CZECH
TECHNICAL
UNIVERSITY
IN PRAGUE

FACULTY OF
ELECTRICAL ENGINEERING

BACHELOR THESIS

2024

FRANTIŠEK
BŮŽEK

Bachelor thesis František Bůžek 2024

Czech Technical University in Prague

Faculty of Electrical Engineering

Department of Telecommunications Engineering

Bachelor thesis

Management and Monitoring of Industrial Operational Technology Networks

Author: František Bůžek

Supervisor: Ing. Ivan Pravda, Ph.D.

Supervisor – specialist: Ing. Jan Strašík

Study program: Electronics and Communications

Prague 2024

BACHELOR'S THESIS ASSIGNMENT

I. Personal and study details

Student's name: **Bůžek František** Personal ID number: **499009**

Faculty / Institute: **Faculty of Electrical Engineering**

Department / Institute: **Department of Telecommunications Engineering**

Study program: **Electronics and Communications**

II. Bachelor's thesis details

Bachelor's thesis title in English:

Management and Monitoring of Industrial Operational Technology Networks

Bachelor's thesis title in Czech:

Management a monitoring průmyslových OT sítí

Guidelines:

Design a solution to provide a centralised way to monitor, diagnose and manage industrial OT (operational technology) networks using available products. Connection of tools to heterogeneous network topology (plant bus, terminal bus, profinet - I/O bus), without affecting their function (interconnection of unrelated networks) and minimization of necessary costs (use of functionalities of existing network elements).
1. Describe the current network topology.and SINEC NMS (network management software).
2. Analyze current network management solutions, network growth plans, and management requirements.
3. Suggest the necessary hardware changes in the network for the possibility of central monitoring.
4. Implement the network management software, set up devices, and prepare the procedure to realize the network growth.

Bibliography / sources:

[1] Pigan, R.; Metter, M.: Automating with PROFINET: industrial communication based on Industrial Ethernet. Publicis, Erlangen, 2006. 355 str. ISBN: 978-38-95782-565.
[2] Firemní dokumentace Siemens na https://support.industry.siemens.com/cs/document/109747975/ [on-line]
[3] Firemní dokumentace Siemens SINEC NMS na https://support.industry.siemens.com/cs/document/109824030/ [on-line]
[4] Firemní dokumentace Siemens SINEC NMS na https://support.industry.siemens.com/cs/document/109762792/ [on-line]

Name and workplace of bachelor's thesis supervisor:

Ing. Ivan Pravda, Ph.D. Department of Telecommunications Engineering FEE

Name and workplace of second bachelor's thesis supervisor or consultant:

Ing. Jan Strašík SIDAT, spol. s r. o.

Date of bachelor's thesis assignment: **18.01.2024** Deadline for bachelor thesis submission: **24.05.2024**

Assignment valid until: **21.09.2025**

Ing. Ivan Pravda, Ph.D. Supervisor's signature	Head of department's signature	prof. Mgr. Petr Páta, Ph.D. Dean's signature

III. Assignment receipt

The student acknowledges that the bachelor's thesis is an individual work. The student must produce his thesis without the assistance of others, with the exception of provided consultations. Within the bachelor's thesis, the author must state the names of consultants and include a list of references.

.	
Date of assignment receipt	Student's signature

Declaration

I declare that I have prepared the submitted thesis independently and listed all the information sources used per the Methodological Instruction on the observance of ethical principles in preparing university final theses.

In Prague ....

Author‘s signature

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

V Praze dne ....

Podpis autora práce

Acknowledgements

I thank my supervisor Ing. Ivan Pravda, Ph.D. for his time and consultations. A big thanks also goes to my supervisor Ing. Jan Strašík for his leadership and support.

Abstract

This thesis aims to analyse actual OT (operational technology) networks, describe their management needs and solutions, and implement SINEC NMS (network management system). Firstly, the equipment of the OT network of the actual plant is analysed in the physical context. Then, the network is analysed in terms of subnets and logic topology. This includes analysing the settings of the switches, firewall settings, and management options and solutions. Along with this analysis, the NMS software was implemented and used for further analysis. As a result, all devices across the network are documented, and this information serves as the root for preparing network growth and changes. The plans were also discussed with the plant management and are ready for realisation.

Keywords: NMS, PCN, OT network, DCS, PCS

Abstrakt

Cílem této práce je analýza reálné sítě OT (provozní technologie), popis potřeby a řešení její správy a implementace SINEC NMS (systém správy sítě). Nejprve je analyzováno fyzické vybavení OT sítě v reálném závodě. Poté je síť analyzována z hlediska podsítí a logické topologie. To zahrnuje analýzu nastavení přepínačů, nastavení brány firewall a zvážení možností a řešení správy. V průběhu této analýzy byl implementován software NMS, který sloužil pro další analýzu. Výsledkem je, že všechna zařízení v síti jsou zdokumentována a tyto informace slouží jako základ pro přípravu růstu a změn sítě. Plány byly rovněž projednány s vedením závodu a jsou připraveny k realizaci.

Klíčová slova: NMS, PCN, OT síť, DCS, PCS

List of abbreviations used

AS	Automation System
CCR	Central Control Room
CLI	Command Line Interface
CPU	Central Processing Unit
DCP	Discovery and Configuration Protocol
DCS	Distributed Control System
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ESXi	Elastic Sky X Integrated
FO	Fibre Optic
FW	Firewall
GUI	Graphical User Interface
GW	Gateway
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I/O	Input/Output
ICMP	Internet Control Message Protocol
iDRAC	Integrated Dell Remote Access Controller
IM	Interface Module
IPv4	Internet Protocol Version 4
IT	Information Technology
LAG	Link Aggregation Group
LC	Little Connector
MAC	Media Access Control (address)
NAS	Network Attached Storage
NIC	Network Interface Controller
NMS	Network Management System
OLM	Optical Link Module
OS	Operating System
OSI	Open System Interconnection
OSS	Operator Server System
OT	Operational Technology
PCN	Process Control Network
PCS	Process Control System

PLC	Programmable Logic Controller
PN	Profinet
RAM	Random Access Memory
RDP	Remote Desktop Protocol
RMM	Remote Management Module
SFP	Small Form-factor Pluggable
SNMP	Simple Network Management Protocol
SSH	Secure Shell
ST	Straight Tip
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
VLAN	Virtual Local Area Network
VM	Virtual Machine

Figures

All figures were created specially for this thesis. The sensitive information is deliberately blurred in the screenshots of the topology map.

Contents

1. Introduction

This thesis is about industrial OT (Operational Network) and its monitoring and management. Industrial automation is expanding, and the demand for network management and monitoring solutions is increasing. Due to Industry 4.0, almost every device in a single plant is connected to one network, or more separate networks are growing inside the plant. Devices are also generating more data, and the requirement for consistent and sometimes uninterruptible connections is increasing. This leads to a robust network.

With growing robust networks and tenths of network devices like switches, routers, etc. The need for some central, easy monitoring and management solution is coming. The network administrator does not want to connect to every single network device by writing its IP address to the web browser and then configuring or seeing the status of the device. Also, when the networks are separated, he has to physically connect his computer to the network. It is time-consuming, and he must know all the IPs and passwords and the network. Or, every time, look into some documentation.

Some solutions exist for network monitoring and management, but it depends on the specific needs of specific use cases. For example, industrial automation operational networks have different needs than some IT networks. Also, some software solutions the specific producer provides can be designed to work better with their own devices and using them with third-party devices is harder.

This thesis is about OT network analysis and applying software solution for the specific case of needs in the specific operational network.

2. Industrial networks

This chapter is an introduction to networks in the industry and their composition and description of several network segments labelled as levels of control.

2.1. Layers of PCS7-controlled plant

Middle and large plants are often controlled with DCS (Distributed control system), which means there is no central computer, and the process is controlled on layers. One of the DCS solutions is SIMATIC PCS7 by SIEMENS AG. PCS7 (process control system) consists of three main layers called together as PCN (process control network) or OT (operational technology) network. Above the OT layers, there is usually a separate IT network for offices and administrative buildings.

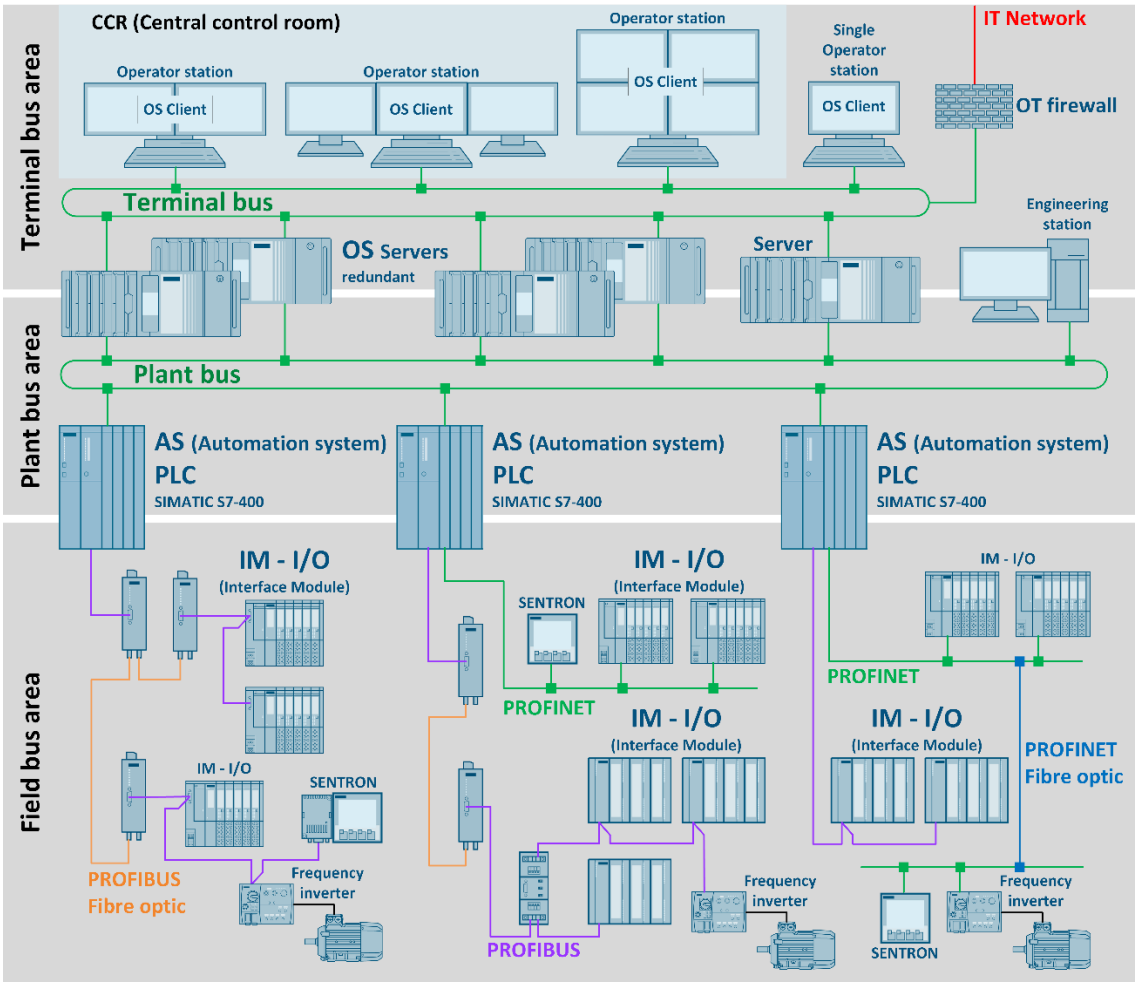

Figure 2-1: Layers of PCS7-controlled plant

As shown in

Figure 2-1 the OT network consists of terminal bus, plant bus, and field bus, where terminal bus and plant bus intertwine and sometimes can merge into one. The OT network is one whole and has its firewall, which also controls the connection to the IT network and makes it safe and secure. Let's describe the layers further.

2.1.1. IT network

As said before, an IT network is at the top and used for offices. This network is connected to the internet through its firewall. If a plant is part of a bigger corporation, this IT network is associated with other plants and locations worldwide and has specific corporate policies. The IT network is often physically separated in plants, which is offered due to different places of administrative and production buildings. Because of corporate policies and internet connection, managing several plants remotely from one location is possible and often used. Connection to the OT network is often set up through both IT and OT firewalls, and it is usually used for data collection for corporate usages, such as statistics and production plans.

2.1.2. Terminal bus area

A terminal bus is the highest layer in the OT network and is composed of workstations, which are here for operators to control the plant. Usually, there is one CCR (central control room) with many monitors connected to several workstations, and operators are here 24 hours a day, seven days a week. Some workstations can also be on smaller technological units where local operators can control their sections. Workstations or, more accurately, clients are visualising the whole plant and containing all control elements. Then, servers at the back are computing data for the clients. These servers are at the border between the terminal bus and plant bus because they have to be connected to both networks.

2.1.3. Plant bus area

A plant bus is a network between servers and PLCs (programmable logic controllers). Servers in PCS7 systems called OSS (operator server system) are connected to clients in the terminal bus and provide computing power. On the other hand, PLCs in PCS7 systems called AS (automation system) process the data from the field bus and provide automatic plant control. Therefore, they also have to be connected to the field bus, so they are at the border between the plant bus and the field bus.

2.1.4. Field bus area

The field bus is the lowest layer of the control and is the area of devices connected to the PLCs (AS). Usually, it consists of separate branches, so it is not a layer in the sense of one network but more like a label for networks at this level. Usually, each PLC has one or more branches connected. They can be determined because of different physical locations of the technology or as technological units or groups of device types across technological units.

A wide variety of devices can be connected to the field bus, but the main ones are often IM (interface modules) and frequency inverters. The frequency inverters are for drives, mainly motors, and the IM connects several other signal modules called IO cards.

Signal modules are there for a variety of I/O (inputs/outputs), for example, digital inputs (DI card) for induction sensors, optical gates, etc., digital outputs (DO card) for relays and operating actuators like simple valves, simple motors, etc., analogue inputs (AI card) for measuring analogue values like pressure, temperature etc., and analogue outputs (AO card) for actuators with sort of control by current or voltage level. Also, there are many modules for specific devices, such as encoders, strain gauges, etc.

2.2. Networking in PCS7-controlled plant

Physical networking in plants depends on several conditions. The main ones are how important or hazardous the actual production is and how much redundancy is required for different layers.

It is common to use optical connections between technological units or buildings, which also depend on the size of the plant area. However, the advantage of optics is significant over longer distances. The usual physical laying of data cables into the same cable channels with power cables, often kilovolts in the case of big industrial machines, makes the electrical distraction significant, and optics are an easy solution.

The redundancy requirements can determine whether the topology is a tree or a combination of several rings. Redundancy can also occur at the level of redundant workstations, servers, PLCs (AS), and IMs, which also determines network redundancy.

As mentioned, the IT network is usually completely separated. It uses its hardware, such as switches and routers, to connect devices like computers and printers across the IT network area. On the other hand, the OT network is more divided due to more layers and types of devices. It is commonly divided into VLANs (virtual local area networks) at the terminal bus and plant bus levels, and there is more than one type of connection in the field bus area.

2.3. PCS7 virtualisation

The modern way to provide multiple servers and clients in the plant is through virtualisation. This is the future, and plants are implementing this solution one after another. The hardware contains minimally two powerful physical servers, which are powerful enough to run all servers and clients on the plant bus and terminal bus. All these original servers and client PCs are VMs (virtual machines), as shown in Figure 2-2.

The physical servers are minimally two as basic redundancy requirements, but more with higher redundancy requirements can exist. Each server has a disk field united into the RAID (redundant array of independent disks) and several NICs (network interface controllers) with more ports. That is for a robust connection to the network. VMs are distributed across physical servers. That maintains the operability of the plant in case of failure. Moreover, the replicas of the running VMs are distributed across as well, so when one server crashes, the replicas on the second server can be instantly turned on, and everything starts running on one server. There can also be a backup server to make and store backups of the VMs, and optionally, NAS (network-attached storage) can be used to back up the backups in second place.

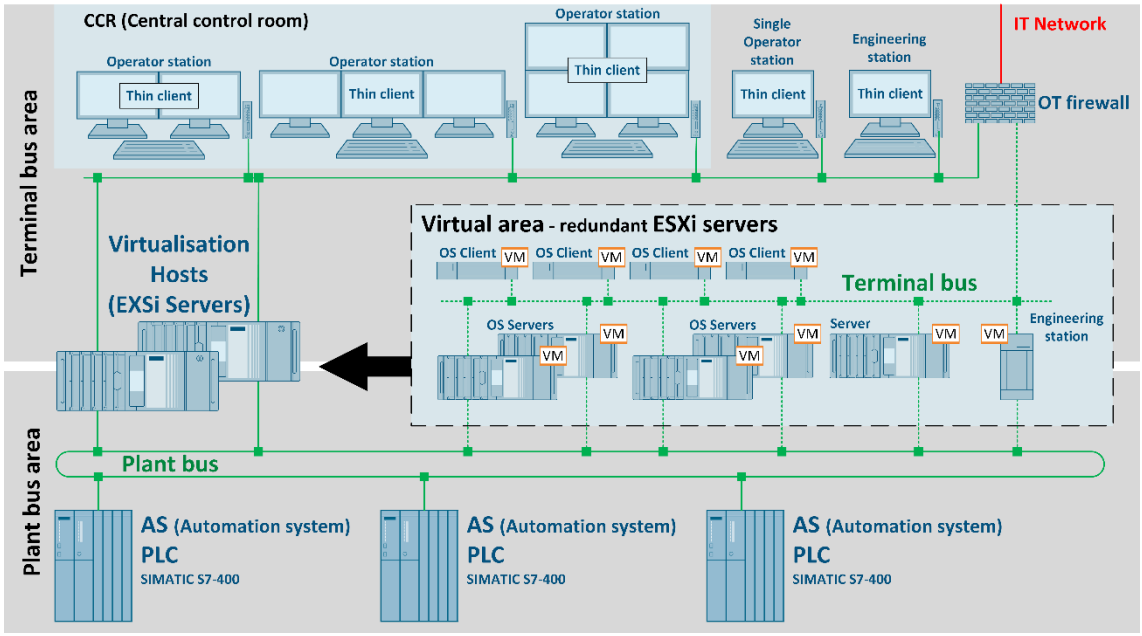

Figure 2-2: Layers of virtualised PCS7-controlled plant

On the CCR and local control rooms, there are only thin clients, which are light and small computers with little computing power. They work like terminals—physical devices with multiple monitors, keyboards, and mousses and they connect to the client workstations on the virtualisation through, for example, RDP (remote desktop protocol). Basically, thin clients run only the OS (operating system) and some solution for a remote connection to the workstation. They commonly use Windows LTSC (long-term servicing channel) and can be set up to run only the remote connection at the operator's account.

This solution moves the network connections between servers and clients mostly into virtual switches into virtualisation and the one physical connection to the second virtualisation server. However, the terminal bus area remains because the new network is raised between physically thin clients and virtual workstations.

2.4. Field bus area network solutions

The field bus, as mentioned, has multiple solutions. The most known in the context of PCS7 are Profibus, Profinet, and Modbus, where Profibus and profinet are the leading solutions, and Modbus is often used just as a connection to a few single devices.

2.4.1. Modbus

Modbus has several versions, but two of them are used in this context: Modbus RTU (remote terminal unit) and Modbus TCP (transmission control protocol), where Modbus RTU works on serial communication, and Modbus TCP works on TCP/IP communication.

2.4.2. Profibus

Profibus has historically been the leading field bus solution. It is a serial communication standard with many variants. The variant mostly used in DCS (distributed control system) is called Profibus DP (decentralised periphery) and is based on the RS-485 (recommended standard 485), which works on the principle of difference between voltages on two wires. The linear topology that is mostly used requires end resistors on both sides of the line, and devices are connected between the two. The line can be single or redundant and can connect up to 125 devices despite the addresses being 0 to 127. That is because addresses 0, 126, and 127 have special usage.[1]

The cable used for Profibus DP is a twisted pair with shielding and is easily recognisable because of its purple colour. One of the disadvantages of the Profibus DP is the length limit, which depends on the required transmission speed, and it is 100 meters up to 1200 meters. This disadvantage has the solution with OLMs (optical link modules), which convert Profibus DP to an optic signal and then back from an optical signal to Profibus DP.[1]

The advantage is that devices connected to one line or, more accurately, field bus branch are connected directly via one cable without using other devices like splitters, switches, or hubs, as shown in Figure 2-3. Only repeaters are used for longer distances, and OLMs are used for distribution via optic cables.

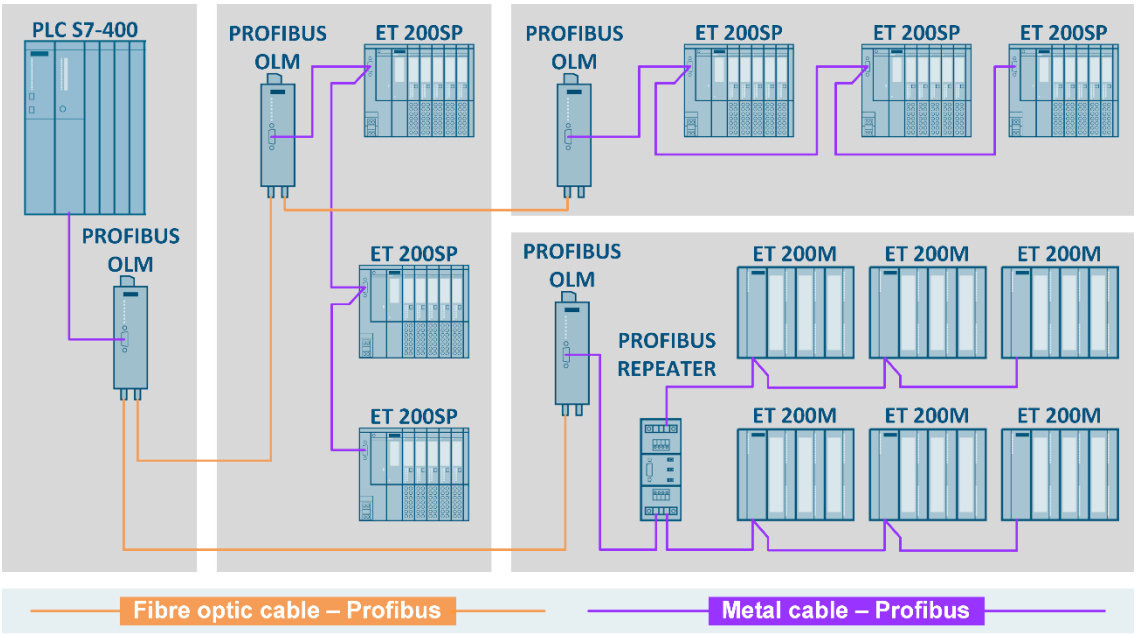

Figure 2-3: Profibus network

2.4.3. Profinet

Profinet is currently the leading field bus solution. It belongs to industrial ethernet solutions, which means it is ethernet-based TCP/IP communication. The main advantage against Profibus is that Profinet is way faster. Through Profibus DP, it is from 9600 bits per second on 1200 meters up to 12 megabits per second on 100 meters. On the other hand, the Profinet can operate at 100 megabits per second and can also operate at 1 gigabit per second. That enables more data transfer, which is a significant benefit for future applications.[2]

For Profinet, a four-wire cable with a speed of 100 megabits per second can be used, or a regular ethernet cat5 or higher can be used for higher speeds. The cable should be green, but in case of usage of any ethernet cables, it is hard to recognise in cabinets. As with classic Ethernet, there is a length limit of 100 meters, which is easily solved by using optic cables. Compared to the use of OLMs, which are not small and still have to have their power supply in the case of profibus, there is a simple solution: use devices with SFP (small form-factor pluggable) ports and then SFP optic modules.

In terms of topology, Profinet has many variants, as it’s the same as any non-industrial network. It is possible to make various types of redundancy, like two connections next to each other or a combination of rings. Compared to Profibus, using addresses from 1 to 127, Profinet has even three types of addresses, which are IP addresses, MAC addresses, and device names, allowing an almost unlimited number of devices in one Profinet topology by addresses. There is a limit on a master, though; for example, 256 devices maximum and data limit per one PLC as a master. Each address serves a different kind of communication, which is included in the Profinet.[3]

Many profinet devices have a two-port built-in switch, so no switches are needed to connect devices to the profinet network. However, the advantage of using additional switches for branching is significant due to better diagnostics and management, which is not available in Profibus, where connecting diagnostic devices directly at the field level is necessary.[3]

Profinet also has more security requirements due to an ethernet base. That is becoming more important when connecting profinet branches to one field bus network. But then, the advantage is the possibility of central remote management monitoring and diagnostics, as it is no longer necessary to be physically at the production with diagnostic devices. This possibility leads to one central NMS (network management system) solution.

3. OT network analysis

This chapter describes the current OT network solution. Since this thesis uses a real OT network in an actual plant as an example, specific information such as IP addresses, MAC addresses, and real names of locations with hardware equipment has to be hidden due to GDPR and security.

Because the plant is controlled by the Siemens PCS7 solution, there are layers of control. There is also one IT network separated from the OT network, with its physical connections and switches from different series than in the OT network to be easily recognisable. Also, its optical connections use single-mode fibres, while the OT network uses multi-mode optical cables. The IT network has its firewall and is connected to corporate networks worldwide. It is remotely controlled and has a strict corporate policy on all devices connected to this network.

3.1. Central server room of OT network

This plant's hardware heart is within seventeen cabinets in one central location. The cabinet setups can be divided into three logical groups, as shown in Figure 3-1. Five "AS" cabinets contain ten PLCs, specifically SIMATIC S7-400 by Siemens. Seven "server" cabinets contain seventeen hardware servers, three NAS data stores, and five Cisco SG550X-24 stackable switches connected into one stack, hereafter called "main stack." Also, the OT firewall ZYXEL USG FLEX 700 is located within these cabinets and connected to the main stack via six cables carrying various VLANs. Finally, five "fibre optics" cabinets spread the network over the plant via fibre optic cables in a tree topology. The server room also has a massive UPS (uninterruptible power supply), which is also connected to the main stack for monitoring.

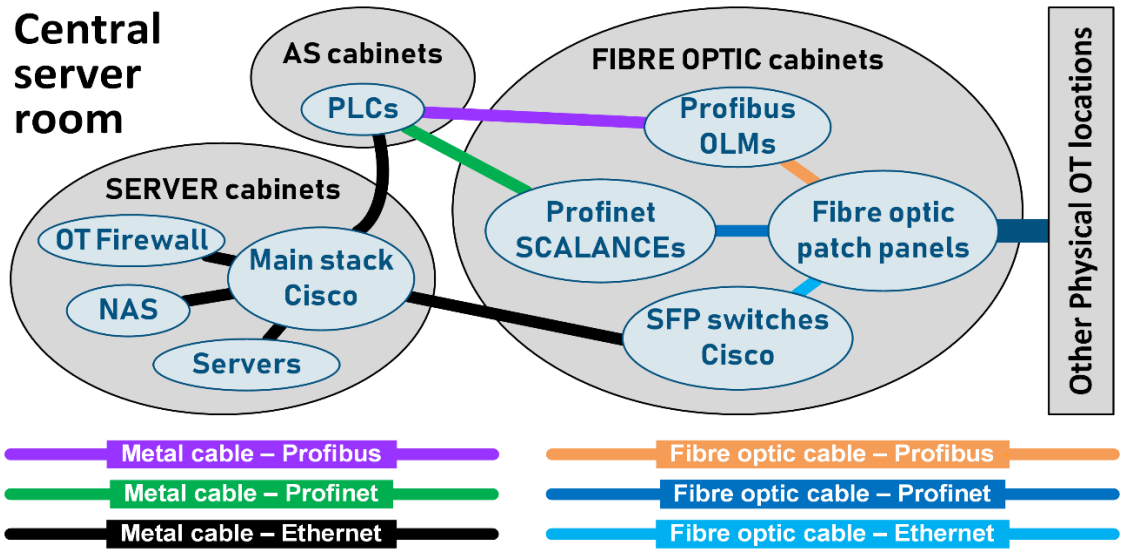

Figure 3-1: Central server room

3.1.1. Stack and LAG (link aggregation) network solutions

A stack is a network solution containing two or more switches connected into the group, which then acts like a single device with a single management and MAC address. The advantage mainly lies in the physical ports increment with little management increment and also in redundancy. When one of the switches crashes, the other switches remain working. That perfectly leads to using LAG (link aggregation), a network solution that enables two or more physical cable connections between devices to act like a single connection. So, connecting the server with two physical cables to two different switches within a stack with LAG not only doubles the data transfer capacity but also brings redundancy to the level where crashing one of the two cables or even crashing one switch does not endanger the connection.

3.1.2. Server cabinets

Most servers in the server cabinets are connected with two cables to two different switches within the main stack, using the LAG setting, which has the advantages mentioned before. Also, the servers have a port for remote management, called RMM (remote management module) in the case of Intel servers and iDRAC (integrated Dell remote access controller) in the case of Dell servers. These ports are also connected to the stack, where one VLAN is dedicated just for these connections.

Server cabinets also include path panels connecting each AS cabinet, fibre optic cabinets, and programmers' service room. These patch panels connect each PLC to the main stack, and the Profinet branches from PLCs are patched through these connections to the fibre-optic cabinets.

3.1.3. Fibre optic cabinets

Two cabinets in the fibre optic cabinets area are dedicated to terminating about thirty fibre optic cables, which spread the network throughout the plant. These cables are terminated inside fibre optic patch panels with ST connectors, where patch cables can be connected to every single fibre.

Another cabinet hosts twenty-five OLMs to convert Profibus branches from Profibus serial to optic signal for spread via fibre optic cables. So, the Profibus serial purple cables are wired directly to these OLMs from PLCs. Each OLM has two pairs of ST connectors so it can spread the Profibus via optics in two different directions. OLMs are then connected to the patch panels via ST-ST patch cords.

The next cabinet contains two Cisco SG300-28SFP switches, which serve to spread the network via fibre optics. The first SFP switch is connected via LAG to the first and second switches of the main stack, and the second SFP switch is connected to the third and fourth switches of the main stack via LAG. Both SFP switches are configured the same, but the first has occupied only the first half of the ports, and the second switch has occupied only the second half. So, when one of them crashes, it is possible to connect all cables connected to his ports to the free ports on the other switch, and it will work. SFP switches are then connected to the patch panels via LC-ST patch cords.

The last of the fibre optic cabinets is used for SCALANCEs, which are Siemens switches. Here, they are used for Profinet branching and conversion to optic signal via SFP modules inside these switches. Connections are the same as those of Cisco SFP switches with LC-ST patch cords. Currently, there are only three branches because most of the plant is still working with the Profibus solution.

3.2. Physical OT locations

Excepting for the aforementioned server room, there are many other OT locations across the whole plant. There is one CCR (central control room), one backup server room, twenty switchgear rooms with Fieldbus peripherals, and twenty-five other locations with some OT equipment.

3.2.1. Backup server room

A backup server room is prepared to replace the main server room in case of an accident. There is a cabinet ready with OLMs, a cabinet with fibre optics with optic cables to most of the plant locations, a cabinet with PLCs, a cabinet with two Cisco SG500-28 stackable switches connected into stack, cabinets with servers, NAS, and, of course, UPS. Currently, there are running only servers with backups of the system, which is running in the main server room.

3.2.2. Switchgear rooms

Across the whole plant, there are around twenty-five locations where the Fieldbus peripherals are settled. The ones with power distribution for production machines are called switchgear rooms, and they include many cabinets with frequency inverters, relays, IM (interface modules) with IO cards, and other stuff for controlling the production machines and feeding them with power.

Almost all these locations have one, let's say, data cabinet with one or more fibre optic patch panels, usually one Cisco switch and one or more OLMs, which are the source of the local

Profibus line (converted back to serial) that connects all peripherals in the switchgear room to Fieldbus. In the recently upgraded locations where the Profinet solution is present, there is SCALANCE with SFP instead of OLM, and the local devices are connected via Profinet.

There are also two high-voltage switchgear rooms. In the first one, on the power supply for the whole plant, three Ruggedcom switches are creating two fibre optic rings for high-voltage protection, which are connected to the particular VLAN in the Cisco switch.

3.2.3. CCR (central control room)

There is one CCR within the plant, where the operators are present 24 hours a day, seven days a week. In this room, approximately thirty monitors are connected to around twenty clients (physical computers) running the software to monitor and control the whole plant's production. This room also has a cabinet with a fibre optic connection to the central server room and Cisco switches to connect the clients to the network.

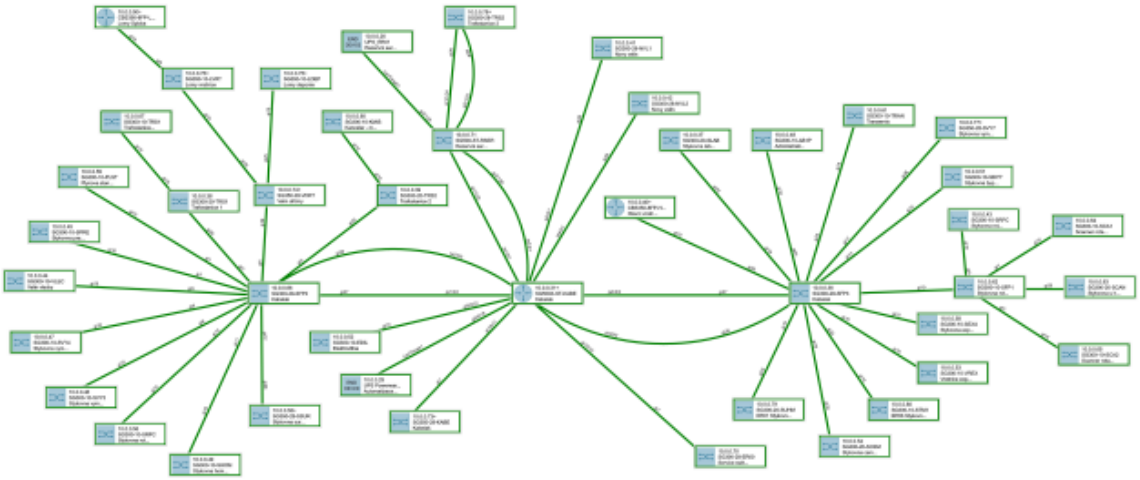

Figure 3-2: Actual OT network topology

3.3. OT network topology

As mentioned, Cisco switches are in almost all OT locations across the plant. The Cisco SG300 and SG350 series are used mainly in switchgear rooms and some other locations. The stackable switches SG550 series are in the main server room, and the SG500 series are in the backup server room. These switches together create a physical network across the plant OT area and connect all devices to the network, as shown in Figure 3-2.

Physically, they are in a tree topology predestined with the fibre optic connections topology, with five stacked switches in the central server room as a central element and the two SFP switches ensuring the branching and spread via fibre optic cables. This physical OT network is divided into twenty VLANs dedicated to several purposes.

3.3.1. VLAN solution

VLANs are spread through the network via trunk connections between switches. On each switch port, there is set access or trunk mode. The port with access mode can be assigned only to one VLAN, and any device connected to this port connects to the network on the assigned VLAN. The port with trunk mode can be assigned to one untagged VLAN and any amount of tagged VLANs. When the device without VLAN knowledge connects to this port, it connects to the untagged VLAN as it was the accessed mode port and doesn't see the tagged VLANs, and if there is no untagged VLAN, this device doesn't connect at all. If the device knows the VLANs and has the same VLAN settings on its port, the tagged VLANs go through the trunk connection to the device, and the device's management is primarily connected to the untagged VLAN. This setting can also be combined with a LAG setting, where several physical connections are set the same as one port in the case of VLANs.

3.3.2. Plant bus VLAN

The plant bus and terminal bus are merged together into one primary and most used VLAN. All PLCs, servers, clients, NAS, UPS, and some printers are connected to this VLAN, as shown in Figure 3-33. This VLAN also connects other field bus devices that need to be connected to PLCs, such as analysers, X-rays, scanners, and SENTRONS, which are power monitoring devices by Siemens AG. That is due to historical development where Profinet was not used in this plant at all, so the field bus devices with TCP/IP connection had to be connected via the Plantbus network. This VLAN is called the plant bus despite the fact it covers more than just the plant bus area. All switch management is also connected to this VLAN, so management IP addresses are from this plant bus IP range.

The IP range in the plant bus VLAN has mask 255.255.252.0, so it consists of 1024 IP addresses, and 1022 can be used for hosts. This network is designed to work without DHCP, so almost all IP addresses are static. Therefore, the IP area is divided into smaller areas where the groups of related devices are. For example, all servers have their IP addresses in their own range. Since this does not affect functionality, someone did this just for clarity.

Although most addresses are static, this network has a DHCP server. It runs within a Windows server OS on a hardware Intel server, and it serves primarily for connecting devices without IP addresses. When a device with a DHCP expectation is connected to the network without a DHCP, it can damage some connections. After all, the device can use an IP address that has already been taken.

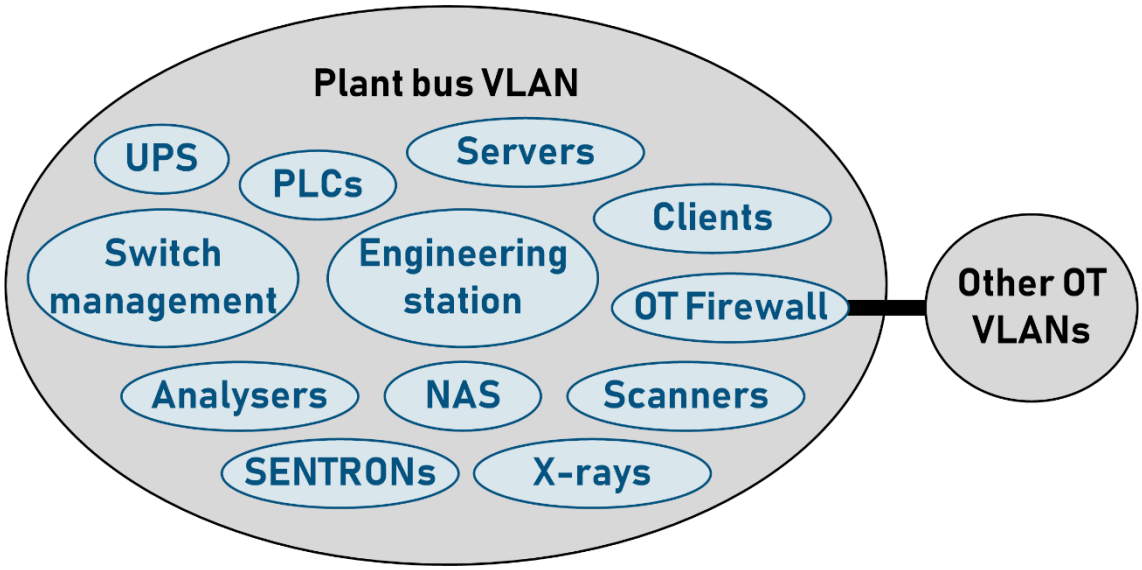

Figure 3-3: Plant bus VLAN

3.3.3. Other VLANs in OT

As mentioned, a VLAN is dedicated to connecting all server remote management connections, including RMM and iDRAC connections.

One VLAN is dedicated only to interconnecting IT and OT firewalls and controlling communication via security policy rules inside the OT firewall.

A specific VLAN is intended for programmer's personal computers, which have almost entirely their network DHCP with some static assignments. This VLAN provides particular access to the Plantbus VLAN, mainly allowing remote connection to servers and clients.

Except for a few cameras connected to the IT network, most of the cameras across the plant are connected to their own VLAN in the OT network because it is the only network with switches physically on all plant locations where cameras are. Besides almost fifty cameras, this network also connects computers, enabling porters and other authorised staff to monitor the areas through cameras. Last but not least, two essential servers record all the camera views and through which the staff's computers look at the cameras.

The remaining VLANs serve other specific purposes, such as monitoring emissions, energy, security systems, and high-voltage protection.

3.4. OT firewall

As mentioned before, an OT firewall is connected to the main stack. Its primary purposes are serving as a gateway for each VLAN, providing DHCP servers within the VLANs, and creating interconnections between them with detailed, specific rules called security policy.

3.4.1. VLAN settings

Due to the connection via more cables to the stack, some of the VLANs are connected as access mode, and then they aren't tagged inside the firewall, so they are treated as physical port networks, and the gateway and DHCP settings are under the port settings. On the other hand, the tagged VLANs flow above the port settings into the VLAN settings, although they physically go via the same physical ports. They are then generally treated as VLANs with their tag numbers and names. Under the VLAN settings, the DHCP servers and gateways for the VLANs are set. Due to these two options, not all VLANs connected to the firewall are in the firewall VLAN list.

DHCP servers are usually set just on the smaller segment of the range, and most of the range works on the static IP base, so it can work without the DHCP, which is common in industrial networks. Also, in some cases, there is a more considerable DHCP range. Still, under the DHCP settings, there are static assignments of IP addresses to specific MAC addresses and labelling the assigned devices with names. For example, in a VLAN for cameras, all cameras are assigned IP addresses and names that way.

3.4.2. Security Policy

The security policy setting is the core setting inside this firewall. It consists of single rules with parameters such as source, destination, IPv4 source, IPv4 destination, service, and action, which is allowed or denied. Rules can be activated, deactivated, or even scheduled so that they can be automatically activated and deactivated.

Source and destination are in the interface context, which means VLANs, physical ports (VLANs connected untagged into ports), and zones. Simplified, zones are groups of VLANs and physical ports that are automatically interconnected. So, a source or destination can be either a VLAN, physical port, or zone.

IPv4 source and destination are in the context of IP address objects. Labelled IP addresses, IP address ranges and labelled groups of labelled IP addresses and IP address ranges are meant by IP address objects.

Services are types of communication which are, in the end, allowed or denied in the connection. Services also belong to objects because they are labelled communication ports, which refer to communication protocols. Service objects can be a single labelled communication port or a labelled group of other services with single or multiple ports.

Each of these source, destination, IPv4 source, IPv4 destination, and service parameters can also be set to the “any” option, which is frequently used.

3.5. Network management solution

Currently, network management is done primarily through web management of the devices reached from allowed areas. LanTopoLog, a network mapping software, is also used to create an overall network image.

Documentation is important because, for example, Profibus OLMs cannot be managed, and staff must know how the branches are connected through the optics and the arrangement of the devices in the Profibus line topology. For this purpose, a huge Excel sheet with information about all devices in the networks and all optic connections exists.

3.5.1. Cisco switches management

LanTopoLog is used to scan the network and find the Cisco switches. Then, detailed information about the configurations of the switches is available in the individual switch management. The managements are reached via the HTTP or HTTPS protocol, where it is necessary to know the IP addresses of the switches to write them in the search box in an internet browser.

Among the firewall security policy rules, it is allowed to reach the IP range where switches are from the programmer’s VLAN but only with HTTP (port 80) or HTTPS (port 443) communication. Since the switch management is located within the Plant bus VLAN, it can also be reached from all devices connected to the Plantbus VLAN.

The web management of the Cisco switches is GUI (graphic user interface), so it is easy to manage the switches without knowledge of the CLI (command line interface) commands. It just requires knowing the IP address, username, and password to access the web management.

3.5.2. Servers management

As mentioned before, the servers are connected to a particular VLAN with a connection to their management port. It is called RMM or iDRAC. The management can then be reached from certain areas since the firewall controls access to this VLAN. The management is accessible in web management through HTTP/HTTPS, where IP addresses, usernames, and passwords are needed.

3.5.3. Firewall management

The Zyxel firewall is also managed via GUI web management, which can also be reached from certain areas but with port 8888. And again, a particular IP address, username, and password are needed.

3.5.4. Profinet management

Because the Profinet branches are at the beginning of their growth, they aren’t managed yet. SCALANCE switches used in the profinet branches work just on basic factory settings as a branching component, and as long as the branches are entirely physically separated, no additional setting is needed. The state of the end devices in the profinet branches can be seen in the PLCs as they are included in the hardware configuration of the PCS7.

4. Plans for future network growth

This chapter is about plans for network growth, which have recently become more actual because the network upgrade is on the table. This year, the whole PCS7 system is being upgraded to a newer version, and with this upgrade comes a hardware upgrade. All servers and client's hardware solutions will be changed until the end of this year.

4.1. Virtualisation

Some virtualisation servers are already running in server cabinets in the main server room and in the backup room, but they are old and not powerful enough. Several servers and clients are already running as VMs on them. The new solution brings new virtualisation powerful enough to run all current hardware servers and client computers into virtualisation, plus current VMs will also be transferred to the new one.

The solution that will be used is made by VMware, Inc., a company developing virtualisation software.

4.1.1. Hardware servers

The hardware used for the upgrade consists of two identical powerful Dell Inc. servers, one general Dell server for backup, and one NAS by QNAP Systems, Inc.

Each of the two powerful servers has enough power to run all servers and client workstations to control the entire plant, which means about 512 GB of RAM, a summary 99 GHz speed of the processors, and SSD disks with a capacity of 7,6 TB. Also, each has two power units and three NIC (network interface controllers) with a total of ten network ports for robust network connection and separate iDRAC (integrated Dell remote access controllers) for remote connection to the hardware server, for example, for access to bios settings. The storage is provided by seven 1,9 TB disks, six of which are connected into the RAID 6 system, and one is set as hot backup, meaning when one disk crashes, it automatically takes over its function.

Simplified, RAID 6 (redundant array of independent disks) means that two-thirds of the total capacity of the disks are available, and one-third is redundancy. Internally, all six disks are divided into segments. The advantages are increased performance and fault tolerance, where one disk can fail, and the system will continue to run without any trouble. Combined with the hot backup disk, two disks can fail one after another, and the system will continue to run without any capacity loss or data loss.

Due to redundancy, there are two servers. One will be in the main server room, and the second will be in the backup server room, including a backup server and NAS. The backup server will make and store backups of the VMs, and the NAS will also store the backups as a second backup storage.

4.1.2. Virtual machines

On the physical servers, ESXi, enterprise software by VMware, will run, providing the environment for the VMs to run. Therefore, the physical servers can be called ESXi servers. Then, on one of the ESXi servers, a VM with a vCenter server will be running, which is a server that controls and manages all ESXi servers and VMs in the virtualisation area.

The VMs will be divided into two halves, and both ESXi servers will host all of them, but only one half will run, and the other half will be managed as VM replicas. For clarity, for example, the first twenty VMs are turned on on the first ESXi server, and at the same time, their replicas are in the second ESXi server but turned off, and the second twenty VMs are on the first server as replicas, and they are turned on the second ESXi server. Again, the advantages are performance increase and fault tolerance. When one physical server fails, the other can quickly turn on the second half of the VMs and then host all VMs until the first server is replaced or repaired.

The VMs division into halves can be predestined with the current usage of two pairs of PCS7 visualisation servers, where one in the pair is always running. The other is ready in backup, and when the changes are played, they are played first to the server that is stopped, it is turned on, and then they are also played to the first server which is stopped. Each server pair, which currently has two physical servers, will have one VM server running on one ESXi server and the second VM server running on the other ESXi server.

4.1.3. Thin clients

The client workstations currently running on physical computers in the CCR will also be virtualised as VMs, so there will be only thin clients with remote access to the VMs in the CCR.

4.2. Network changes

The hardware changes and virtualisation require some changes in the current network. Also, this hardware change is a good chance to modernise the network solution. The shift in the minimally new IP addresses is needed because the old hardware has to partially run together with the new solution, but a network solution upgrade is offered. There were several network upgrade solutions, and the one now prepared was selected due to minimal network hardware change.

4.2.1. New VLAN standard

Now, most of the VLANs in the OT network have their IP address ranges, which have nothing in common, not even the mask, and there is no system in them. That is why the idea of the system came up, which has three rules which are mask 255.255.255.0 on all VLANs, the first two octets of the IP address are the same across all VLANs, and the third octet of the IP address is the same number as the VLAN tag number. For example, if the first two octets of the whole OT network are 164.24. the VLAN 50 will have an IP address range from 164.24.50.0 to 164.24.50.255.

The main change in the network upgrade includes dividing the current Plant bus VLAN into several VLANs, such as the new Plant bus, Terminal bus, Thin clients, Backup, and Admin. These will be created using the standard described above.

The ranges of the new VLANs will be divided into segments according to the type of device. Since this solution is designed to work without massive data flow through a firewall, devices that communicate with devices in other VLANs must have network interfaces with connections in these particular VLANs. The idea is that the last octet of each device's IP address remains the same in both VLANs to which it is connected, which requires the same IP range reservation in both VLANs. For example, servers will be between 70 and 99 on both the terminal bus and the plant bus.

This solution with multiple network connections doesn’t need a powerful firewall because the massive data flow between servers in the plant bus and clients in the terminal bus flows directly through network interfaces to particular VLANs. The more secure option would require a powerful redundant firewall since using a single device in such an important role as core communication between servers and clients is unsafe. However, the redundant firewall would be such an expensive solution that it was rejected.

The new Plantbus, shown in Figure 4-1, VLAN will contain PLCs, servers, and field bus devices, which will later be moved into Profinet branches. The terminal bus VLAN will contain client workstations, servers, and a DHCP range for the possibility of connecting thin clients directly to that VLAN in case of Firewall failure. The thin client VLAN will have only a DHCP range for thin clients. The Admin VLAN will contain the management of the switches, ESXi servers, and vCenter server. Lastly, the new iDRAC VLAN is for remote management of the physical servers with the same last IP octet range as ESXi servers in the Admin VLAN.

Specific solutions will be used for thin clients. As they are in physical locations and operators have physical access to them, their communication to virtual client workstations will flow through the security policy rules in one existing firewall. Since their purpose is to serve as hardware terminals to connect to the VMs, and nothing remotely connects to them, they rely on DHCP. In case of a firewall failure, the thin client VLAN can be via one physical cable connected to the terminal bus VLAN, where the DHCP server is in the main stack, and thin clients can then operate without a firewall.

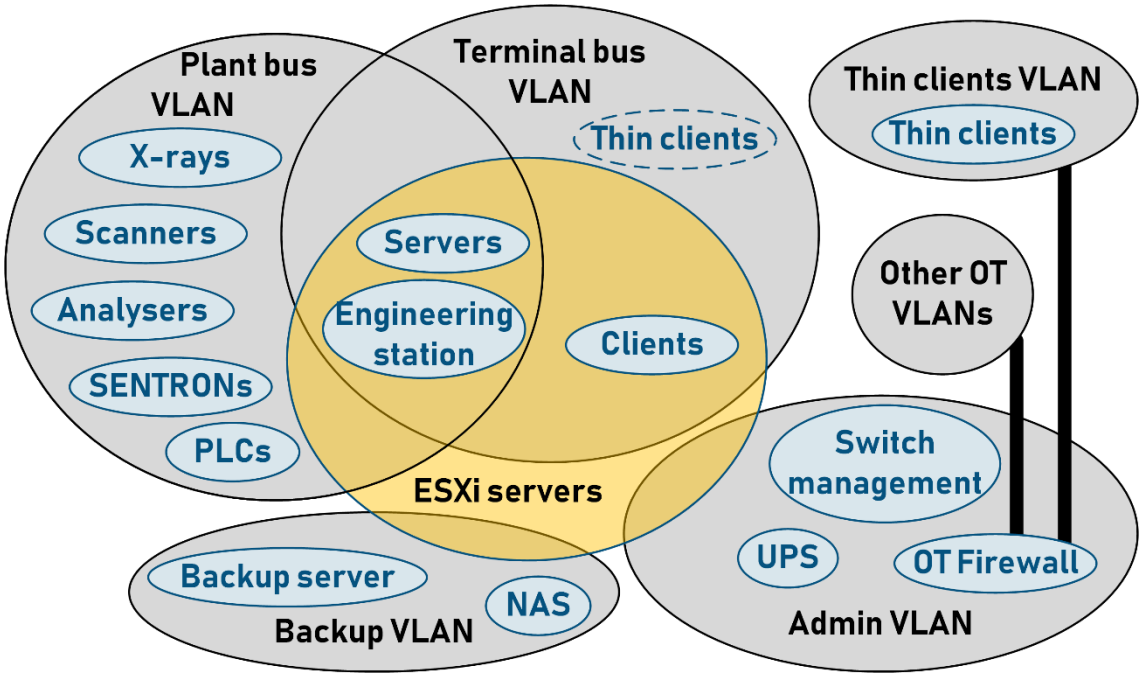

Figure 4-1: New VLANs

4.2.2. Virtual switches

The ESXi servers, among other functions, also have virtual switches, which allow the management of all physical ports of the server and all network interfaces of the VMs.

One option is to use each physical port or group of ports for one VLAN, and inside ESXi, there will be a virtual switch for each VLAN which is needed. The other option that will be used is to use virtual switches with VLAN knowledge and, through the physical ports of the server, create trunk connections to the physical switch, in this case, the main stack or stack in the backup server room. Most communication between servers and clients will be transferred only through a virtual switch, as all clients and servers are VMs in one physical device. Only communication will be to the other half in the backup server room. Still, the connection between the main stack and the stack in the backup server room is through LAG, where the first and second switches in the main stack are with SFP and fibre optic cables connected to the first and second switches in the backup server room stack.

Connecting the virtual switch to the physical switch with more cables with the same settings but without LAG is possible. This option works, but the VMs are automatically and randomly connected through one or another physical connection, so when it is possible, it is better to use LAG. The best way is to connect all ten physical ports on the physical server to the stack in LAG that way, where in the case of the main stack to every switch, there will be two connections to two different NICs on the server and in the case of backup server room all NIC on the server will connect to both stack switches with a total of five connections to each switch. Then, each ESXi will have one virtual switch to connect all VMs to particular VLANs. This solution ensures significant traffic increase and connection failure resistance.

4.2.3. Profinet branches growth

In the case of profinet branches, the slower, gradual replacement of Profibus with profinet is planned due to the requirement of hardware changes in switchgear rooms, and it is better to do it after the significant PCS7 upgrade mentioned. As mentioned, profinet is spread from PLCs only via SCALANCE switches by Siemens AG. Now, there are three separate branches, two of which are for recently constructed switchgear rooms where devices are connected to IMs with profinet connection, and the third is for auxiliary operations and is more divided into several locations. Some devices now connected via Cisco switches will be moved to this branch.

4.2.4. Service bridge

Since the individual profinet branches are physically separated from the rest of the OT network, a device that connects them together for central management is needed. This device is called a service bridge. Basically, it is just a SCALANCE switch specially configured to do this job. It is also designed to work with Siemens' SINEC NMS software.[4]

This solution will also occur among the profinet branching SCALANCEs in the main server room as the Profinet branches grow.

Currently, the SCALANCE switches used in the branches are not configured at all and run just basic configuration. Unless a service bridge is installed yet, there is no safe way to monitor or manage the switches, as connecting computers to the branches is not recommended.

5. NMS software

This chapter describes NMS (network management system) and available NMS software solutions for central monitoring and management, such as SINEC NMS and LanTopoLog.

5.1. NMS Description

NMS (network management system) works mainly on two principles, which are discovering devices on the network and managing them. This is achieved using the ICMP for network discovery and the SNMP for management.

5.1.1. ICMP

ICMP (internet control message protocol) is a communication protocol working on layer three of the OSI (open systems interconnection) model, which is a network layer where packets are transferred. For example, IP (internet protocol) with IP addresses is on this layer.

ICMP has several messages identified as types. The most used types are echo request, which is type 8; echo reply, which is type 0; and destination unreachable, which is type 3.

Ping is a great example of using ICMP, where one device sends an ICMP type 8 echo request message to the other, which sends an ICMP type 0 echo reply message back to the first device.

5.1.2. SNMP

SNMP (simple network management protocol) is a communication protocol that works on the seventh layer of the OSI model, the highest layer, called the application layer. This is where HTTP (hypertext transfer protocol) is, for example. SNMP works on ports 161 and 162.

Communication ports are numbers that dedicate the destination service for the data. They are used by TCP (transmission control protocol) and UDP (user datagram protocol) on layer 4 (transport layer) of the OSI model. The protocols on the higher layers of the OSI model, which are mainly application-layer protocols, have their port numbers. SNMP works primarily with UDP on the transport layer.

A network management station runs NMS software (manager), and the managed devices run agent software. The manager sends the request messages to the agents and receives their response. Agents also asynchronously send SNMP trap messages, which notify the manager. An SNMP trap receiver catches these trap messages. For example, Windows has a built-in SNMP trap service. The trap messages use port 162, while the rest of the SNMP communication uses port 161.

The SNMP protocol has three versions: SNMPv1, SNMPv2, and SNMPv3. SNMPv2 improved the first version overall, and SNMPv3 mainly enhanced the security of the communication.

In SNMPv1 and SNMPv2, the only authentication allowing communication between managers and agents is a password sent as a clear text called a community string. In SNMPv3, there is an SSH (secure shell) protocol for authentication on the transport layer of the OSI model.

5.2. LanTopoLog

LanTopoLog is a simple application that provides physical network topology discovery, visualisation, and monitoring. It has a free or 50 USD licence, which is very cheap. The app is very simple, but it is beneficial.[5]

The primary function is that it scans your network on the range you specify and with the community string in the case of SNMPv1 and SNMPv2 or username and password in the case of SNMPv3. It finds all SNMP devices and creates a topology map out of the data collected via SNMP.[6]

The topology map is then editable and searchable and provides information about devices such as IP addresses, connections to ports, traffic, VLANs, and MAC addresses. Devices such as computers can be seen as connections to the ports with their IP and MAC addresses.[6]

Among the other functions, it can publish the data to the web server, notify when something happens, such as new device detection, traffic threshold reaching, send emails with notifications, monitor devices with ping, export a list of devices with collected information, and export topology. The whole app can even run as a Windows service.[6]

5.3. SINEC NMS

SINEC NMS is network management software developed by Siemens AG. It is specifically designed for industrial networks, mainly those based on Siemens SIMATIC NET technology, which means that it is designed to work with Siemens industrial solutions.[7; 8]

SINEC NMS solution licences have different variants with different use cases, depending on the number of devices and the scope of the network monitoring and configuration. The licence then determines the price, which relies on the scope of the network. It often means thousands of USD. The licences are then stored and managed in the automation licence manager app by Siemens AG.[7; 8]

5.3.1. Components

The SINEC NMS (network management system) consists of two components: one Control component and several Operation components, as shown in Figure 5-1. The Control administers the whole network, while the Operation administers individual subnets. The Control is there for the central administration of the Operations.[7; 9; 8]

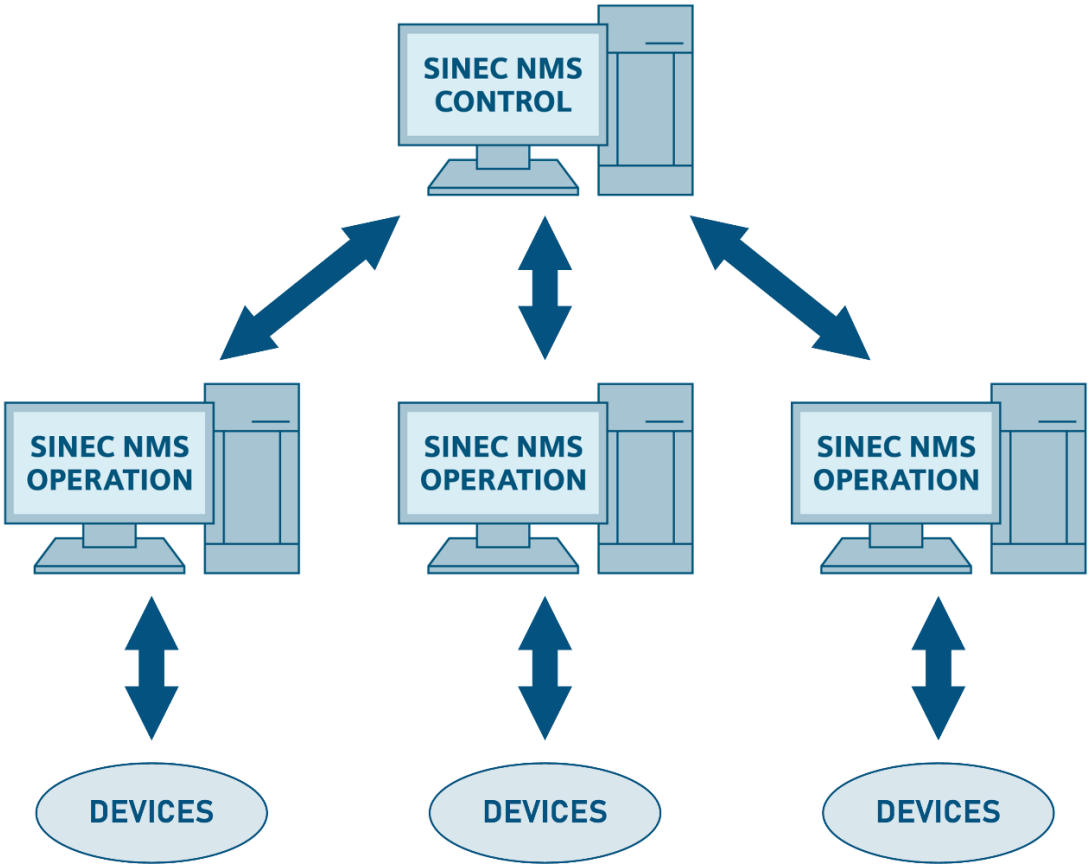

Figure 5-1: Components of SINEC NMS

Operation and Control can be individually installed on their stations, which means Control and each Operation has its PC or VM. That is a multi-node installation. On the other hand, a single-node installation means that both Control and Operation are installed on a single PC or VM. In this case, there is only one Operation in the system. [9]

5.3.2. User Management

The SINEC NMS has role management, where different user roles with different access authorisations are created. Role management can define a role hierarchy, which is stored in Control.[9]

5.3.3. Network discovery

The network discovery IP ranges are defined in Operations by Control, which manages the ranges inside Operations. One operation can store several different IP ranges. The network is discovered via ICMP and SNMP. SINEC NMS also possesses DCP discovery, which can search DCP discoverable devices in or outside the IP range for discovery.[9]

5.3.4. DCP

DCP (discovery and basic configuration protocol) is a communication protocol that works at the link layer, the second layer of the OSI model, where, for example, MAC (medium access control) with MAC addresses takes place.

DCP is used in profinet networks to configure Profinet device names and IP addresses of the devices, which are important parameters in the case of Profinet networks.

5.3.5. Network monitoring

In Control, a list of all monitored devices across all operations with their properties can be displayed. In operations, the devices are monitored in detail. They are divided into groups by different properties. For example, by device category, they are divided into groups such as PC/HMI, PLC-CP, Router, Switch, and others. By vendors, such as Siemens AG, Cisco, Eaton, etc., and by subnet. Then, they can also be divided by status.

The network monitoring tab in Operation contains four basement parts: a topology map, device list, interface list, and MAC monitor. The topology map view visualises devices in their topology with information about their interconnections. The device list includes detailed information about devices, and the interface list contains information about each device interface. MAC monitor list is similar to an interface list but also contains MAC addresses detected at the interfaces.

Of course, all the lists and maps are exportable. For example, lists can be converted into a .csv file and topologies into a .png image.

5.3.6. Network management

The SINEC NMS also has the possibility to configure devices via SNMP protocol. In the case of Siemens hardware, the options are even wider. It can also monitor the firmware of the Siemens devices and notify the available updates.

6. NMS software implementation

This chapter is about implementing SINEC NMS software on the OT network. SINEC NMS was chosen because of the advantages of Profinet management.

6.1. Management needs

The primary purpose of the management is to map the whole network of devices and their connections and create an environment for an easy way to find each device and its parameters such as IP address, MAC address, and connection to another device in the network, such as switch port and VLAN. The easy way to configure switches just by clicking on them on the map is also a benefit of central management, which is enabled by redirecting to web management of the switches.

6.1.1. Profinet management

The important part of network management is Profinet monitoring and management. This is a specific discipline because Profinet branches are physically separated and may even have the same IP address ranges. Also, there is the demand for profinet name monitoring and assignment, which makes adding devices into the profinet network a lot easier and in case of profinet growth, it will be used a lot.

6.2. Hardware changes

For interconnection of the unrelated profinet branches, there is a hardware solution called service bridge, which was partially described in a paragraph under plans for future network growth, so it is planned but not yet implemented.

The installation will be in place after Plantbus changes due to the new VLAN division. Also, a new virtualisation system will be used to place SINEC NMS into its VM. Then, the Service bridge is recommended to connect to the Plantbus through the firewall.

6.3. Firewall setup

The firewall needs to allow communication from the physical device or VM where SINEC NMS is installed to the required networks and back from them to SINEC NMS. Currently, it is installed inside a VM within the programmer's PC.

As there is no service bridge yet, the SINEC NMS needs to have access just to the Plantbus VLAN. This is done via a security policy rule. The rule allows communication from the particular

IP address in the programmers' VLAN into the Plantbus VLAN to any IP address. Inside the DHCP server of the programmers' VLAN, the static assignment of the specific VLAN is made to the MAC address of the network adapter of the virtual machine with the SINEC NMS.

The rule then allows communication specified in the “NMS_ALLOW” service group, which was created for this purpose. The service group consists of several services. The “NMS_ALLOW” group has members ICMP type 0, ICMP type 8, SNMP_TCP port 161, SNMP_UDP port 161, SNMP-TRAPS_TCP port 162, and SNMP-TRAPS_UDP port 162.

Other communication services, such as HTTP and HTTPS, are already allowed from the programmer’s VLAN to Plantbus VLAN.

6.4. SINEC NMS implementation

The SINEC NMS is installed within the VM on the programmer's PC. The installation is single-node, meaning Control and Operation are both inside that VM.

6.4.1. Setting up Operation

After installation, the Operation have to be settled within the Control. It can be done within system administration, where a list of operations takes place. The IP address of the host of the Operation is needed, which is, in this case, the VM where SINEC NMS is as one unit. Then, after the name and other parameters, there are individual scan ranges, which are defined by name and first and last IP addresses. Then, the created Operation has to be synchronised and initialised, which is done automatically because of single-node installation.

After Operation initialisation, the network scan process can be launched. It scans the IP addresses in the IP range one after another and lists the reachable ones in the device list.

Then, for the SNMP information collection, the operation's parameter profile has to be appropriately set in the Control. The SNMP port 161, version 2 and community string, because version 2 is used. As these settings are done, the Operation automatically gathers information about the devices via SNMP.

6.4.2. Topology map

The network's visualisation in the topology map is beneficial. The topology in Figure 3-2 in the chapter about the topology of the OT network comes just from SINEC NMS. The topology is automatically generated, but the one in the picture was manually adjusted to be more apparent. Three pieces of information about the devices can be displayed on the map.

Currently, there are IP addresses, device names, and locations. On the connections between devices, there is information about ports where the connections are physically connected.

The map has a function to filter connections by VLAN, so it can show only connections and devices where the particular VLAN goes. For example, in Figure 6-1, the blue lines highlight the filtered VLAN.

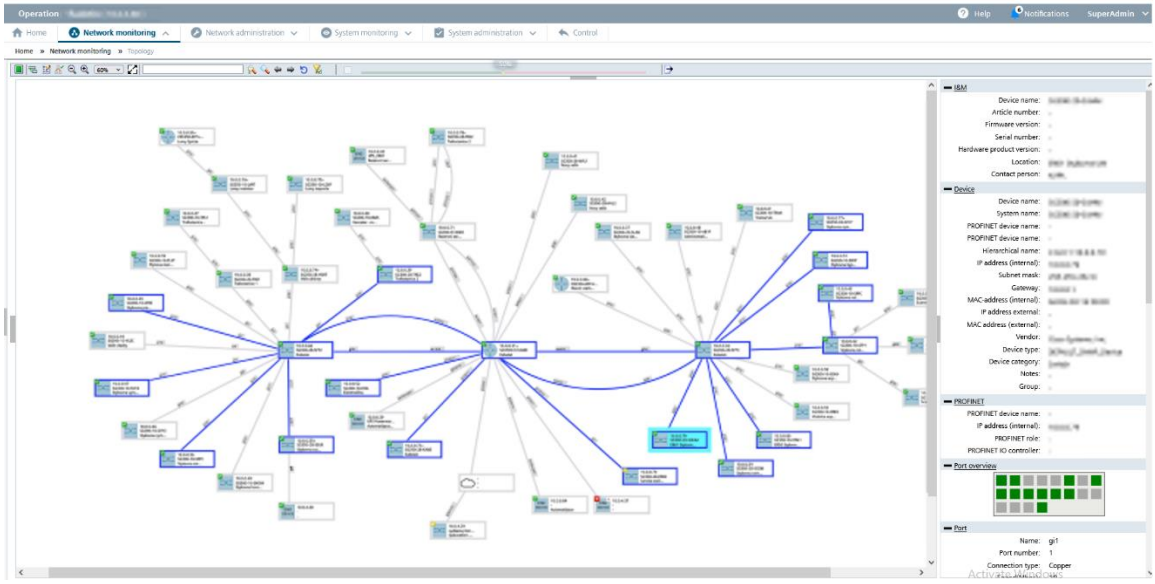

Figure 6-1: SINEC NMS topology map

The device properties can be seen on the right side by clicking on the device on the map. It includes the device name, IP address, MAC address, location, vendor, device type, etc. The port occupancy is visualised by grey and green squares, where the green ones are occupied and currently up, and the grey ones are down. Also, detailed information about the interfaces is shown below when clicking on these squares. There are properties such as port alias name, connected MAC address, port mode, connection type, speed, status, link aggregation name, transmitting and receiving utilisation, and even trunked VLANs or information about redundancy in case of rings.

Also, pointing the mouse on the device can reveal a lot of information about it, and double-clicking opens a popup with tabs containing even more information about the device and a link to the web management configuration. In the case of Cisco switches, this redirects the browser to the configuration page.

6.4.3. Device, Interface and MAC lists

The device list stores the same device properties as can be found through the network map. Each device has one row, and the columns with different properties can be adjusted. More detailed is the interface list, where every interface of all devices has a row with details. Like that is the MAC monitor, where interfaces are also listed, but there is an option to show a column with information about MAC addresses discovered on ports. For example, the device list contains one hundred devices, but both the interface and MAC lists have around nine hundred and twenty rows.

The disadvantage of MAC monitoring is that there can be shown maximally four MAC addresses in the cell and six when pointing with the mouse on that cell, but when there are more, they cannot be displayed. In the case of trunk ports, it is acceptable because hundreds of MAC addresses are discovered. However, when devices are connected via a wireless link, the wireless transmitter and receiver also have their MAC addresses. When they are connected through one port to the manageable switch, all MAC addresses can be seen just in the web management of the particular switch.

These lists' columns can be easily adjusted to show or hide different properties. They can also be ordered and filtered by any column. All the lists can be easily exported to .csv files and transferred to Excel.

6.5. Practical use cases

Many practical use cases proved the advantages of the SINEC NMS solution. As the OT network was mapped and revised, a solution was needed to search devices from documentation in physical locations and physically search their connections to the switches.

For example, searching for physical servers and their connections to the main stack was done via MAC tale or searching cameras, where their view was on display. Still, nobody knew where the camera was connected to the network. Also, searching for the non-working cameras and their connections and physical locations was more challenging, as some were connected wirelessly via additional modules.

6.6. Preparing for Growth

As the new virtualisation is realised with significant OT network changes, the SINEC NMS will probably occur within the virtualisation and then be ready to connect to the service bridge and manage the profinet branches.

7. Conclusion

This bachelor thesis aimed to analyse the OT network, describe the SINEC NMS solution, implement it on the network with its knowledge, and prepare for future changes and growth.

The analysis was an actual network revision project because, for certain reasons, the network was not properly documented, and there was no accurate and complete documentation. The network was analysed entirely from every single optical fibre across metallic connections to all devices' IP addresses, MAC addresses, and other detailed information. The old documentation was updated and expanded.

The NMS solution was described and then implemented in the actual use case, proving that it is helpful in network revision. The implementation was similar to the network analysis on the alive network, with a partial production shutdown due to planned repairs. Despite partially stopping production, the rest of the network was necessary to run without shutdown, so it was a highly responsible job. Therefore, high knowledge of performed changes and possible risks had to be considered, and all steps were double-checked before applying.

The future plans described in the thesis were discussed with competent plant management and are based on the executed network revision and analysis results.

Bibliography

[1] PROFIBUS NUTZERORGANISATION E.V. PROFIBUS. PROFIBUS NUTZERORGANISATION E.V. *PROFIBUS.com* [online]. 2024 [cit. 2024-05-18]. Dostupné z: https://www.profibus.com/technologies/profibus

[2] PROFIBUS NUTZERORGANISATION E.V. PROFINET Technology Description. PROFIBUS NUTZERORGANISATION E.V. *PROFINET.com* [online]. 2024 [cit. 2024-05-18]. Dostupné z: https://www.profinet.com/profinet-explained/technology-description

[3] PIGAN, Raimond a Mark METTER. *Automating with PROFINET : industrial communication based on Industrial Ethernet*. Erlangen: Publicis, 2006. ISBN 978-38-95782-565.

[4] SIEMENS AG. Service Bridge – Setup and Configuration. SIEMENS AG. *SiePortal* [online]. 2020, 2020-07-15 [cit. 2024-05-18]. Dostupné z: https://support.industry.siemens.com/cs/document/109747975/

[5] YURIY VOLOKITIN. LanTopoLog - Manual. YURIY VOLOKITIN. *LanTopoLog - Map Your Network* [online]. 2007 [cit. 2024-05-18]. Dostupné z: https://www.lantopolog.com/files/help_en.pdf

[6] YURIY VOLOKITIN. *LanTopoLog - Map Your Network* [online]. 2007 [cit. 2024-05-18]. Dostupné z: https://www.lantopolog.com/

[7] SIEMENS AG. Download and sales and delivery release for the product SINEC NMS V2.0. SIEMENS AG. *SiePortal* [online]. 2023, 2023-09-07 [cit. 2024-05-18]. Dostupné z: https://support.industry.siemens.com/cs/document/109824030/

[8] SIEMENS AG. Getting Started: Understanding and Using SINEC NMS. SIEMENS AG. *SiePortal* [online]. 2022, 2022-01-24 [cit. 2024-05-18]. Dostupné z: https://support.industry.siemens.com/cs/document/109762792/

[9] SIEMENS AG. SIMATIC NET Network management SINEC NMS. SIEMENS AG. *SiePortal* [online]. 2024, 2024-03-12 [cit. 2024-05-18]. Dostupné z: https://support.industry.siemens.com/cs/mdm/109824255?c=171084625931&lc=en-CN