850 : Vaasa Engineering Oy," Yrkeshögskolan Novia, Vaasa, 2010.
- [7] Motorola, Inc., "SCADA Systems: A comparison of RTUs and PLCs," [Online]. Available: https://www.motorolasolutions.com/content/dam/msi/Products/scada-systems/SCADA_Sys_Wht_Ppr-2a_New.pdf. [Accessed 2 February 2023].
- [8] Inductive Automation, "What is SCADA? Supervisory Control and Data Acquisition," [Online]. Available: <https://inductiveautomation.com/resources/article/what-is-scada>. [Accessed 24 May 2023].
- [9] C. Kozierok, *The TCP/IP Guide - Version 3.0*, San Francisco: No Starch Press, 2005.
- [10] C. Kozierok, in *The TCP/IP Guide - Version 3.0*, San Francisco, No Starch Press, 2005, p. 159.
- [11] C. Kozierok, "The TCP/IP Guide - Version 3.0," San Francisco, No Starch Press, 2005, p. 195.
- [12] "TCP/IP protocols - IBM Documentation," IBM Corporation, 1 March 2023. [Online]. Available: <https://www.ibm.com/docs/en/aix/7.1?topic=protocol-tcpip-protocols>. [Accessed 3 March 2023].
- [13] C. Kozierok, "The TCP/IP Guide - Version 3.0," San Francisco, N Starch Press, 2005, p. 878.
- [14] C. Nyman, "Styrsystem för DEMVE-projekt," Yrkeshögskolan Novia, Vaasa, 2014.

- [15] Ensotest, "Introduction to the IEC 60870-5-104 standard - ENSOTEST," [Online]. Available: <https://www.ensotest.com/iec-60870-5-104/introduction-to-the-iec-60870-5-104-standard/>. [Accessed 7 May 2023].
- [16] P. Maynard, K. Mclaughlin and B. Haberler, "Towards Understanding Man-In-The-Middle Attacks on IEC 60870-5-104 SCADA Networks," September 2014. [Online]. Available: https://www.researchgate.net/publication/301389196_Towards_Understanding_Man-In-The-Middle_Attacks_on_IEC_60870-5-104_SCADA_Networks. [Accessed 21 February 2023].
- [17] M. G. Zampati, "Cybersecurity and Energy - The Case Study of Stuxnet," University of Piraeus, Piraeus, 2022.
- [18] NetworkLessons.com, "IPsec (Internet Protocol Security)," [Online]. Available: <https://networklessons.com/cisco/ccie-routing-switching/ipsec-internet-protocol-security>. [Accessed 24 May 2023].
- [19] "VMware Workstation Pro," [Online]. Available: <https://www.vmware.com/nordics/products/workstation-pro.html>. [Accessed 21 May 2023].
- [20] "IPCOMM, Fink WinPP Protocol Simulator," [Online]. Available: <https://www.ipcomm.de/product/FinkWinPP/en/sheet.html>. [Accessed 21 May 2023].
- [21] "riclolsen/qttester104: Protocol tester for IEC60870-5-104 protocol," [Online]. Available: <https://github.com/riclolsen/qttester104>. [Accessed 21 May 2023].
- [22] "pfSense - Worlds Most Trusted Open Source Firewall," [Online]. Available: <https://www.pfsense.org/>. [Accessed 21 May 2023].
- [23] "Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution," [Online]. Available: <https://www.kali.org/>. [Accessed 21 May 2023].
- [24] "Wireshark - Go Deep," [Online]. Available: <https://www.wireshark.org/>. [Accessed 21 May 2023].
- [25] "Ettercap Home Page," [Online]. Available: <https://www.ettercap-project.org/>. [Accessed 21 May 2023].
- [26] "sudo(8): execute command as another user - Linux man page," [Online]. Available: <https://linux.die.net/man/8/sudo>. [Accessed 23 May 2023].
- [27] "Manua Page - ettercap(8)," [Online]. Available: <https://www.irongeek.com/i.php?page=backtrack-3-man/ettercap>. [Accessed 23 May 2023].
- [28] "etterfilter(8) - Linux man page," [Online]. Available: <https://linux.die.net/man/8/etterfilter>. [Accessed 23 May 2023].
- [29] "ettercap/etterfilter.8.in at master - Ettercap/ettercap - Github," 29 November

-] 2022. [Online]. Available:
<https://github.com/Ettercap/ettercap/blob/master/man/etterfilter.8.in>.
[Accessed 23 May 2023].
- [30 "sed, a stream editor," [Online]. Available:
] <https://www.gnu.org/software/sed/manual/sed.html>. [Accessed 23 May 2023].