JHSS (Journal of Humanities and Social Studies) *Volume 10, Number 01, Page 863-870*
https://jhss-lppm.unpak.ac.id/index.php/jhss *e-ISSN: 2598-120X; p-ISSN: 2598-117X*

AN EXPLORATION OF INFORMATION SECURITY FACTORS IN DWDM TRANSMISSION SYSTEMS FOR TELECOMMUNICATIONS INFRASTRUCTURE: A CASE STUDY OF PT. XYZ

Afrursah Satrio Bia Pratama [a*)], Setiadi Yazid [a)]

[a)] *Universitas Indonesia, Depok, Indonesia*

[*)]*Corresponding Author: afrursah.satrio@ui.ac.id*

Article history: received 12 April 2026; revised 26 May 2026; accepted 05 June 2026 *DOI: https://doi.org/10.33751/jhss.v10i01.377*

Abstract. This study aims to explore the factors influencing the information security of the DWDM transmission system at PT. XYZ using a qualitative approach. The research was conducted through semi-structured interviews with experts directly involved in the operation of the DWDM network and analyzed using thematic analysis techniques with the assistance of ATLAS.ti. Technical parameters of optical networks such as OSNR, BER, and optical power were used to understand network conditions; ITU-T standards were used to map the architecture and assets of the DWDM transmission system; and the NIST SP 800-30 methodology was used to interpret the findings in the context of threats, vulnerabilities, and their impact on Confidentiality, Integrity, and Availability (CIA). The research results identified seven main groups of factors affecting the information security of DWDM transmission systems, namely Outside Plant (OSP) Security Issues, Inside Plant (ISP) Security Issues, Monitoring & Detection Limitations, Access Control & Configuration Weaknesses, Documentation, Policy & Governance Gaps, Environmental & Power Risks, and Incident & Preventive Weaknesses. These findings indicate that the information security of DWDM transmission systems is influenced by the interaction between technical and non-technical aspects; thus, this research is expected to provide an academic contribution and serve as a practical reference for PT. XYZ in enhancing the security resilience of its DWDM network.

Keywords: DWDM, ITU-T, NIST SP 800-30, Information Security

I. INTRODUCTION

Current communication technology demands networks with high capacity, low latency, and high reliability to support various digital services such as cloud computing, the Internet of Things (IoT), big data analytics, and 5G/6G networks [1], [2]. Dense Wavelength Division Multiplexing (DWDM) technology is a primary solution used in modern optical transport communication systems due to its ability to transmit multiple data signals simultaneously through a single optical fiber using different wavelengths, thereby increasing transmission efficiency and capacity [1]. With the increasing use of DWDM transmission systems for information delivery over optical infrastructure, threats to the security of DWDM transmission systems have become increasingly significant. These threats directly impact the continuity of information security in DWDM networks and jeopardize the core pillars of information security: Confidentiality, Integrity, and Availability (CIA) [3].

PT. XYZ, as a telecommunications company managing optical backbone infrastructure utilizing DWDM to connect Points of Presence (PoP), data center interconnects, and international gateways, handles data traffic reaching hundreds of terabits per second. With such high data traffic, PT. XYZ has a critical need to ensure the security of its DWDM transmission systems to prevent threats that could cause large-scale service disruptions and result in significant losses for the company. The main problems addressed in this study are: (1) what factors influence the information security of DWDM transmission systems at PT. XYZ, and (2) what recommendations can be proposed to enhance the security of DWDM transmission systems based on these findings.

The objective of this study is to explore the factors affecting the information security of DWDM transmission systems and to produce recommendations that can strengthen PT. XYZ's defense mechanisms against technical and operational threats. This research refers to the ITU-T G.870 standard as a reference for optical network architecture under evaluation, and NIST SP 800-30 as a framework for qualitatively analyzing threats, vulnerabilities, and risks.

The results of this study are expected to contribute academically to the field of information security in DWDM transmission systems and provide a new perspective by not only focusing on technical parameters but also exploring real operational conditions. Additionally, the findings are expected to offer practical benefits for the telecommunications industry, particularly PT. XYZ, in enhancing the resilience of DWDM transmission systems in a measurable and sustainable manner.

Volume 10, Number 01, Page 863-870
e-ISSN: 2598-120X; p-ISSN: 2598-117X

II. RESEARCH METHODS

This study employs a qualitative method to explore the factors influencing the information security of the DWDM transmission system within PT. XYZ's telecommunications infrastructure. The approach aims to gain an in-depth understanding of the DWDM transmission-system architecture, both from the perspective of technical parameters and relevant threat and vulnerability patterns. Through semi-structured interviews and technical-document analysis, the qualitative approach allows the researcher to understand operational practices, infrastructure conditions, the effectiveness of security controls, and the direct experience of DWDM engineers in incident handling. Identification of the architecture and assets is carried out based on ITU-T, while the technical assessment of the optical transmission system is performed by referring to physical parameters such as OSNR, BER, optical power, and OTDR results to identify indications of disturbances in the DWDM transmission system. The mapping of threats and vulnerabilities using the NIST SP 800-30 framework is carried out entirely through these qualitative techniques.

A qualitative approach is used because the information security of the DWDM transmission system is influenced not only by network technical parameters, but also by operational factors, environmental aspects, and infrastructure-management practices that are often not documented in network monitoring systems. In large-scale DWDM optical networks, many physical security incidents arise from third-party activities, technician errors, degradation of passive components, and weaknesses in operational procedures, all of which can only be understood through the experience of practitioners directly involved in network operations. Therefore, interviews with experts are considered an appropriate approach to uncover implicit knowledge and field experience that are not recorded in system data.

Risk assessment in this study is conducted qualitatively following NIST SP 800-30. The likelihood and impact levels are determined through the interpretation of interview findings and thematic analysis results, while considering their effects on the Confidentiality, Integrity, and Availability (CIA) aspects. The assessment results are used to categorize the information-security conditions of the DWDM transmission system into risk levels, which then become the basis for formulating security-enhancement recommendations. The overall research flow is shown in Figure 1.

The approach applied in this research method complements the technical analysis based on optical-network parameters with an operational perspective drawn from network practitioners, thus providing a more comprehensive understanding of the information-security risks in the DWDM transmission system. The comparison of the contributions of each approach in the analysis of DWDM transmission-system information security can be seen in Table 1.

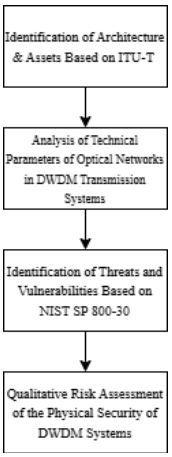

Figure 1. Research Process

Table 1. A Comparison of Information Security Analysis Approaches for DWDM Transmission Systems

Approach	Data Sources	Generated Information
Optical performance monitoring (Quantitative)	OSNR, BER, optical power	Detecting signal degradation or transmission performance anomalies
Network monitoring system (Quantitative)	Device logs, network alarms	Identifying device failures and network operational incidents
Expert interviews (Qualitative)	Operational experience of DWDM engineers	Identifying operational vulnerabilities, procedural weaknesses, and operational security risks not recorded in the monitoring system

A. Identification of Architecture and Assets Based on ITU-T

The initial phase of the research began with identifying the architectural structure of PT. XYZ's DWDM transmission system based on the ITU-T reference model. During this phase, the OTN layers (OTS, OMSC, OTU, OSC, and Node Infrastructure) were mapped, along with physical and logical assets such as fiber spans, amplifiers, OADM/ROADM, optical channels, and supervision systems (OSC). The primary objective of this phase is to understand the critical components that could potentially serve as physical attack vectors in the DWDM transmission system. The mapping results for these critical components are presented in Table 2.

Table 2. ITU-T Mapping of PT. XYZ's DWDM Infrastructure

No	TU-T Identification	Asset	Function
1	OTS	Fiber-Optic Cable	Primary transmission media between DWDM
2	OTS	Konektor/ *Joint Closure*	Connecting optical fibers and protecting connection points
3	OTS	OTB (*Optical Termination Box*) and ODF (*Optical Distribution Frame*)	Fiber optic termination at the DWDM site
4	OTS	*Optical Amplifier* DWDM	DWDM components for manipulating DWDM transmission signals
5	OMSC	*Multiplexer* DWDM	DWDM components for combining service channels
6	OMSC	FOADM / ROADM	DWDM components for configuring channel destination
7	OMSC	Transponder DWDM	DWDM components for converting user signals into DWDM signals
8	OCH	*Cross Connect* DWDM	DWDM logic components that carry end-to-end data payloads
9	OTS	OSC DWDM	Operational management channels for DWDM devices
10	Node Infrastructure	DWDM Equipment Racks and Rooms	External support facilities for DWDM

B. Analysis of Technical Parameters of Optical Networks in DWDM Transmission Systems

At this stage, the information security of PT. XYZ's DWDM transmission system is analyzed using optical-network technical parameters. The analysis is carried out by understanding how the physical characteristics and signal-performance of the optical link can reflect the security condition of the network. Each physical parameter such as OSNR, BER, and optical power in the DWDM system behaves in a specific way under normal operating conditions and will show anomalous patterns when disturbances or interventions occur. The results of this analysis form the basis for exploring threat and vulnerability factors in the subsequent stage, without performing numerical calculations or quantitative assessments.

C. Identification of Threats and Vulnerabilities Based on NIST SP 800-30

Threat and vulnerability identification are conducted to determine threat sources, threat events, and system weaknesses that can be exploited. This process follows the NIST SP 800-30 framework, which emphasizes a systematic approach to identifying assets, threats, vulnerabilities, and operational conditions that can increase the likelihood of incidents [11]. In DWDM networks, threat evaluation on the optical link is particularly important because the transmission medium fiber optic is sensitive to physical interference and tapping.

Based on expert information from PT. XYZ regarding the physical parameters of optical fiber and NIST standards, threat sources are categorized into two groups: incidental and intentional. The identification of threat sources is presented in Table 3.

Table 3. Identification of Threat Sources

No.	Identification	Category	Threat Source	Example
1	Source of Threat	Incidental	Environmental conditions	Vibration, high temperatures, humidity, animal interference
2			Degradation of passive components	Dirty connectors, aging splices, loose closures
3			Human error	Technician errors during patching, misconfiguration
4		Purpose	Optical tapping	Installation of Optical Splitters
5			*Unauthorized splicing*	Illegal splices on fiber optic lines
6			Device sabotage	Tampering with amplifiers, ROADMs, and OSCs
7			Direct physical interference	Mechanical stress, bending, and vandalism resulting in cuts

After threat sources have been identified, the threat events in the DWDM network describe the concrete forms of actions or disturbances that may occur on the network's physical assets. These events are identified based on optical-anomaly patterns observed in parameters such as OSNR, BER, power, and OTDR traces, supported by relevant optical-physical security studies. The identified threat events, categorized according to the CIA triad, are presented in Table 4.

Table 4. Identification of Threat Events

No.	Threat Events	Technical Impact	CIA Impact
1	*Fiber Flapping*	OSNR down, *power anomaly*, OTDR *reflection*	C
2	Unauthorized Splicing	*Insertion loss* increase, *return loss* high	I, A
3	Amplifier/ROADM Manipulation	*Gain tilt*, spektral bergeser, kanal interferensi	I, A
4	Fiber Bending / Mechanical Stress	*Localized attenuation*, BER up	A
5	Connector Degradation	Return loss high, power drop	A
6	OSC Manipulation	Lost *management/ control plane*	A

The final identification step is the vulnerability, which refers to weaknesses in the DWDM infrastructure, procedures, or physical characteristics of the network that can be exploited by threats. Vulnerability identification is performed by referring to the technical baseline from ITU-T, the technical parameters of optical networks, and the risk-assessment guidelines of NIST SP 800-30. The identified vulnerabilities can be seen in Table 5.

Table 5. Vulnerability Identification

No.	Vulnerability	Description	Impact
1	Insecure physical access	*Joints are not locked, manholes are easy to open, OTB racks/devices are not locked*	Sabotage
2	Lack of power line monitoring	No OSNR/BER/power baseline	Undetected faults
3	Limitations of G.652 & G.655	Mixed use of G.652 and G.655 cables	OSNR Drop
4	DWDM Monitoring Vulnerability	OMS/OSC Issues	DWDM Not Monitored
5	Lack of technician access logging	No access audit for OTB/DWDM	*Unauthorized Access*
6	Degraded passive components	Dirty connectors, damaged patch cores, damaged splices	Increased BER

D. Research Participants

Participants were selected using purposive sampling. Purposive sampling is a sampling technique in which the researcher deliberately chooses participants based on specific criteria and characteristics [12]. The sampling criteria are based on respondents who have strong understanding, full responsibility, and direct involvement in the DWDM operational activities of PT. XYZ.

Six expert respondents were selected for the qualitative data collection; these individuals have full responsibility and the authority to implement information-security-method improvements at PT. XYZ. The qualitative approach based on expert interviews was adopted to emphasize depth of information rather than statistical generalization, given that the number of participants in this study is relatively small. In qualitative research, sample size is usually determined by the concept of data saturation that is, the point at which additional interviews no longer yield new themes. Methodological studies indicate that most research themes often emerge within a small number of interviews, typically around the first six interviews [13].

The interviews were conducted online using Microsoft Teams, following a semi-structured approach considered appropriate for descriptive qualitative research aimed at obtaining direct information consistent with existing facts [14]. The interviews took place in November 2025 and involved DWDM engineer specialists and regional network specialists. The complete respondent data can be seen in Table 6.

Table 6. Qualitative Participant Data

No.	Participant ID	Job Title	Years of Experience	Gender
1	R1	DWDM *Engineer Specialist*	8	L
2	R2	DWDM *Engineer Specialist*	9	L
3	R3	DWDM *Engineer Specialist*	5	L
4	R4	DWDM *Engineer Specialist*	8	P
5	R5	DWDM *Engineer Specialist*	8	L
6	R6	Region Network Specialist	9	L

E. Research Instruments

The interview questions in this study were formulated using a semi-structured approach, developed based on previous studies to identify the factors that influence the information-security of the DWDM transmission system [15]. The interview questions can be seen in Table 7.

Table 7. Research Questions

No.	Factor	Question
1	Architecture and Asset Identification (ITU-T G.870)	What is an overview of the DWDM architecture you are working on (OTS–OMS–OCh)?
2		What physical assets do you think are most critical in DWDM services?
3		What is the condition of fiber optics and passive devices such as *joint closure* and ODF/OTB?
4		How good is the documentation and *labeling* of DWDM devices/paths in the field?
5	*Monitoring & Optical Parameters*	Are OSNR, *power*, and BER monitored regularly?
6		Is OTDR used periodically to detect *bending/splicing*?
7		How often do you encounter power anomalies or *loss spikes*?
8		Is the *monitoring system* capable of detecting the symptoms *of fiber tapping*?
9	Physical Threats (Threat Events)	Have there ever been indications of *illegal fiber tapping* or *splicing*?
10		How often does *there be bending* or physical stress on the fibers in your area?
11		Has there ever been a significant *amplifier* or ROADM outage?
12		What do you think are the most common physical threats in the DWDM network?
13	Infrastructure Vulnerabilities (NIST – Vulnerabilities)	What is the level of physical security *of joint closures*, *manholes*, and device spaces?
14		Are DWDM access controls and maintenance SOPs running consistently?
15		What vulnerabilities most often cause physical impairment of DWDM?
16		How good is the documentation of technician activities (*splicing*, OTDR, repair)?
17	Incidents & Field Experiences	What are the most frequent physical incidents in the past year?
18		How long does it usually take to detect the cause of physical disorders?
19	Control Evaluation & Recommendations	What information security controls for DWDM are most effective today?
20		In your opinion, what are the most important steps to improve the information security of PT. XYZ?

F. Data Analysis

This study uses thematic analysis as the analytical method. According to Gareth Terry and Nikki Hayfield in the book *Essentials of Thematic Analysis*, thematic analysis is a flexible method that allows researchers to identify themes based on patterns emerging from qualitative data [16]. The analysis in this study is presented using the software Atlas.ti version 24. The first step is to create codes derived from key issues identified in the interview results. Then, patterns and themes are identified within the collected data. After the analysis results are obtained, the themes are verified with experts to ensure their appropriateness and alignment with the findings [17].

III. RESULT AND DISCUSSION

Based on the interview results, the research findings were coded and then grouped into several main code groups representing information security factors in DWDM transmission systems. This grouping was performed through an axial coding process, taking into account contextual similarities, asset types, and their impact on network security. The research results are presented in Table 8.

Table 8. Research Findings

No.	Dimensions	Construction	CIA
1	OSP *Security Issues*	*Distance and Hop Problem*	A
2		*Optical Termination Issues*	
3		*OSP Bending Issue*	
4		*OSP Cable Merging*	
5		*OSP Deployment Issue*	
6		*SPOF Link*	
7		*Third Party Issues*	
8		*Vandalism*	
9	ISP *Security Issues*	*Animal Disturbance*	A
10		*Degrade DWDM Module*	
11		*Degrade Optical Patchcore*	
12		*ISP Optical Termination Issues:*	
13		*Obsolete OTB*	
14		*Spare Part Issues*	
15	*Monitoring & Detection Limitations*	*Invalid Data*	I, A
16		*Lack of Early Warning System*	
17		*Long Detection Problem Time*	
18		*Manual Performance Monitoring*	
19	*Access Control & Configuration Weaknesses*	*Access Room Management*	C,I
20		*Unauthorized Access DWDM Configuration*	
21		*Unsecure DWDM Rack*	
22	*Documentation, Policy & Governance Gaps*	*Lack of Document Standardization*	C, I
23		*Information Labeling Problem*	
24		*Policy Updates*	
25	*Environmental & Power Risks*	*Cooling System Issues*	A
26		*Electrical Issues*	
27	*Incident & Preventive Weaknesses*	*Critical Issues*	I, A
28		*Preventive Action Issues*	

A. OSP Security Issues

OSP (Outside Plant) security factors include assets and activities outside the building, such as fiber spans, joint closures, duct routes, and the environmental conditions around the transmission path. The interview results indicate that OSP disturbances consist of the number and distance of hops per device, termination points of the DWDM cable, third-party interference and vandalism, as well as the condition of the optical cable related to the construction method, quality, and how it is combined with other optical cables.

Conceptually, optical fiber is highly sensitive to mechanical stress and physical interference, which can cause signal degradation detected through changes in optical-channel characteristics [5]. Within the NIST SP 800-30 framework, these conditions are mapped as threat events influenced by environmental and external threat sources and reinforced by vulnerabilities in the physical security of the fiber route [11]. The findings regarding the OSP aspect show that physical disturbances to the optical transmission infrastructure can significantly impact the continuity of DWDM network services. This is consistent with risk-assessment studies on critical infrastructure, which emphasize that damage or disruption of key physical components greatly increases service risk and must therefore be prioritized in risk management [18]. The following are several illustrative respondent quotes related to OSP security issues:

"The most common cause, both in my region and in other regions, is still third-party activities." (R6)

"For vandalism, it happens quite frequently, probably because many cables emerge at the surface, so those surface-level cables are very vulnerable to being cut because people assume they are copper cables." (R3)

"Most of the time this actually comes from the initial project, where the specifications were insufficient; later on, disturbances like the ones mentioned earlier occur, for example, when fiber-optic cable gets crushed or run over, precisely because the original design was not up to standard." (R5)

B. ISP Security Issues

ISP (Inside Plant) factors relate to the management of DWDM network devices and components inside the node, including OTB/ODF, patch cores, amplifiers, ROADM, and transponders. The interview results show that degradation of passive and active components, limited spare parts, obsolete OTB units, and intrusions by wild animals all contribute to operational instability of the network. In the optical-network architecture, ISP components are critical assets in the OTS, OMS, and OCh layers [4], where physical degradation can lead to power fluctuations and increased BER [5]. According to NIST SP 800-30, these conditions are classified as asset vulnerabilities that heighten the risk of service disruption [11]. The following are several illustrative respondent quotes regarding ISP security issues:

"Usually, if it's inside the room, it's mostly the patch core…" (R5)

"Modules fail mostly because of age; most of the failures are due to age. We have many modules that are quite old and they are the ones that fail." (R2)

"So there are rodents getting in, and this has actually caused outages at several locations more than once." (R1)

C. Monitoring & Detection Limitations

Limited monitoring and early-stage detection constitute a significant factor in the information security of the DWDM transmission system. Monitoring that remains largely manual and lacks effective early-warning mechanisms prolongs the time needed to detect disturbances and amplifies the impact of incidents. In the NIST SP 800-30 framework, these monitoring limitations are classified as control vulnerabilities that increase both the likelihood and the impact of security incidents [11]. These findings are consistent with earlier research indicating that the absence of effective monitoring systems for optical networks raises the risk of service outages and expands the operational impact on backbone networks [19]. The following are several illustrative respondent quotes regarding monitoring and detection limitations:

"Yes, under normal operations it is like that we wait for complaints; we only begin checking after a disturbance or service issue appears." (R1)

"As it is now, DWDM itself does not yet have a dedicated monitoring system, so we only find out when there is flapping or poor attenuation from the service layer." (R3)

"There is none yet, so we are only triggered when, for example, there is a reported fault." (R8)

D. Access Control & Configuration Weaknesses

The weakness of access control and system DWDM-configuration factors covers the security of equipment rooms, DWDM racks, and the restriction of access to devices and network configurations. The interview results show that access control to the DWDM system that is not yet optimal increases the potential for unauthorized access and operational errors. In the NIST SP 800-30 framework, access-control weaknesses are treated as vulnerabilities that can directly affect the Confidentiality and Integrity of information and increase the risk of operational disturbances [11]. The following are several illustrative respondent quotes regarding access control and configuration weaknesses:

"There are still many loopholes; anyone can still access it without being noticed, and even administrator-level access can be obtained quite easily." (R1)

"In the WDM now, there is no access control, so everyone can perform configuration changes, like adjusting something or modifying service status." (R5)

"There are several locations where there actually is a door, but we had to remove it because it was impossible to keep opening and closing the door; the access then became difficult." (R2)

E. Documentation, Policy & Governance Gaps

Governance and documentation aspects emerge as non-technical factors that influence the information security of the DWDM transmission system. The interview findings indicate a lack of standardized technical documentation, issues with information labeling, and outdated or loosely enforced company rules. In the NIST SP 800-30 framework, procedural and organizational weaknesses are classified as non-technical vulnerabilities that can amplify system risk by hindering incident response and change-control processes [11]. These findings are also consistent with the resilience approach for critical communication infrastructure, which stresses the importance of managing threats comprehensively not only in the technical domain, but also in organizational readiness, operational procedures, and incident-response capability [20]. The following are several illustrative respondent quotes regarding documentation, policy, and governance gaps:

"Documentation itself has actually been a long-standing issue that frequently becomes a problem for various parties, throughout the time I have been at PT. XYZ." (R5)

"For the physical labels themselves, because of changeover or frequent link changes, the application has been somewhat inconsistent; physical labels are perhaps applied less rigorously." (R1)

"There is a regulation from the rectorate or PR level that we still use as a reference. However, in terms of content it is already outdated because it has not been updated since 2016, at least for the transport-layer equipment. Therefore, in my view, it is no longer relevant today." (R5)

F. Environmental & Power Risks

The environmental and power factor encompasses the electrical conditions and cooling systems at DWDM node sites, indicating that power disturbances and suboptimal cooling can accelerate equipment degradation and trigger service outages. In the NIST SP 800-30 approach, environmental conditions are treated as factors that can increase the impact of incidents, especially on network availability [11], and are recognized as an essential prerequisite for DWDM system reliability [21]. In the context of critical infrastructure, the network's dependence on stable power and a controlled operating environment constitutes a major risk factor that can cause system failure and reduce service resilience, as discussed in studies on the security of industrial networks and control systems [21]. The following are several illustrative respondent quotes regarding environmental and power risks:

"Our cooling system has many problems. It tends to spread; eventually the modules themselves also start to malfunction." (R2)

"From a critical standpoint, it is certainly the power supply or the DWDM feed itself. When one DWDM goes down, many more services will be affected. That is why we have a power-supply availability system whose KPIs we also maintain." (R1)

G. Incident & Preventive Weaknesses

The factor Incident & Preventive Weaknesses reflects limitations in early detection, incident response, and the implementation of preventive measures for the information security of the DWDM transmission system. The interview results show delayed response actions and a lack of systematic preventive activities, as well as incomplete understanding of problems across the organization. In the NIST SP 800-30 framework, these weaknesses are classified as operational vulnerabilities that increase both the likelihood and the impact of incidents, especially with respect to Availability and Integrity [11]. This condition aligns with studies on network-infrastructure security that emphasize how limited prevention mechanisms and insufficient readiness to respond to targeted attacks can increase the risk of recurring

outages and weaken the resilience of critical-infrastructure services [22]. The following are several illustrative respondent quotes regarding incident and preventive weaknesses:

"Why critical? Because this amplifier itself carries multiple services underneath it. So if just one subsystem in this amplifier is disturbed, many services can be affected." (R1)

"In my opinion, preventive activities actually play a bigger role. However, this is still not covered properly, either in their standard procedures or in their contracts; it is still not standardized." (R5)

IV. CONCLUSIONS

This study successfully explores the factors influencing information-security in the DWDM transmission system at PT. XYZ's telecommunications infrastructure using a qualitative approach. Based on expert interviews and thematic analysis using ATLAS.ti, the research identifies seven main groups of factors that affect the information security of the DWDM transmission system: Outside Plant (OSP) Security Issues, Inside Plant (ISP) Security Issues, Monitoring & Detection Limitations, Access Control & Configuration Weaknesses, Documentation, Policy & Governance Gaps, Environmental & Power Risks, and Incident & Preventive Weaknesses. The results show that technical and non-technical factors interact closely in determining the security level of the DWDM transmission system. From the perspective of optical-fiber physical parameters, physical disturbances and component degradation can be detected through changes in optical parameters such as OSNR, BER, optical power, and OTDR results; however, the effectiveness of detection strongly depends on the readiness of monitoring systems and operational response. The mapping based on ITU-T standards helps identify critical assets in the OTS, OMS, and OCh layers, while the NIST SP 800-30 framework is used to interpret these findings in terms of threats, vulnerabilities, and their impact on Confidentiality, Integrity, and Availability (CIA). Overall, this study confirms that the information security of the DWDM transmission system is not determined solely by optical transmission technology, but also by the quality of operational governance, access control, monitoring readiness, and the organization's capability in incident handling and preventive measures.

REFERENCES

[1] G. N. A. A. Saputra and A. Firdausi, "Analisis Performa Sistem Dense Wavelength Division Multiplexing dengan Hybrid Optical Amplifier dan Single Amplifier Menggunakan Optisystem," InComTech J. Telekomun. Dan Komput., vol. 12, no. 2, p. 84, Aug. 2022, doi: 10.22441/incomtech.v12i2.12458.

[2] F. Guo, F. R. Yu, H. Zhang, X. Li, H. Ji, and V. C. M. Leung, "Enabling Massive IoT Toward 6G: A Comprehensive Survey," IEEE Internet Things J., vol. 8, no. 15, pp. 11891–11915, Aug. 2021, doi: 10.1109/JIOT.2021.3063686.

[3] "An Introduction to Information Security," National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-12 Revision 1, 2017. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/12/r1/final

[4] "Architecture of Optical Transport Networks (OTN)," International Telecommunication Union (ITU-T), Geneva, ITU-T Recommendation G.872. [Online]. Available: https://www.itu.int/rec/T-REC-G.872/en

[5] I. B. Djordjevic, S. Zhang, and T. Wang, "Physical-layer security in optical communications enabled by bessel modes," in 2017 IEEE Photonics Conference (IPC), Orlando, FL: IEEE, Oct. 2017, pp. 719–720. doi: 10.1109/IPCon.2017.8116295.

[6] W. Qu et al., "Application of Optical Fiber Sensing Technology and Coating Technology in Blood Component Detection and Monitoring," Coatings, vol. 14, no. 2, p. 173, Jan. 2024, doi: 10.3390/coatings14020173.

[7] "Optical Transport Network Physical Layer Interfaces," International Telecommunication Union (ITU-T), Geneva. [Online]. Available: https://www.itu.int/rec/T-REC-G.959.1/en

[8] "Characteristics of a Single-Mode Optical Fibre and Cable," International Telecommunication Union (ITU-T), ITU-T Recommendation G.652, 2016. [Online]. Available: https://www.itu.int/rec/T-REC-G.652/en

[9] "Characteristics of a Non-Zero Dispersion-Shifted Fibre," International Telecommunication Union (ITU-T), ITU-T Recommendation G.655, 2020. [Online]. Available: https://www.itu.int/rec/T-REC-G.655/en

[10] "Spectral Grids for WDM Applications: DWDM Frequency Grid," International Telecommunication Union (ITU-T), ITU-T Recommendation G.694.1, 2012. [Online]. Available: https://www.itu.int/rec/T-REC-G.694.1/en

[11] "Guide for Conducting Risk Assessments," National Institute of Standards and Technology (NIST), Gaithersburg, MD, NIST Special Publication 800–30 Revision 1, 2012. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

[12] A. Fauzy, Metode Sampling, Edisi 3. in 3. Tangerang Selatan.

[13] G. Guest, A. Bunce, and L. Johnson, "How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability," Field Methods, vol. 18, no. 1, pp. 59–82, Feb. 2006, doi: 10.1177/1525822X05279903.

[14] N. Azizah, "Metode Penelitian," p. 17, 2017.

[15] M. Schöberl, S. Tuyisabe, C. Hollauer, and J. Fottner, "Managing Projects More Successful: Evaluation of a Concept for Implementing Critical Success Factors in Practice," in 2022 IEEE 28th International Conference on Engineering, Technology and Innovation (ICE/ITMC) & 31st International Association For Management of Technology (IAMOT) Joint Conference, 2022, pp. 1–6. doi: 10.1109/ICE/ITMC-IAMOT55089.2022.10033150.

[16] S. J. Taylor, R. Bogdan, and M. L. DeVault, Introduction to qualitative research methods: a guidebook and resource,

Volume 10, Number 01, Page 863-870
e-ISSN: 2598-120X; p-ISSN: 2598-117X

Fourth edition. Hoboken, N.J.: John Wiley & Sons, Inc., 2016.
[17] G. Terry and N. Hayfield, Essentials of thematic analysis. Washington: American Psychological Association, 2021. doi: 10.1037/0000238-000.
[18] S. Tweneboah-Koduah and W. J. Buchanan, "Security Risk Assessment of Critical Infrastructure Systems: A Comparative Study," Comput. J., vol. 61, no. 9, pp. 1389–1406, 2018, doi: 10.1093/comjnl/bxy040.
[19] International Journal of Research Publication and Reviews, "Security and Reliability Issues in Optical Fiber Communication Networks," Int. J. Res. Publ. Rev. IJRPR, vol. 5, no. 12, pp. 1–6, 2024.
[20] K. Nova, "Security and Resilience in Sustainable Smart Cities through Cyber Threat Intelligence," Int. J. Inf. Cybersecurity, vol. 6, no. 1, pp. 21–42, 2022.
[21] E. D. Knapp, Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Amsterdam, Netherlands: Elsevier, 2024.
[22] A. Kumar and G. Somani, "Security Infrastructure for Cyber Attack Targeted Networks and Services," in Recent Advancements in ICT Infrastructure and Applications, M. Chaturvedi, P. Patel, and R. Yadav, Eds., in Studies in Infrastructure and Control. , Singapore: Springer Nature Singapore, 2022, pp. 209–229. doi: 10.1007/978-981-19-2374-6_9.