

Šarūnas Paulius

# THE DATA TRANSMISSION NETWORK PROJECT OF THE PRODUCTION PROCESS CONTROL SYSTEM

Bachelor's thesis

Bachelor of Engineering

Degree Programme in Information Technology

2024



South-Eastern Finland  
University of Applied Sciences

Degree title	Bachelor of Engineering
Author(s)	Šarūnas Paulius
Thesis title	The data transmission network project of the production process control system
Commissioned by	
Year	2024
Pages	41 pages, 3 pages of appendices
Supervisor(s)	Matti Juutilainen

## ABSTRACT

This project presents a data transmission network design for a production process control system. Currently, Ethernet-type networks hold the top place when it comes to building production line networks. However, this work suggests an alternative new way to control production lines using a type of technology called gigabit-passive optical network, or G-PON. An analytical comparison between the two network types is conducted, with calculated examples demonstrating the superior efficiency and advanced cybersecurity of G-PON technology. The project involves careful selection and configuration of network equipment to ensure optimal performance. A key focus is on cybersecurity, identifying potential vulnerabilities in the designed network and proposing measures to address them. The design phase of the project includes an overview of the optical trunk blueprint and calculations of passive optical elements parameters. In the experimental section, optical network equipment and devices were selected, and a minimalistic optical trunk prototype was deployed. The thesis concludes with the project outcomes and potential benefits of using a G-PON system for controlling production lines.

**Keywords:** G-PON, optical line terminal, optical network unit, signal attenuation, networking.

# CONTENTS

1	INTRODUCTION .....	5
2	G-PON VS ETHERNET: A PRODUCTION PROCESS ANALYSIS.....	7
2.1	Types of data transmitted during the production process .....	7
2.2	Relevance of G-PON technology.....	7
2.3	G-PON energy efficiency requirements .....	12
2.4	Comparative analysis of data flow management methods.....	14
3	SPECIFICATION AND DESIGN OF THE OPTICAL NETWORK .....	15
3.1	Object to be designed.....	15
3.2	Hardware parts .....	15
3.3	Network project specification .....	16
3.4	Production line optical network plan .....	16
3.5	Calculation of optical network parameters .....	18
3.6	Cybersecurity assessment of G-PON technology.....	21
3.7	Comparison of 1+1 and 1:1 reservation schemes .....	22
3.8	VPN establishment in G-PON network .....	24
3.9	Application of network security enhancing measures .....	24
3.10	Vulnerability assessment of G-PON for production management.....	26
4	EXPERIMENTS WITH G-PON .....	29
4.1	Implementation of the optical trunk.....	29
4.2	Production line "Packet Tracer" G-PON model.....	34
5	CONCLUSION.....	35
	REFERENCES .....	36
	APPENDICES.....	39
	General network vulnerability score assessment .....	39
	Network attack vector.....	39

Attack complexity vector.....	39
Attacker privileges vector .....	40
Attacker collaboration vector .....	40
Attacker scope vector.....	40
Confidentiality impact vector .....	41
Integrity impact vector .....	41
Availability impact vector .....	41

## 1 INTRODUCTION

The production process control system is designed to collect data on the status of devices used in production, monitor their parameter compliance with the values projected in the designs, and adjust parameter values depending on the product being manufactured. For the operation of the control system, it is crucial that the data transmission is fast, reliable, and protected from cyber-attacks. If the data transmission is disrupted, the production process becomes uncontrollable, the quality of the product being manufactured suffers, or the production itself may even be disrupted.

To ensure a smooth production process, this thesis proposes the implementation of a G-PON (Gigabit-Passive Optical Network) technology (ITU-T, 2008a). G-PON can provide faster and higher quality communication between devices, has a higher reliability, and is not affected by external electric fields.

In the production, an internal network completely separated from the outside network. This ensures protection against cyber-attacks of the outside network. The use of G-PON in an internal network is a new and unexplored aspect. Considering the distances and speeds at which data is transmitted using optics, it can be argued that it may be useful in cases where very reliable data transmission is required (ITU-T, 2014).

Currently in the production, electronic switches connected by copper network cables are used, which consume a lot of electricity and are less resistant to the external environment. The network cable consists of as many as 8 copper wires of  $0.5 \text{ mm}^2$ , and this metal is relatively expensive. Applying optical technology, only one optical fiber with a diameter of  $0.125 \text{ mm}$  is needed to connect two network devices. The signal going through the optical fiber is directed to the required network device using a separate, very small-sized, optical signal splitter, which does not use any electrical energy. At present, the optical cables in production are used only to connect network switches. The use of G-PON opens up opportunities to implement a network that uses optical data transmission technology.

The aim is to design a reliable optical data transmission network to ensure the high-quality functioning of the production process. This network is vital for the operation of the control system, ensuring fast, reliable, and secure data transmission. Any disruption in this system could lead to uncontrollable production processes and potentially compromise the quality of the products that are being manufactured.

This thesis will explore the potential of G-PON technology for the data transmission in the production environment, assessing its suitability for delivering fast, reliable, and high-quality communication between devices. The research will focus on designing a G-PON-based data transmission network specifically for production process control systems, a novel approach in the context of internal networks. A critical component of the study will be evaluating the cybersecurity level of G-PON, ensuring the designed system is resilient against potential cyber threats. A Practical application will be demonstrated through the creation of a full network project model using the "Packet Tracer" program.

## **2 G-PON VS ETHERNET: A PRODUCTION PROCESS ANALYSIS**

This section of the thesis presents the analytical aspects of the project, including the types of data transmitted, the relevance and design of G-PON technology, energy efficiency requirements, and the differences compared to conventional Ethernet-based networks.

### **2.1 Types of data transmitted during the production process**

Various processes in production are continuous. These processes are managed by PLC controllers (IEC, 2013) designed to control production devices, sensors used to collect process and product information. Computers for processing the collected information, and surveillance cameras to monitor the production processes and the entire production line's operation. These devices use Ethernet technology, which is unreliable, consumes a lot of electrical energy, and requires careful maintenance (often, there is a high temperature in the smaller network racks).

By utilizing G-PON technology, we can create a network that allows the transmission of a large amount of data in various forms (visual, audio, measurements - temperature, pressure, etc.) and ensures high reliability and consistent performance. Additionally, it provides an opportunity to save significant energy costs. Unlike traditional Ethernet technology, G-PON offers a more efficient, reliable, and energy-saving solution for managing and monitoring the complex and continuous processes involved in production.

### **2.2 Relevance of G-PON technology**

The longevity of G-PON is ten times greater than Ethernet. Optical network equipment is characterized by its small size and high speed, moreover, information can be transmitted over long distances (ITU-T, 2008c). In a G-PON network, optical line terminals (OLTs), optical network access blocks (ONUs, sometimes marked as ONT - Optical Network Terminal), and passive elements such as optical fibers and optical splitters are used instead of conventional

switches and network cable bundles. Passive elements are durable and do not use electricity at all (UFiber, 2020).

The comparison of Ethernet and G-PON networks is presented (Figure 1). The flows transmitted by the Internet core network are distributed differently to users. In the Ethernet network, flows are distributed using network routers. The internet flow is transmitted to the end users via network switches. In the case of G-PON, all the main flow from the OLT is sent directly to all end users via a single optical fiber and optical splitters.

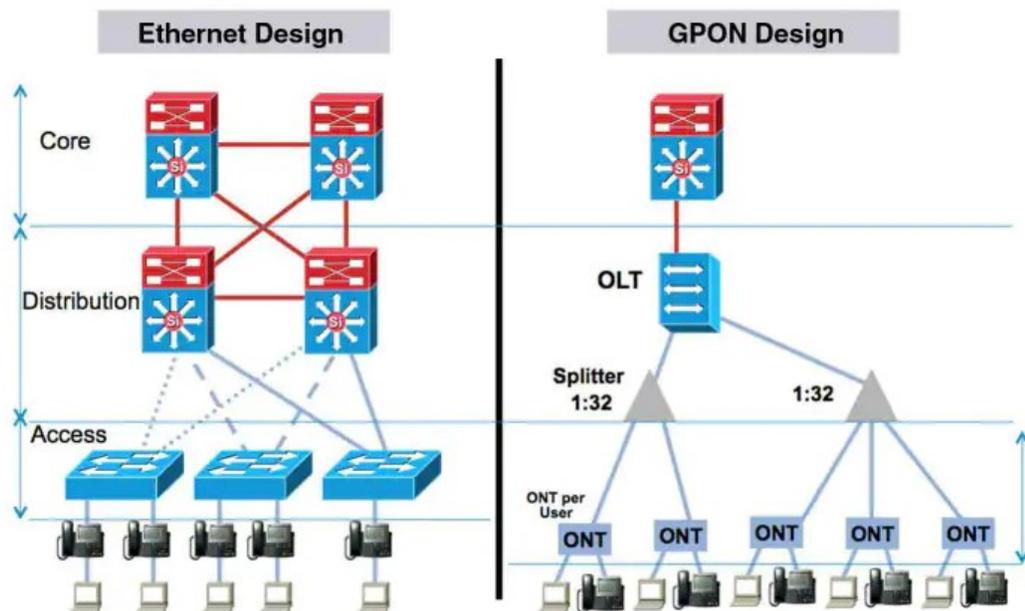


Figure 1 Comparison of Ethernet and G-PON networks (CISCO, 2022)

The information of different users is separated according to the ONU identifier and encryption key. In individual cases, a VPN can be used (Yeh, C. H., Wang, B. Y., Hsu, W. H., Liu, L. H., & Ko, H. S., 2021). Using a VPN, the device's information is encrypted and travels through a private service provider instead of the used internet provider. A VPN also masks the device's IP address, thus protecting against various cyber-attacks. In practice, it is common for devices to use internet access, but in the internal network, the main protection is the configuration of ports against unauthorized device connections, which, using malicious tools, pose a threat to the entire network.

The distance from the distribution router to the access switch according to the Ethernet standard cannot exceed 100 meters, while G-PON is capable of sending a signal up to 60km. Moreover, only one device can be connected via a single Ethernet cable, while up to 128 end devices can be connected to a single optical fiber. The G-PON network is economical not only because of the single fiber but also due to the three possible states of the ONU: off, standby, and active. A network device in standby mode switches to active mode only when a signal is received from the end device (Bertoldi, P., & Lejeune, A., 2021). In this way, the device consumes less electrical energy.

To compare energy consumption, we need to consider the electrical energy consumption of the devices, as outlined in Table 1.

Table 1 Electric power consumption of Ethernet and G-PON devices

Name of the device	Electric energy consumption (W)	Visual of device	URL	Energy consumption per user
<b>Cisco Ws-C3650-24Ps-L 24 Port Poe 4X1G – switch</b>	100-390W		<a href="#">Cisco-WS-C3650-24TS-L</a>	From 4,14W To 16,25W
<b>UISP Fiber OLT</b>	85W		<a href="#">UISP Fiber OLT</a>	From 0,66W To 0,08W

For a standard switch port, which is dedicated to each user, the average power consumption ranges from  $100/24 \approx 4.17W$  to  $390/24 = 16.25W$ . In the case of an OLT, one port can be shared by 128 users, or 1024 users in the case of NG-PON2. The average power consumption per user is  $85/128 \approx 0.66W$  or  $85/1024 \approx$

0.08W, respectively. This demonstrates the superior energy efficiency of G-PON technology, particularly when serving a larger number of users.

The parameters of a three-output optical splitter 1x2 are marked in Figure 2. They are most often described by the ratios of signal powers, expressed in decibels (dB). The splitter itself takes into account power losses, which vary from 0.2 to 0.3 dB depending on the manufacturing technology (ITU - L.208, 08/2019).

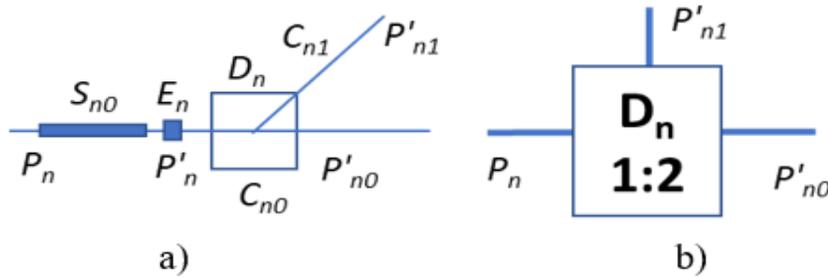


Figure 2 a) - Diagram of the optical splitter; b) – Labelling of the optical splitter

The main parameters of the optical splitter are as follows:

- signal losses in the trunk direction

$$IL_{n0} = -10 \lg \frac{P'_{n0}}{P'_0} \quad (1)$$

- signal losses in the branch direction

$$IL_{n1} = -10 \lg \frac{P'_{n1}}{P'_0} \quad (2)$$

- splitter signal power losses

$$E_n = -10 \lg \frac{P'_{10} + P'_{10}}{P'_0} \quad (3)$$

- splitter attenuation in the branch direction

$$C_{n1} = -10 \lg \frac{P'_{10}}{P'_{10} + P'_{11}} \quad (4)$$

- splitter attenuation in the trunk direction

$$C_{n0} = -10 \lg \frac{P'_{11}}{P'_{10} + P'_{11}} \quad (5)$$

Optical splitters in packages usually also specify the power ratio of branches N:M.

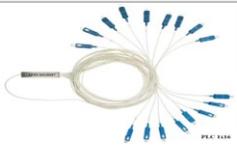
$$N = 10^{-\frac{C_{n0}}{10}}; M = 10^{-\frac{C_{n1}}{10}} \quad (6)$$

The notations used in the formulas are:

- $S_{n0}$  – optical fiber signal losses;
- $P_n$  – signal power at the element input;
- $P'_n$  – signal power at the splitter input;
- $P'_{n0}$  and  $P'_{n1}$  are signal powers at the splitter outputs.

Theoretical and real splitter parameters are presented in Table 2.

Table 2 "Fiber Optics Association" provided splitter parameters (FOA, 2019b)

Splitter Ratio	Example	Theoretical Losses IL 10lg (dB)	Splitter Losses En (dB, max)	Manufacturers specified IL+En Losses (dB)
1x2		3	1	4
1x4		6	1	7
1x8		9	2	11
1x16		12	3	15
1x32		15	4	19

The numerical values of the parameters  $C_{n0}$  and  $C_{n1}$  are calculated when designing the optical trunk. By calculating the signal attenuations, we find out what type of optical splitter power ratio we need in each splitter to get the same

signal attenuation from the OLT to each ONU. The standards provide for both transmitted and received signal levels in OLT and ONU devices. NG-PON2 (Next Generation-Passive Optical Network 2) provides for four classes of ODN (Optical Distribution Network) (ITU, 2021). To ensure reliable network operation, it is very important to maintain the set signal level differences specified in Table 3 (ITU-T, 2021).

Table 3 Attenuation limits in the optical trunk (ITU-T, 2021)

<b>FTTx class</b>	<b>N1</b>	<b>N2</b>	<b>E1</b>	<b>E2</b>
Minimum attenuation	14 dB	16 dB	18 dB	20 dB
Maximum attenuation	29 dB	31 dB	33 dB	35 dB
Attenuation difference	15 dB			

In production lines, distances from the access switch to devices according to the IEEE 802.3 standard are up to 100 meters. G-PON technology is adapted for longer distance transmission. The documentation of the "Fiber Optics Association" indicates - single-mode fiber attenuation at 1310 nm wavelength is 0.5 dB, and at 1550 nm wavelength it is 0.4 dB. In this case, the requirements are specified in Table 3.

### **2.3 G-PON energy efficiency requirements**

In the case of G-PON as described in the subchapter 2.2, less electrical energy is consumed than ethernet (Table 1) and copper cables are not used for inter-device connection. The OLT (Optical Line Terminal) does not require careful maintenance since this device has a good cooling system. When using Ethernet electronic switches, it is necessary to follow the manufacturer's specified temperature mode, as copper wires and other internal components can damage the device at high temperatures. Artificial cooling of switching cabinets is often used in practice.

The ONU (Optical Network Unit) device used in the optical network is in two states: On-State and Idle-State. The On-State is when the user is connected and using the internet connection, the Idle-State is when the device is in standby

mode and transitions to the On-State when the internet connection is active. In Idle-State, the device consumes less energy (Table 4).

Table 4 Comparisons of electrical consumption for network interface modes (Bertoldi, P., & Lejeune, A., 2021)

Home gateway central functions plus WAN interface	Tier 2021: 1.1.2021 - 31.12.2021		Tier 2022: 1.1.2022 - 31.12.2022		Tier 2023: 1.1.2023 - 31.12.2023	
	<b>Idle- State (W)</b>	<b>On- State (W)</b>	<b>Idle- State (W)</b>	<b>On- State (W)</b>	<b>Idle- State (W)</b>	<b>On- State (W)</b>
Gigabit Ethernet WAN	2,3	3,5	2,3	3,3	2.3	3.3
2.5 Gigabit Ethernet WAN	2,9	5,0	2,9	5,0	tbd	tbd
5 Gigabit Ethernet WAN	2,9	5,0	2,9	5,0	tbd	tbd
10-Gigabit Ethernet WAN	3,9	6,5	3,9	6,5	tbd	tbd
Fibre PtP Fast Ethernet	2,1	3,9	2,1	4,1	tbd	tbd
Fibre PtP Gigabit Ethernet	2,1	4,1	2,1	4,1	tbd	tbd
GPON	3,0	3,2	2,8	3,0	2,7	2,9
1G-EPON	3,0	3,2	2,8	3,0	2,7	2,9
10/1G-EPON	3,0	4,0	2,9	3,8	2,8	3,8
10/10G-EPON	3,3	5,0	3,2	5,0	3,0	5,0
10/2.5 XG-PON1	3,0	4,5	2,9	4,5	2,8	4,5
10/2.5 NG-PON2	3,0	4,5	3,0	4,5	tbd	tbd
10/10 XGS-PON	3,3	5,5	3,2	5,1	3,0	4,8
10/10 NG-PON2	3,3	5,5	3,3	5,5	3,3	tbd
DOCSIS 3.1	9,8	13,4	9,3	13,1	tbd	tbd
4G	2,8	4,0	2,8	4,0	tbd	tbd

The user device can also be in a third state, Off-State, when it is disconnected from the power supply. The notations used in the table are: On-State - working state, Idle-State - standby state (Bertoldi, P., & Lejeune, A., 2021a).

The conventional Ethernet network technology is older and has a similar data transmission speed to G-PON, but the electricity consumption is higher in both states. G-PON has reduced energy consumption from 3.2W to 2.9W in the "On-State" over the past three years, and compared to Ethernet, there is a difference of 0.3-0.4W over 3 years (Table 4) (Bertoldi, P., & Lejeune, A., 2021a). According to a document provided by the European Commission, it can be asserted that G-PON will continue to be improved and maintain its energy efficiency.

## **2.4 Comparative analysis of data flow management methods**

The CISCO switches currently used in the companies have many configuration settings, numerous port modifications, rules, and other security measures. One of the security practices is setting rules. A great example is MAC address filtering of ports, where the switch knows the set safe devices, and if a device is maliciously replaced, the port would be blocked and become inactive. OLT does not lag behind these technologies. The crucial thing when using G-PON is setting the correct configuration. The OLT has an easy-to-understand GUI (Graphical User Interface), where various modifications can be made, and various rules can be set for the used ports.

Using G-PON, several devices can be connected with one fiber, and this may seem unsafe, but it's not true, the OLT sees all connected devices, as signal transmission occurs at different wavelengths (ITU-T, 2022a), in this way, the device understands that more than one device operates on this fiber. Information from different users is separated according to the ONU ID and encryption key. The data transmitted between devices are protected by AES encryption, and due to high transmission speed, the information travels very quickly.

Using an Ethernet switch, only one device can be connected with one cable, each port has protection when a device is connected to the network. If the device successfully connects to the network, depending on the configuration, the user using various network port scanning tools can determine what devices are on the network and what information is available. Ethernet switches also use high transmission speed, but this is often limited to maintain a stable data stream

between all connected devices. The speed limit is set according to the type and size (in bits) of data being sent.

G-PON distributes the data flow evenly to all users, depending on the transmission speed set by the internet provider, all end devices can see changes in the data stream. Let's say there is a large data transfer in our network, at this time, checking the speed would show a decrease, and after the large flow ends, it would increase again.

So, G-PON and Ethernet networks have several differences: in device identification, data transmission, and data flow control. Both types of networks are unique, according to set configurations and data transmission capabilities.

### **3 SPECIFICATION AND DESIGN OF THE OPTICAL NETWORK**

This chapter outlines the design components of the optical network, offering an overview of the hardware and the specifications of the network elements. It includes calculations related to signal attenuation at the end points of the optical trunk branches. Moreover, it provides a snapshot of the cybersecurity considerations associated with this network design.

#### **3.1 Object to be designed**

The optical data transmission network for the production process control system.

#### **3.2 Hardware parts**

The hardware used in the designed network includes:

- Optical Line Terminal (OLT) - (1 unit) Connects the communication between the end device and the main server.
- Optical Network Unit (ONU) - (20 units) Converts the light signal into an electrical signal, and the electrical signal into a light signal.

- Optical Splitters 1x2 - (20 units) For distributing the trunk signal to end devices and for signal attenuation.
- Optical fibers - (Compliant with G.657 standard) Used to establish connections between active and passive network devices.

### **3.3 Network project specification**

The main OLT optical trunk from the production line, connected using optical fibers and 1x2 ratio signal splitters, is divided into 4 branches, forming 20 outputs. An ONU device is connected to each output, and an Ethernet port is led from it to the production devices (controllers, sensors, etc.). By using signal splitters, a uniform signal attenuation is achieved at the trunk outputs, which meets the attenuation limits of FTTx class signals (Table 3) (ITU, 2019a). This ensures safe and reliable data transmission between all devices in the network. Additionally, at the beginning of the trunk, a signal attenuator (from 5 to 10dB) is installed to regulate the signal attenuation at the outputs.

### **3.4 Production line optical network plan**

In production, the optical trunk is connected using active and passive optical elements: OLT, ONU, signal splitters, and optical fibers. All primary sensor data is stored in the main server, where backup data copying is performed. Since the distances between devices on production lines are up to 100 m, the transmitted signal is too strong, so we apply splitters (Figure 3) to create appropriate signal attenuation at the optical trunk outputs (ITU-T, 2019).

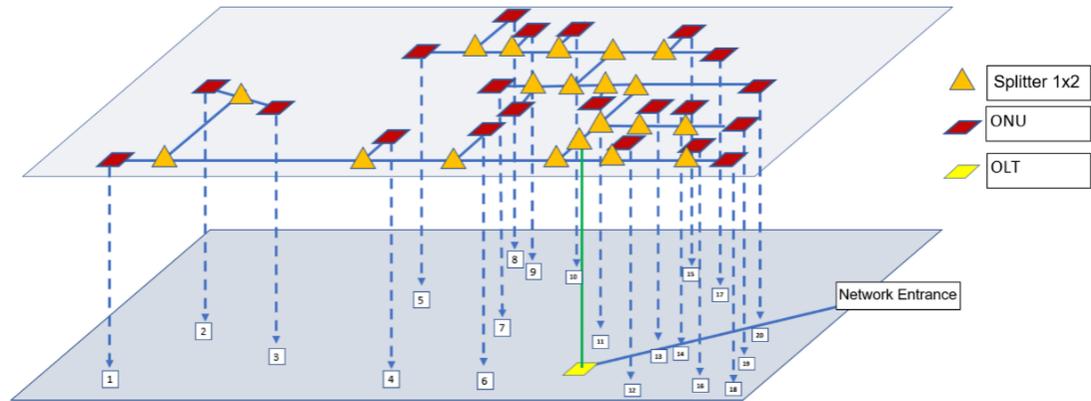


Figure 3 Layout of Optical Network Above Production Devices

From the network lead-in, we run the trunk above the production devices (Figure 3). When running the trunk, we connect splitter branches to it, at the ends of which network blocks ONU are turned on. The signal sent by the OLT can be attenuated using signal splitters or attenuators. By correctly calculating the values of the splitter parameters, uniform attenuation is obtained at the trunk outputs.

The G-PON can be successfully applied in this manner. The layout of the production line devices is indicated (Figure 3). An Ethernet type connection point is specified for each production device. The total number of connection points is 20.

The network consists of:

- Network lead-in cabinet, in which the OLT router is placed (1 unit).
- User optical network units (ONU) (20 units).
- Optical connecting cables (standard G.657).
- Optical splitters 1x2 (20 units) (Figure 4).



The network consists of a main trunk with branch trunks. The main trunk consists of OLT, a signal attenuator, and splitters  $D_9, D_8, \dots, D_1$ . A branch is connected to the  $D_9$  splitter, which consists of splitters:  $D_{9-4}, D_{9-3}, D_{9-2}$ , and  $D_{9-1}$ . A branch is connected to the  $D_8$  splitter, which consists of splitters  $D_{8-3}, D_{8-2}$ , and  $D_{8-1}$  and  $D_{8-1-1}$  and  $D_{8-2-1}$ . A branch is connected to the  $D_7$  splitter, which consists of splitters  $D_{7-2}$  and  $D_{7-1}$ . An additional splitter  $D_{6-1}$  is connected to the  $D_6$  splitter. The signal attenuator is designed to increase the signal attenuation to 15.15 dB, as provided for in the standard (ITU-T, 2019a).

Using the splitter parameters indicated in Figure 2, we calculate the signal attenuation at all ends of the splitters. To standardize signal attenuation in the network, only 1x2 type splitters (Table 2) are used (FOA, 2019b). First, we calculate the attenuation parameters for each branch. The calculation results are presented in Table 5 ( $T_{Nn}$ dB).

Table 5 The parameters of the network trunks branches

n	$S_{n1}+C'_n$	$S_{n0}+E_n$	$C_{n0}$ dB	$C_{n1}$ dB	N:M	$T_{Nn}$ dB	
<b>Branch out of 4 elements</b>							
1	0.00	0.20	3.01	3.01	0.50	0.50	7.56
2	0.00	0.20	1.69	4.90	0.68	0.32	7.56
3	0.00	0.20	1.16	6.27	0.76	0.24	7.56
4	0.00	0.20	0.88	7.35	0.82	0.18	7.56
<b>Branch out of 3 elements</b>							
1	0.00	0.20	3.01	3.01	0.50	0.50	8.32
2	3.21	0.20	3.01	3.01	0.50	0.50	8.32
3	3.21	0.20	1.69	4.90	0.68	0.32	8.32
<b>Branch out of 2 elements</b>							
1	0.00	0.20	3.01	3.01	0.50	0.50	5.11
2	0.00	0.20	1.69	4.90	0.68	0.32	5.11
<b>Branch out of 1 element</b>							
1	0.00	0.20	3.01	3.01	0.50	0.50	3.21

The table 5 contains the following notations:

- $S_{n1}+C'_n$  – signal attenuation in the splitter branch, consisting of the branch connection attenuation  $S_{n1}$  and the attenuation of the branch itself -  $C'_n$ ;
- $S_{n0}+E_n$  – signal attenuation in the optical line connecting two adjacent optical splitters;
- N:M – optical splitter signal splitting ratio (always  $N+M=1$ );

- $T_{Nn}$  – optical signal attenuation at the ends of the trunk.

For branches consisting of 3 elements, in the column  $S_{n1}+C'n$ , rows 2 and 3, the attenuations of the splitters  $D_{8-1-1}$  and  $D_{8-2-1}$  are inserted.

By summing the data marked in blue to the overall table, the attenuation obtained at each of the terminal devices of the splitters is determined. The total trunk attenuation is indicated in Table 6.

Table 6 Overall parameters of the network trunks branches

n	$S_{n1}+C'n$ , dB	$S_{n0}+E_n$	$C_{n0}$ dB	$C_{n1}$ dB	N:M		$T_{Nn}$ dB
1	0.00	0.20	3.01	3.01	0.50	0.50	15.15
2	0.00	0.20	1.69	4.90	0.68	0.32	15.15
3	0.00	0.20	1.16	6.27	0.76	0.24	15.15
4	0.00	0.20	0.88	7.35	0.82	0.18	15.15
5	0.00	0.20	0.70	8.25	0.85	0.15	15.15
6	3.21	0.20	1.13	6.38	0.77	0.23	15.15
7	5.11	0.20	1.27	5.95	0.75	0.25	15.15
8	8.32	0.20	1.78	4.72	0.66	0.34	15.15
9	7.56	0.20	1.03	6.72	0.79	0.21	15.15
10	5.00	0.20	0.46	9.94	0.90	0.10	15.15

After calculating the attenuations in the branches, we calculate the signal attenuation in the entire network. In the rows 6, 7, 8, 9, 10 of the column  $S_{n1}+C'n$ , the branch attenuations given in Table 5 are substituted.

Finally, after calculating the total trunk signal attenuation at the ends, we get 15.15dB, which fully satisfies the signal requirement standard for terminal devices. In addition, it should be noted that a 5 dB attenuator is used at the beginning of the line (Figure 5), also indicated in the tenth row of Table 6, as the combined splitters, without the attenuator inserted at the beginning, do not provide sufficient attenuation. This trunk principle is flexible, as at any time, if there is a need to increase attenuation, we can insert a more powerful attenuator at the beginning, as there are several types of them with different power levels.

### 3.6 Cybersecurity assessment of G-PON technology

In PON, all downstream data is broadcast to all ONU connected to the PON. If a malicious user reprogrammed their ONU, they could receive everyone's data. The PON security system is designed to eliminate this specific "threat".

An advanced encryption algorithm (AES) is used for this purpose. This is a block cipher that operates on 16-byte (128-bit) data blocks. It accepts keys of 128, 192, and 256 bits. This algorithm is described in documents published by the U.S. National Institute of Standards and Technology (NIST). Only the GEM (Gigabit Passive Optical Network Encapsulation Method) frame/fragment is encrypted. The GEM headers are not encrypted. As fragments do not necessarily have to be a contiguous number of blocks, the last data block (from 1 to 16 bytes) is XOR marked with the most significant part of the last AES encryption block (16 bytes long). The redundant part of the last cipher block is discarded. GEM frames have a dependent interface ID and only identify GEM frames that belong to a certain ONU (Figure 6) (ITU-T, 2014).

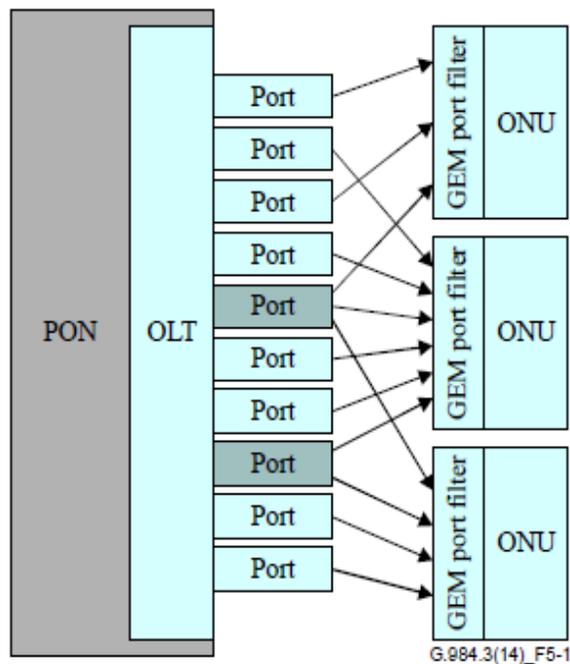


Figure 6 Data transmission multiplexing (ITU-T, 2014)

It is also assumed that the OLT and ONU already have configured port IDs for encrypted operation and they already have a set key, which is used for data exchange. Both the ONU and OLT store their key information in *active\_key\_registers*, which is the register used by the algorithm. The key exchange is initiated by the OLT. It sends a *request\_key* message to the PLOAM channel. The ONU responds by generating, saving, and sending a key. The ONU stores the new key in the *shadow\_key\_register*. The generated key, created by the ONU, should be cryptographically unpredictable.

### 3.7 Comparison of 1+1 and 1:1 reservation schemes

The 1+1 and 1:1 reservation schemes in GPON are important protection mechanisms that can be implemented to improve network availability and reliability.

In the context of a GPON network, "1:1" refers to a protection scheme where two identical optical paths are set up between the Optical Line Terminal (OLT) and the Optical Network Unit (ONU) or Optical Network Terminals (ONT) (Figure 7) (Lo. R., 2013a).

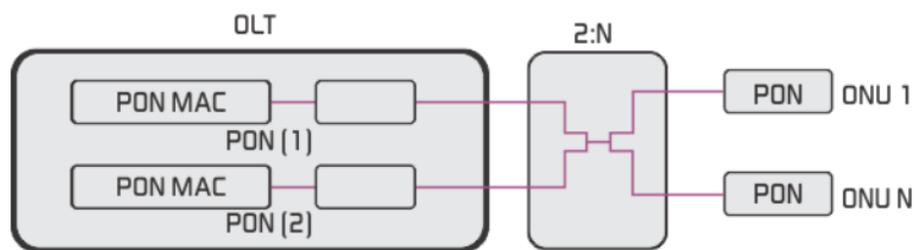


Figure 7 1:1 duplication (Lo. R., 2013a)

One path is designated as the primary, while the other is left as a backup or standby path (meaning it is unused until needed). Suppose an incident occurs where the primary line is disrupted, then all traffic is automatically redirected to the backup path. In this case, the data flow is uninterrupted and the network automatically becomes more reliable, with downtime being zero or very minimal in the event of a problem.

On the other hand, the "1:1" protection scheme refers to a specific backup path designated for each primary path. This means that for each active optical path between the OLT and the ONU/ONT, there's a backup path in case of failure. This ensures a higher level of availability and protection compared to the "1+N" scheme (Figure 8) (Lo. R., 2013a).

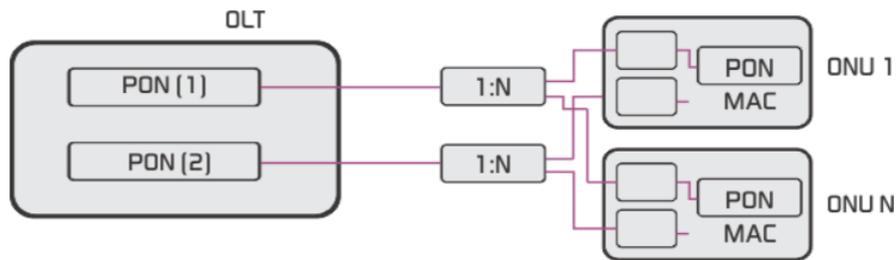


Figure 8 1+1 duplication (Lo. R., 2013a)

Currently, a similar model is used in production, where a device always has an active backup that allows continuous operation. Companies currently use "Cisco WS-3650-24PS-L" model switches, installing them in each production line in switch cabinets. Optical cables are led into each cabinet because they are faster and cheaper to bring over longer distances. These are second-level switches with 24 10/100/1000Base-T ports and 4 10G SFP+ ports.

The main switch is duplicated with duplicated power and operates in such a way that if one stops, the work will continue with the other. This is a good example of redundancy and high availability in network design, which is crucial for maintaining continuous production processes. However, the transition to G-PON technology may offer even more benefits in terms of reliability, energy efficiency, and scalability.

### **3.8 VPN establishment in G-PON network**

Chien-Hung Yeh, (Member, IEEE), Bo-Yin Wang, Wei-Hung Hsu, Li-Hung Liu, and Han-Shin Ko: A Simple WDM-PON Architecture Together with Private Interconnected ONUs.

The authors of the article suggest using separate wavelength signals for VPN creation in a G-PON network. This can be achieved by utilizing the capabilities of WDM technology. For this, a 4-wavelength grating in the OLT device and a remote node performing MUX/DEMUX functions are used. In this way, data between two ONUs are transmitted at wavelengths that are independent of G-PON, and the signals do not reach the OLT.

### **3.9 Application of network security enhancing measures**

The internal network of the company is designed for communication between production process control devices. No internet service is used in this, but it does not mean that the network is secure. Often, various repair works, modifications, or other tasks for production devices involve connecting to the network with a computer, which could be infected with various malicious files. Not only the computer, but any other malicious device connected to the internal network can lead to data loss or communication problems. Using the good practice questionnaire created by the SANS Institute and the Council on Cyber Security, which enhances cybersecurity measures (Table 7), the security of the production internal network is established, where it is suggested to replace the currently used Ethernet network technology with G-PON.

Table 7 Questionnaire on measures increasing network security (Ramadan. M., 2015)

Num	Security-enhancing measure	Is the measure applied?	
		Yes	No
1.	Identification of network devices allowed to use the institution's network services	Yes	-
2.	Identification of allowed and disallowed software	Yes	-
3.	Provision for secure configuration of hardware and software in mobile devices, workstations, or service stations	Yes	-
4.	Continuous system vulnerability assessment and security gap remediation	Yes	-
5.	Control over the use of administrator privileges	Yes	-
6.	Monitoring, analysis, and storage of audit log entries	Yes	-
7.	Protection of email and browsers	-	No
8.	Protection against malware	Yes	-
9.	Restrictions on the use of network ports, protocols, and services	Yes	-
10.	Data recovery capability	Yes	-
11.	Provision for secure configuration of network devices, such as firewalls, routers, switches	Yes	-
12.	Network perimeter protection	Yes	-
13.	Data protection	Yes	-
14.	Access control based on the principle of "need to know"	-	No
15.	Wireless access control	Yes	-
16.	Monitoring and control of user accounts	-	No
17.	Identification of network devices allowed to use the institution's network services	Yes	-
18.	Application security	Yes	-
19.	Response to incidents and their management	Yes	-
20.	Penetration testing and "red team" exercises	-	No

The security measures indicated in the table are necessary to ensure the security of any type of network. After conducting the questionnaire, positive answers were given to 16 out of the 20 questions presented. Such a result indicates a high level of cybersecurity and a low level of vulnerability

### 3.10 Vulnerability assessment of G-PON for production management

In further assessing the vulnerability of the G-PON network planned for implementation within the manufacturing company, it has to be considered about the production management network's isolation from the external internet. This isolation shapes vulnerability assessment as follows:

*Attack Vector (AV:P)* - The primary challenge for an attacker is gaining physical access to the internal network, given its disconnection from the external internet. The attacker would need to infiltrate the premises and connect to the network physically, which is further complicated by port security measures that prevent open port access to the internal network. Attempting to disconnect an operating device and connecting to the network through it might seem feasible, but configurations such as "sticky MAC address" and "port security" on the port would automatically disable the port. Given these complexities and the time required to overcome them, the attack vector score is low (appendix 2).

*Attack Complexity (AC:L)* - If an attacker connects to the network, in this case he can exploit the vulnerability at any time. This very much depends on whether he will be fast and efficient. If he doesn't make it in time, the network's security measures can automatically disconnect devices to prevent the spread of malware throughout the network, making speed and efficiency critical for the attacker (appendix 3).

*Privileges Required (PR:H)* - In order for an attacker to launch an attack, they need to go through a regular user login and then gain administrator rights. Once they launch the component, the security system may be able to block the device from the network faster, even before it has time to infect the network (appendix 4).

*User Interaction (UI:R)* - An attacker connected to the network cannot access administrative tools, so they need rights to perform an attack. Also, to reach the internal network, they need to find a user who is also password-protected, so to launch an attack, they need to obtain the login details of at least one employee (appendix 5).

*Scope (C)* - The attacker can potentially affect a wide range other components as well. Given the star-shaped configuration of the network, if the attacker's program reaches the main switch, the effects could be far-reaching (appendix 6).

*Confidentiality Importance (C:N)* - Confidentiality is not a significant concern in this network. The internal network is designed to contain minimal information from the main computer. The production files do not hold significant secrets, and all data is backed up (appendix 7).

*Integrity Importance (I:N)* - The attacker may try to delete data or lock it, but backup copies are created for all files and devices, so the loss will be zero (appendix 8).

*Availability Importance (A:H)* - If an attacker performs a DDOS attack, they can break access to the internal network. The data tracked by the monitoring program can interrupt data flows and can damage production monitoring information and slow down system performance (appendix 9).

The network vulnerability vector is as follows:

**CVSS:3.0/AV:P/AC:L/PR:H/UI:R/S:C/I:N/A:H.**

This vulnerability assessment is very critical for understanding the potential risks associated with implementing G-PON technology in this specific context and for developing strategies to mitigate these risks (appendix 1).

The full assessment of G-PON vulnerability for production network is presented in Figure 10.

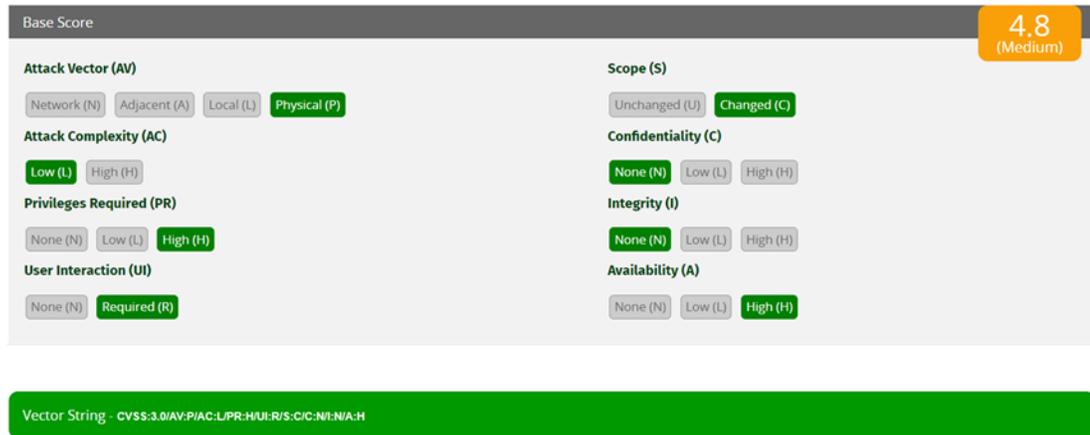


Figure 9 Base network vulnerability calculation assessment (First, n.d.)

This assessment reveals a medium vulnerability score of 4.8 for the production network, based on CVSS metrics such as attack vector, attack complexity, privileges required, user interaction, scope, and the importance of confidentiality, integrity, and availability. This score is relatively typical for an internal network with minimal external connections. It underscores the inherent security risks of the network, despite its isolation from the external internet.

## 4 EXPERIMENTS WITH G-PON

This segment presents an experiment which is conducted using actual hardware. A minimalist prototype of the optical network trunk is created, along with the connected and driven end equipment. The Optical Line Terminal (OLT) user interface and its settings are reviewed. Additionally, a virtual model of the production network is designed using the Packet Tracer program.

### 4.1 Implementation of the optical trunk

In the laboratory, an experiment was conducted using optical equipment such as the Optical Line Terminal (OLT), Optical Network Units (ONU), Optical Network Terminals (ONT), optical splitters, single-mode fibers, and measurement tools. These tools include a light signal source (Figure 12) (SENER, n.d.) and an optical radiation power meter (Figure 11) (TRIBRER, n.d.).



Figure 10 TriBrer BOU350C.ZN is an optical power meter (TRIBRER, n.d.)



Figure 11 ST815C optical signal source (SENER, n.d.)

These tools are used to determine the strength of the transmitted light signal. Incorrectly measuring the signal strength poses a risk of damaging the optical module in the OLT device.

In this experiment, a backbone was created from 6 signal splitters (95% x 5%), to which 3 active optical devices were connected. Before connecting the devices to the backbone, we measured the signal attenuation of all outputs. The measurements were made using the optical signal source shown in Figure 12

and the optical radiation power meter shown in Figure 11. Both devices were set to a wavelength of 1310 nm. Before measuring the backbone, the devices were calibrated by directly connecting them with a simple fiber, resulting in an approximate signal attenuation of -6.01 dB. After calibrating the devices, the signal source is connected to the start of the backbone, which is depicted in red on the right in Figure 13, and the power meter is connected to any output with a 5% attenuation.



Figure 12 Optical Line Terminal

After measuring all the outputs, an approximate signal attenuation of -16.50 dB is obtained. The LITNET 10Gbps internet is connected to the SFP+ port on the OLT.

The full prototype of the network trunk is shown in Figure 14.



Figure 13 Optical network trunk

The signal splitter boxes are placed close to each other, because of the network operation is tested in the lab and equipment parameters are fixed and long distances were not necessary. The test uses 3 active optical devices, 2 ONU, and 1 ONT. They are connected to the power source and with the patch cables to the splitter outputs. Each device has status indicator lights (Figure 15). All of the devices are lit in white, which indicates a successful connection of the device for use. Other light modes that could occur during the use of the device are described in the manufacturer's device documentation.



Figure 15 Optical network devices (ONT-left and ONU-right)

A minimalistic prototype of the optical network trunk is presented in Figure 16.

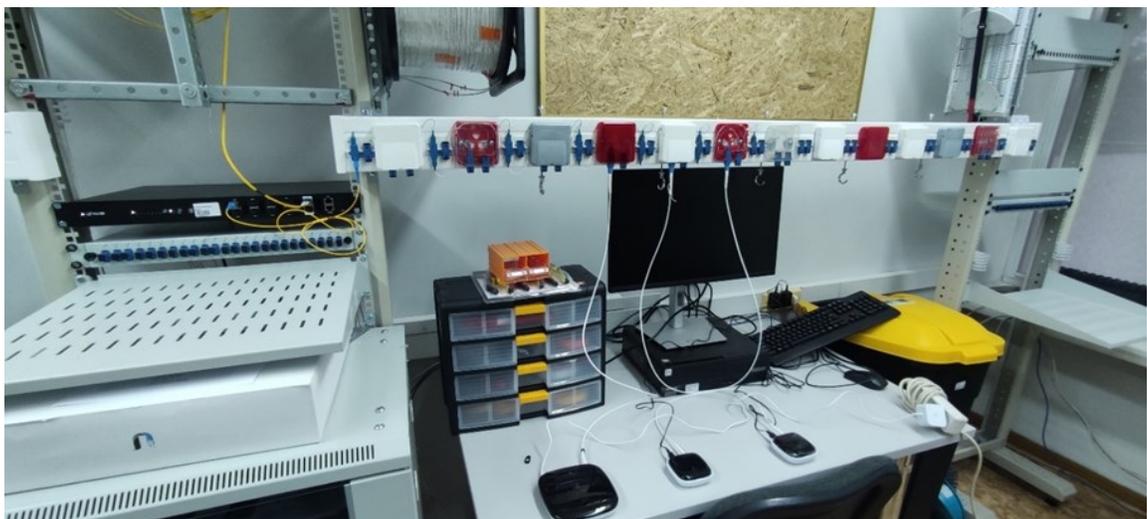


Figure 16 Optical network prototype

In the case of connecting to one of the ONUs - with a computer or phone, an already configured or default IP address is entered into the web browser, and a login window to the OLT user panel should appear on the screen, as shown in Figure 17. Often, the manufacturer provides the login data in the documentation or on the equipment's informational sticker.

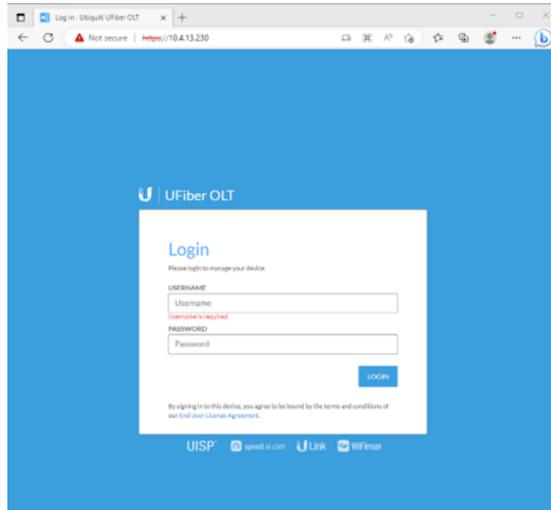


Figure 14 "UFiber" OLT login screen

Upon logging into the user panel, you can see the OLT settings, power consumption, temperature, and cooling fan speed (Figure 18).

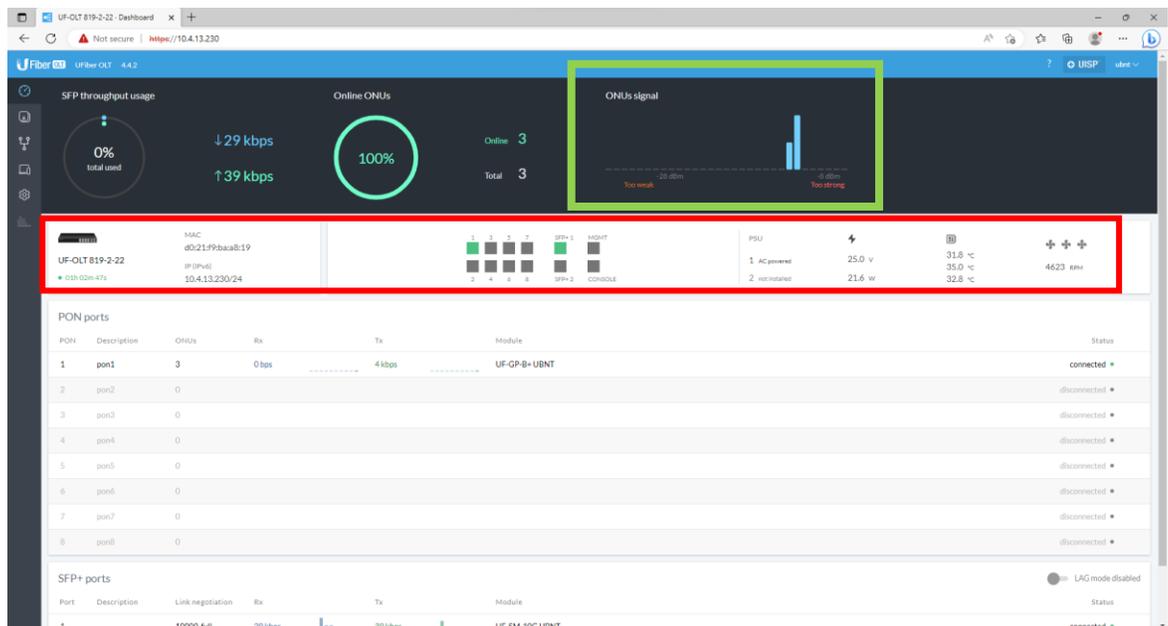


Figure 15 OLT Graphical User Interface



## 4.2 Production line "Packet Tracer" G-PON model

Using the "Cisco Packet Tracer" program, an optical data transmission network for the production process control system has been modeled (Figure 20).

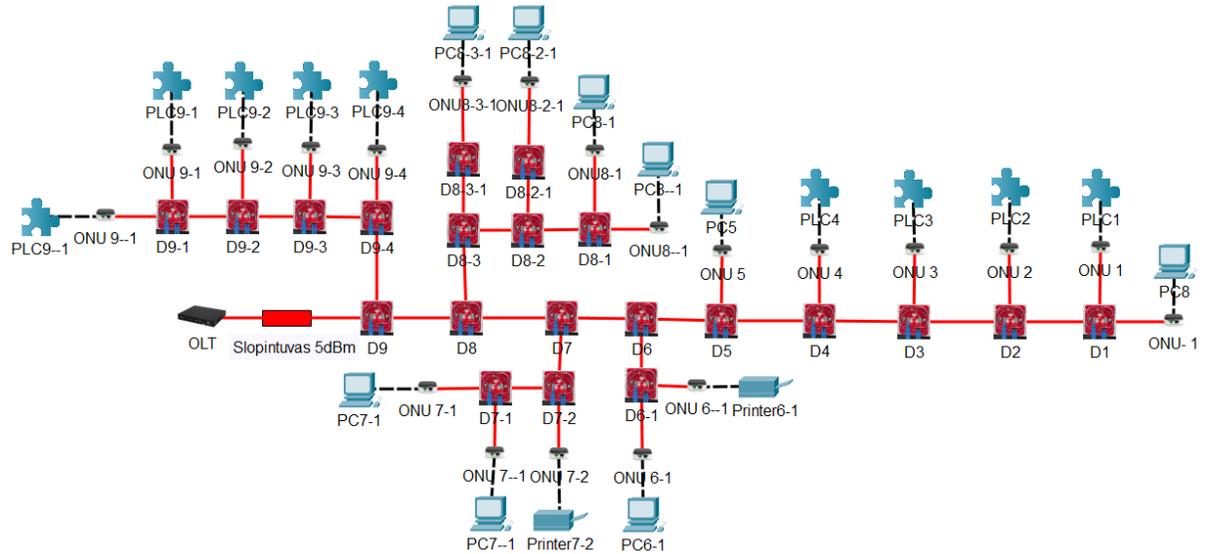


Figure 17 "Packet Tracer" optical trunk model

In this trunk, all devices: PLC controllers, printers, and personal computers are connected to a common trunk through a single fiber, which is divided into 4 branches by signal splitters and has a total of 20 outputs. An ONU device is connected to each output, and from this, an Ethernet cable is run, at the end of which a socket is installed for connecting the production device with a patch cable.

## 5 CONCLUSION

The possibilities of the G-PON network were explored and the suitability of data transmission between manufacturing devices was determined. It was found that G-PON can be applied in production by creating an optical trunk by sequentially connecting signal splitters. The necessary splitter parameters were calculated according to the created trunk, creating conditions for data transmission of production devices.

A data transmission network between manufacturing devices for the production process control system was designed. The project is applied to the production line, the network starts from the main cabinet and is routed above the manufacturing devices.

The level of cybersecurity of G-PON was evaluated by determining the data transmission encryption algorithm, the network redundancy principles of "1+1" and "1:1", the possibilities of applying measures to increase network security, and the determination of cyber vulnerability using the CVSS calculator.

A complete network project model was created using the "Cisco" network system modeling program "Packet Tracer". The model specifies all the necessary devices for project implementation and provides examples of possible devices.

The G-PON project offers superior scalability, data transmission speed, and reliability over Ethernet-based networks, despite its increased complexity in design and setup. However, many companies are not yet prepared to adopt this technology due to gaps in knowledge and management skills.

## REFERENCES

Bertoldi, P., & Lejeune, A. (2021). Code of Conduct on Energy Consumption of Broadband Equipment. Available at: <https://doi.org/10.2760/10053> [Accessed 05 Feb 2024]

CISCO. (2018). Cisco Catalyst 3650 Series Switches. Available at: [https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3650-series-switches/data\\_sheet-c78-729449.pdf](https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3650-series-switches/data_sheet-c78-729449.pdf) [Accessed 06 Feb 2024]

CISCO. (2022, November 9). Understand GPON Technology - Cisco. Available at: <https://www.cisco.com/c/en/us/support/docs/switches/catalyst-pon-series/216230-understand-gpon-technology.html> [Accessed 06 Feb 2024]

First (n.d.) Common Vulnerability Scoring System version 3.1. Available at: <https://www.first.org/cvss/calculator/3.1> [Accessed 08 Mar 2024]

FOA. (2004). Guidelines On What Loss to Expect When Testing Fiber Optic Cables. Available at: <https://www.thefoa.org/tech/loss-est.htm> [Accessed 12 Feb 2024]

FOA. (2019). The FOA Reference For Fiber Optics - Testing Fiber Optic Couplers, Splitters Or Other Passive Devices. Available at: <https://www.thefoa.org/tech/ref/testing/test/couplers.html> [Accessed 12 Feb 2024]

IEC. (2013 IEC 61131-3 | PLCopen. Available at: <https://plcopen.org/iec-61131-3> [Accessed 18 Feb 2024]

IEEE. (2022). 802.3-2022 - IEEE Standard for Ethernet. Available at: <https://standards.ieee.org/ieee/802.3/10422/> [Accessed 18 Feb 2024]

ITU-T. (2006). Implementers' Guide for ITU-T Rec. G.984.3 (02/2004) Gigabit-capable Passive Optical Networks (G-PON): Transmission convergence layer specification. Available at: <https://www.itu.int/rec/T-REC-G.984.3-201401-I/en> [Accessed 19 Feb 2024]

ITU-T. (2008a) ITU-T Rec. G.984.1 (03/2008) Gigabit-capable passive optical networks (GPON): General characteristics. Available at: <https://www.itu.int/rec/T-REC-G.984.1-200803-I/en> [Accessed 19 Feb 2024]

ITU-T. (2008b). ITU-T Rec. G.984.4 (02/2008) Gigabit-capable Passive Optical Networks (G-PON): ONT management and control interface specification. Available at: <https://www.itu.int/rec/T-REC-G.984.4-200802-I/en> [Accessed 27 Nov 2023]

ITU-T. (2008c). ITU-T Rec. G.984.6 (03/2008) Gigabit-capable passive optical networks (GPON): Reach extension. Available at: <https://www.itu.int/rec/T-REC-G.984.6-200803-I/en> [Accessed 27 Nov 2023]

ITU-T. (2009) G. Imp.984.4: Implementers' Guide for Recommendation ITU-T G.984.4. (10/2009) Available at: <https://www.itu.int/rec/T-REC-G.Imp984.4-200910-l/en> [Accessed 26 Nov 2024]

ITU-T. (2009). ITU-T Characteristics of a non-zero dispersion-shifted single-mode optical fibre and cable Recommendation ITU-T G.655. Available at: <https://www.itu.int/rec/T-REC-G.655-200911-l/en> [Accessed 27 Nov 2023]

ITU-T. (2010b). ITU-T Rec. G.984.7 (07/2010) Gigabit-capable passive optical networks (GPON): Long reach. Available at: <https://www.itu.int/rec/T-REC-G.984.7-201007-l/en> [Accessed 13 Nov 2023]

ITU-T. (2010c). ITU-T Characteristics of a fibre and cable with non-zero dispersion for wideband optical transport Recommendation ITU-T G.656. Available at: <https://www.itu.int/rec/T-REC-G.656-201007-l/en> [Accessed 13 Nov 2023]

ITU-T. (2010d). ITU-T Characteristics of a dispersion-shifted, single-mode optical fibre and cable Recommendation ITU-T G.653. Available at: <https://www.itu.int/rec/T-REC-G.653-201007-l/en> [Accessed 13 Nov 2023]

ITU-T. (2014). ITU-T Rec. G.984.3 (01/2014) Gigabit-capable passive optical networks (G-PON): Transmission convergence layer specification. Available at: <https://www.itu.int/rec/T-REC-G.984.3-201401-l/en> [Accessed 20 Jan 2024]

ITU-T. (2015). G.989 40-Gigabit-capable passive optical networks (NG-PON2): Definitions, abbreviations, and acronyms. Available at: <https://www.itu.int/rec/T-REC-G.989-201510-l/en> [Accessed 20 Jan 2024]

ITU-T. (2016a). ITU-T G.657 Characteristics of a bending-loss insensitive single-mode optical fibre and cable. Available at: <https://www.itu.int/rec/T-REC-G.657-201611-l/en> [Accessed 20 Jan 2024]

ITU-T. (2016b). ITU-T G.652 Characteristics of a single-mode optical fibre and cable. Available at: <https://www.itu.int/rec/T-REC-G.652-201611-l/en> [Accessed 20 Jan 2024]

ITU-T. (2016c). ITU-T X.1521 (03/2016) Common vulnerability scoring system 3.0. Available at: <https://www.itu.int/rec/T-REC-X.1521-201603-l/en> [Accessed 20 Jan 2024]

ITU-T. (2018a). ITU-T Rec. G.651.1 (11/2018) Characteristics of a 50/125  $\mu\text{m}$  multimode graded index optical fibre cable for the optical access network. Available at: <https://www.itu.int/rec/T-REC-G.651.1-201811-l/en> [Accessed 12 Jan 2024]

ITU-T. (2019a). ITU-T Rec. G.984.2 (08/2019) Gigabit-capable passive optical networks (GPON): Physical media dependent (PMD) layer specification. Available at: <https://www.itu.int/rec/T-REC-G.984.2-201908-l/en> [Accessed 12 Jan 2024]

ITU-T. (2020a). ITU-T Characteristics of a cut-off shifted single-mode optical fibre and cable Recommendation ITU-T G.654. Available at: <https://www.itu.int/rec/T-REC-G.654-202003-I/en> [Accessed 12 Jan 2024]

ITU-T. (2021). ITU-T Rec. G.9804.3 (09/2021) 50-Gigabit-capable passive optical networks (50G-PON): Physical media dependent (PMD) layer specification. Available at: <https://www.itu.int/rec/T-REC-G.9804.3-202109-I> [Accessed 26 Mar 2024]

ITU-T. (2022a). ITU-T Rec. G.984.5 (02/2022) Gigabit-capable passive optical networks (G-PON): Enhancement band. Available at: <https://www.itu.int/rec/T-REC-G.984.5-202202-I/en> [Accessed 13 Jan 2024]

Lo, R. (2013, August 28). 1:1 uplink backup protection and ring protection scenarios in PON systems. Available at: <https://fiberbit.com.tw/11-uplink-backup-protection-and-ring-protection-scenarios-in-pon-systems/> [Accessed 14 Feb 2024]

OPTINIAI DALIKLIAI - Komutacija.com. (n.d.). Available at: <https://www.komutacija.com/optiniai-dalikliai-fbt-plc-1/> [Accessed 15 Jan 2024]

Ramadan. M. (2015) - 20 Critical Security Controls for Effective Cyber Defence. Available at: <https://www.linkedin.com/pulse/sans-institute20-critical-security-controls-effective-maher/> [Accessed 13 Mar 2024]

SENER. (n.d.) Tool company's website. Available at: <https://www.senter-e.com/optical-fiber-testers-and-tools/laser-source/st815-hand-held-optical-laser-source-1310nm.html> [Accessed 15 Jan 2024]

Tohru, K., Masaki, O. & Yasuke, Y. (2010). Passive optical network system and operating method thereof: Patent. United States Patent. <https://patentimages.storage.googleapis.com/29/75/ce/15ea43df956943/US7680414.pdf> [Accessed 18 Dec 2023]

TRIBRER. (n.d.) Tool company's website. Available at: <https://tribrer.pt/en/home/43-optical-power-meter-bou350c.html> [Accessed 15 Jan 2024]

UFiber. (2020). Gigabit Passive Optical Network. Available at: [https://dl.ui.com/ds/uf\\_gpon](https://dl.ui.com/ds/uf_gpon) [Accessed 15 Jan 2024]

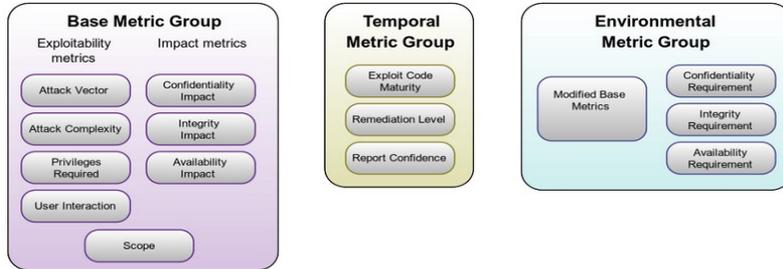
Yeh, C. H., Wang, B. Y., Hsu, W. H., Liu, L. H., & Ko, H. S. (2021). A Simple WDM-PON Architecture Together with Private Interconnected ONUs. Available at: <https://doi.org/10.1109/ACCESS.2021.3110729> [Accessed 05 Feb 2024]

Žalias namas. (n.d.) Company's website. Available at: <http://www.zaliasis-namas.lt/> [Accessed 10 Feb 2024]

APPENDICES

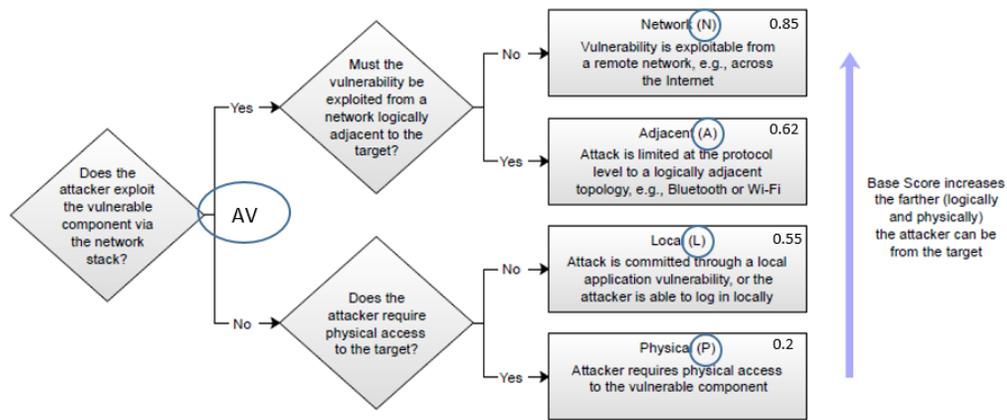
Appendix 1

General network vulnerability score assessment



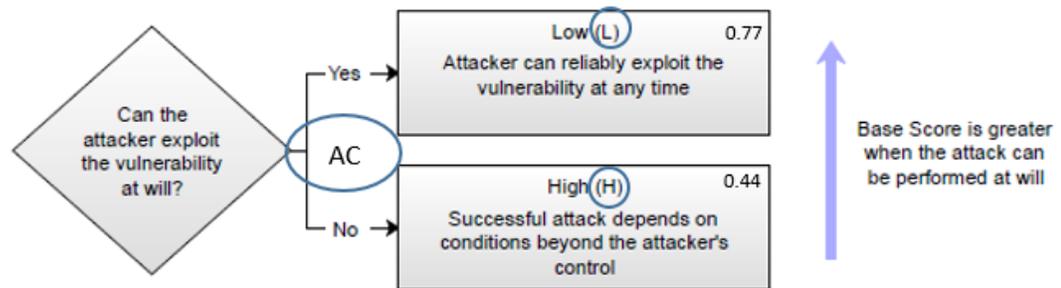
Appendix 2

Network attack vector



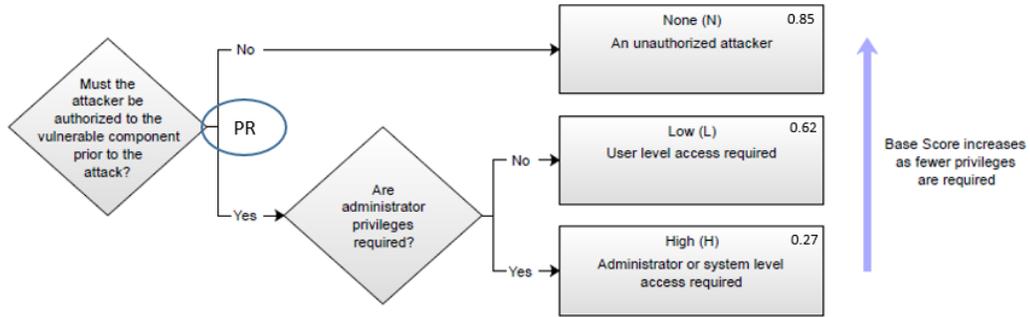
Appendix 3

Attack complexity vector



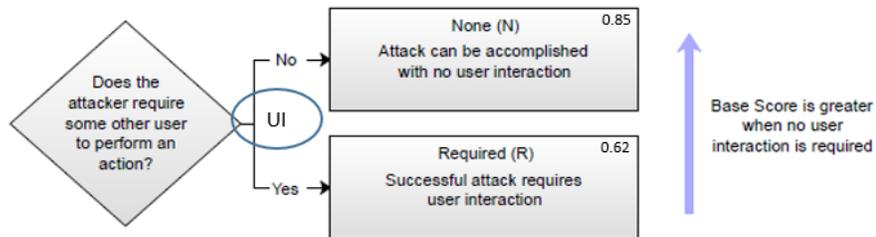
### Attacker privileges vector

Appendix 4



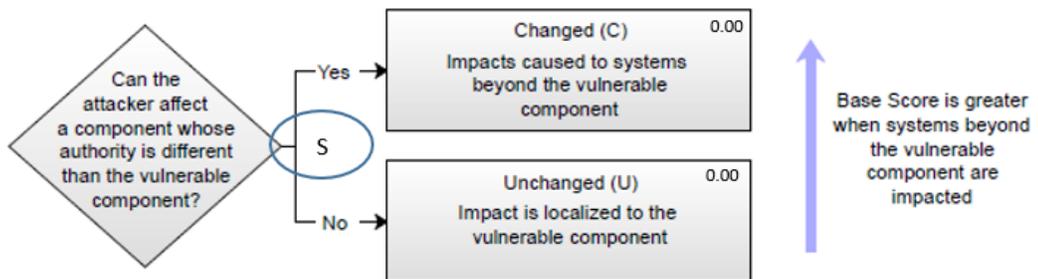
Appendix 5

### Attacker collaboration vector

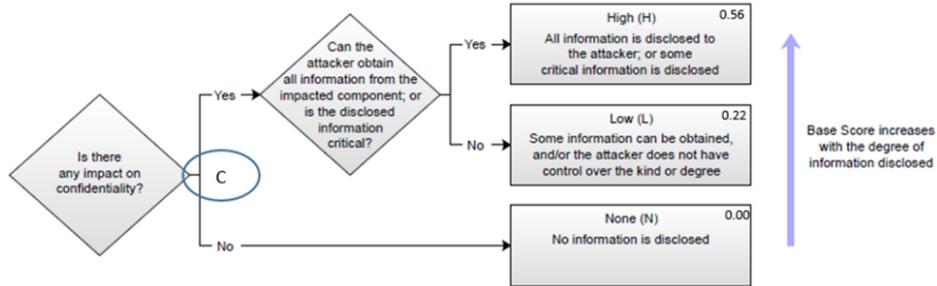


Appendix 6

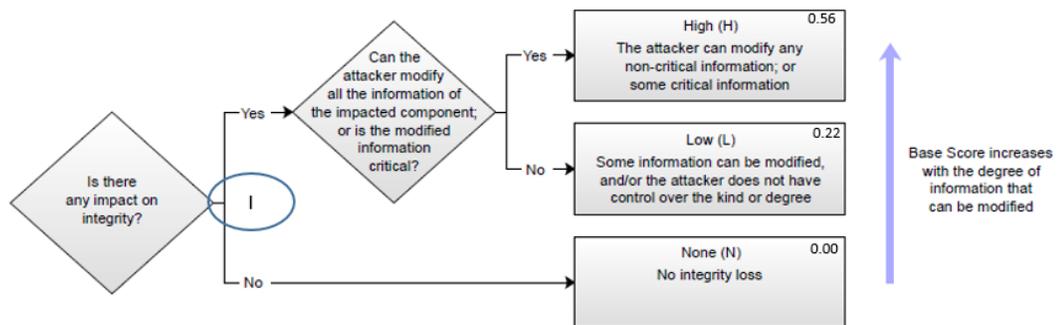
### Attacker scope vector



Confidentiality impact vector



Integrity impact vector



Availability impact vector

