UDC 004.056:004.7:621.391.63. **doi: 10.32620/reks.2026.2.14**

Serhii ZYBIN[1], Dmytro PROKOPOVYCH-TKACHENKO[2], Rostyslav PALAHUSYNETS[3], Yuliia KHOKHLACHOVA[4], Anton HERASYMENKO[1]

[1] ***State University of Information and Communication Technologies, Kyiv, Ukraine***
[2] ***University of Customs and Finance, Dnipro, Ukraine***
[3] ***Permanent Mission of Ukraine to the International Organizations in Vienna, Austria***
[4] ***State University of Trade and Economics, Kyiv, Ukraine***

AN APPROACH TO ENHANCING HYBRID CYBERATTACK NETWORK SURVIVABILITY DURING BLACKOUTS

*The **subject of the study** is the development process of SOHO (Small Office / Home Office) electronic communications networks based on a compact GPON (Gigabit-capable Passive Optical Network) mini OLT (Optical Line Terminal) with one PON (Passive Optical Network) port for up to 32 ONU/ONT (Optical Network Unit/Optical Network Terminal) subscriber terminals. **This study aims** to develop and validate an enhanced network survivability approach under hybrid cyberattacks during blackouts. The research **tasks** are as follows: a formal model of SOHO access survivability should be developed that considers the UPS energy budget and the structure of active nodes; a hybrid risk model in which energy failures are combined with cyber compromise should be formalized; the monitoring methodology IDS+SIEM (Intrusion Detection System + Security Information and Event Management) with machine learning should be developed; a comparative analysis of Ethernet and GPON architectures should be performed; practical recommendations for the implementation, diagnostics and streamlining of management should be formulated in accordance with the principles of Zero Trust and the requirements of information security management, taking into account the human factor and the ease of use of controls in SOHO. The following **results** were obtained. The survivability model was developed that combines the power backup circuit (UPS autonomy assessment), the availability of the active circuit, and a probabilistic model of the risk of compromising control components, including firmware attacks related to SNMP (Simple Network Management Protocol) and SSL/TLS (Secure Sockets Layer/Transport Layer Security) vulnerabilities in embedded software. A monitoring methodology that integrates IDS and SIEM with deep-learning-based analytical model classes was developed and represented by AE+LSTM-type (Autoencoder + Long Short-Term Memory) telemetry analysis and CNN+LSTM-type (Convolutional Neural Network + LSTM) firmware-oriented analysis. Comparative modeling of Ethernet Everywhere and GPON architectures with passive branching was performed for 5–20–32 connection scaling scenarios. Numerical examples of calculations, comparative tables of metrics, and the practical algorithm for diagnosing typical installation errors (APC/UPC, IN/OUT splitter, incompatibility of standards) were provided. The results were interpreted using Zero Trust principles for small networks and the prospects of multimodal AI for correlating SIEM events with firmware artifacts and physical optical channel telemetry were identified. Practical recommendations regarding segmentation, update policies, and privilege minimization for access control in the SOHO segment were offered. **Conclusions**. This study determines that enhancing network survivability is an important and urgent task. The scientific novelty of the results obtained is as follows: the integrated monitoring methodology with machine learning that ensure the transition from component composition and operational assumptions to numerical metrics of survivability, availability, and detection was developed; the formal survivability model was developed considering the UPS energy budget and the structure of active nodes was developed; the risk of hybrid events in which energy failures are combined with cyber compromise was formalized. **Areas for further research:** failure localization methodology; methodologies related to Zero Trust; multimodal AI analysis; decision support under conditions of limited SOHO resources.*

Keywords: *cybersecurity; SOHO; blackout; GPON; mini OLT; IDS, SIEM, Zero Trust.*

1. Introduction

1.1. Motivation

The SOHO environment includes small offices, coworking spaces, private homes with multiple tenants, workshops, small residential complexes, and mixed facilities where business processes, household infrastructure, and security services are simultaneously present. Historically, simple Ethernet and Wi-Fi-based solutions have been typical for such communication networks. However, two interrelated criteria become key in modern operating conditions: survivability during blackouts and cyber resilience to hybrid attacks. The engineering formulation of this problem is appropriate through the prism of the OSI (Open Systems Interconnection) reference

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

model, which allows the formalization of the relationships between failures, security events, and levels of network interaction, as well as the correct determination of the control points and boundaries of responsibility of monitoring and protection tools [1,2].

First, during a blackout, SOHO network degradation often occurs due to cascading failure of small dependencies: an intermediate switch without backup power, a PoE injector outside of a UPS, and an access point powered by a node that is out of power [3]. Consequently, the failure becomes systemic, and even a minor incident at the physical or channel level quickly turns into an application-level service outage. In this sense, SOHO is a network with disproportionately high sensitivity to structural weak links, requiring architectural solutions with fewer active elements in the access zone and better control centralization [4,5].

Second, SOHO is increasingly becoming a target of hybrid cyberattacks that combine both technical and organizational vectors, such as weak credentials, excessive privileges, uncontrolled configuration changes, a lack of asset inventory, simplified logging, and inconsistent access policies [6,7]. Threat modeling approaches combine descriptions of assets, attack vectors, and possible consequences to structure threats and provide a basis for a reasoned selection of protective controls [8]. Furthermore, these controls should align with process risk management, including methods for assessing probabilities and impacts and developing risk treatment plans, as well as with the generally accepted requirements of an information security management system, where inventory, access policies, incident management, and change control are critical [1,7]. In addition, real-world adversary campaigns against operational environments illustrate how combined technical and organizational requirements enable complex disruption scenarios [9].

1.2. State of the art

Existing studies on the survivability of optical networks mainly focus on protection and restoration mechanisms, resilient routing, spectrum allocation, fragmentation management, and resource optimization in large-scale optical or elastic optical networks. These studies provide a strong theoretical basis for understanding communication infrastructure survivability [3]. However, they usually do not consider blackout conditions in small SOHO networks as a permanent operational constraint. In particular, the problem of reducing the number of active access-zone dependencies under UPS limitations remains insufficiently addressed.

Cybersecurity-oriented studies, in turn, actively investigate Zero Trust architecture, IDS/SIEM integration, ML-based intrusion detection, and anomaly detection in software-defined or enterprise-scale environments [7]. However, these approaches are often designed for infrastructures with relatively stable power supply, sufficient computational resources, mature logging procedures, and specialized security teams [6, 8]. Their direct transfer to SOHO during blackouts is limited by small data volumes, heterogeneous devices, simplified administration, weak inventory practices, and constrained energy resources.

Firmware-oriented threat detection and Byte2Image-based malware representation are other relevant research directions [10]. These methods are promising for detecting structural firmware changes and hidden embedded device compromises. Nevertheless, in the SOHO context, firmware analysis is rarely integrated with physical access survivability, UPS autonomy assessment, optical-channel telemetry, and SIEM-level correlation. Consequently, the relationship between communication survivability and cyber-monitoring capability under blackout conditions remains insufficiently formalized.

Firmware attacks occupy a special place in SOHO hybrid attacks because they can provide long-term persistence and resilience against reboots. In a practical context, two typical control compromise channels are critical. In a practical context, two typical channels of control compromise are critical. The first channel is related to SSL/TLS. The use of outdated versions, incorrect certificate validation, weak cryptographic parameters, or the allowance of downgrade scenarios increases the risk of interception or session substitution [10]. The second channel is related to SNMP, which is often used in SOHO environments with simplified access policies and typical community strings, creating conditions for unauthorized modification of device parameters and for indirect firmware compromise [1]. General principles of security control in complex cyber–physical networks further emphasize that in small environments, management-plane weaknesses and simplified configurations often dominate "pure" performance or topology considerations [1].

In response to these threat dynamics, the Zero Trust model is considered a basic principle for building access and control. This model includes the following: microsegmentation, least privilege, continuous verification of requests and states, and constant distrust of internal segments as potentially compromised [7,11]. For SOHO, this means the need for managed access segregation (management, subscribers, IoT/security, guest networks), mandatory event logging, and the ability to correlate incidents in real time, including through IDS and SIEM connections [2,7].

Simultaneously, practice shows that exclusively rule-based monitoring (only signatures and correlation rules) in SOHO faces two limitations. The first limitation is limited training and testing assumptions. In security, machine learning often scales poorly to real-world networks without proper validation, dataset representativeness, drift control, and model updating procedures [2,7].

The second limitation is the high variability of traffic and events even in small environments, which requires a combination of statistical approaches, features and models, as well as a clear methodology for data collection and preparation [2,12]. Additionally, in modern networks with elements of software-defined approaches and centralized management (including SDN), control zone risks and policy errors become as critical as classic data zone risks, while DDoS-oriented and flow-feature ML pipelines demonstrate both potential and sensitivity to feature selection and operating assumptions [13,14].

A catalyst for SOHO incidents is the human factor. In Zero Trust implementation practice, organizational constraints, operational "shortcuts," and usability/complexity barriers repeatedly surface as systemic challenges that directly affect the effectiveness of controls [7,15].

This paper uses an approach that transfers the provider's passive optical architecture to a compact format: a mini OLT of GPON technology with one PON port and a passive optical splitter (typically 1:32) to subscriber ONU/ONT. The splitter's passivity reduces the number of active elements in the access area, reducing the number of nodes that require power backup during blackouts. Concurrently, centralizing control and telemetry allows for greater consistency of access and strengthens the discipline of configuration changes in accordance with Zero Trust [4,5].

An integrated IDS+SIEM approach is justified by adding two machine learning models to enhance hybrid attack detection and reduce incident detection time. The first type is anomaly detection models on event and stream telemetry (including representation learning for "normal behavior" and deviation scoring), aligned with contemporary IDS research directions and practical dataset constraints [2,12]. The second type is deep models capable of handling high-dimensional data and complex dependencies, which are typical of traffic and event sequences in access networks, including SDN environments and distributed/federated settings [11,12]. Methodologically, these approaches are consistent with modern ideas about uncertainty in the security control of complex networks, where it is necessary to explicitly consider the probabilistic nature of events and the incompleteness of observations [1].

The Byte2Image representation is appropriate for analyzing firmware artifacts when byte sequences are converted into images with subsequent application of classification methods and detection of structural changes. The "malware images" approach as a class of ideas has been demonstrated to be viable for the visualization and automatic classification of malware samples [16,17], and the broader trend of hybrid deep learning security models supports the extension of such representations into operational detection pipelines as an additional "modality" of signals to SIEM [1,12]. This is particularly important for firmware attacks, where traditional network telemetry may be insufficient, and the analysis of structural changes in firmware adds an independent modality of evidence for incident correlation [1,16].

Comparison with surveys on optical network survivability and resilient routing/resource allocation [18] allows us to highlight the work's contributions and its applied distinction [19,20]. In the optical networking literature, survivability is often analyzed in terms of protection/restoration, routing/spectrum assignment, fragmentation management, and multi-band constraints, while the "blackout as a SOHO operational constant" and the minimization of active access-zone dependencies are not typically treated as the central engineering variable [21,22]. Simultaneously, the security literature highlights that the practical deployment of ML-based detection and Zero Trust in real networks is constrained by dataset representativeness, operational drift, and organizational factors, especially in small, heterogeneous environments [23,24].

Therefore, the research gap addressed in this paper is the lack of an integrated approach that simultaneously combines the following: SOHO access survivability assessment under blackout conditions; minimization of critical active nodes through GPON passive branching; probabilistic modeling of hybrid cyber-energy events; and IDS+SIEM monitoring enhanced by telemetry-oriented and firmware-oriented machine-learning analytical profiles. This gap determines the proposed approach's scientific and practical relevance. To achieve this goal, it is necessary to develop a model that accounts for two dominant factors simultaneously. Survivability during blackouts and counteraction to hybrid cyberattacks.

1.3. Objectives and tasks

The work developed a formalized, practically applicable approach to increase the survivability of SOHO access networks during blackouts and hybrid cyberattacks. The tasks required to achieve the goal are as follows. It is necessary to reduce the number of critical active nodes, increase availability and simplify redundancy, operationally reduce detection time, increase the explainability of incidents, and reduce recovery time, and reduce the risks of supply chain compromise. The expected final result is an integrated GPON-based survivability model that combines UPS autonomy assessment, active-node availability evaluation, hybrid cyber-risk formalization, and IDS+SIEM monitoring enhanced by machine-learning analytical profiles. This result provides quantitative survivability, availability, and detection metrics, as well as implementation recommendations for SOHO networks built on a mini OLT GPON architecture for up to 32 subscribers [11,12]

This study's main scientific and practical contribution is the integration of three components into a unified survivability-oriented methodology for SOHO access

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

networks operating under blackout conditions. The first component is a GPON-based access architecture with passive optical branching, which reduces the number of critical active dependencies in the access zone. The second component is the concept of a centralized survivability core, which concentrates the minimum set of active nodes that must be protected by UPS and operational controls to preserve connectivity and manageability. The third component is a multimodal monitoring profile that combines IDS/SIEM correlation with telemetry-oriented and firmware-oriented analytical indicators to earlier detection and localization of hybrid cyber incidents. The proposed approach's novelty lies in combining these components into a single assessment and implementation framework for blackout-resilient SOHO networks.

The tasks of this study are structured around one central contribution to avoid fragmentation of the research scope: a formalized approach for assessing and enhancing the survivability of SOHO access networks under blackout-induced constraints and hybrid cyberattacks. Therefore, this study does not aim to solve all problems of Zero Trust implementation, IDS/SIEM deployment, machine-learning-based intrusion detection, or firmware security independently. These elements are considered only as supporting components of the proposed survivability framework, insofar as they influence the availability, hybrid risk, incident detection, and practical manageability of SOHO access networks.

To achieve this goal, the survivability model of SOHO access networks is first formalized by considering the UPS energy budget, the structure of critical active nodes, the availability of the access chain, and cascading-failure behavior. The OSI reference model is used only as an auxiliary framework for classifying fault locations, security events, and monitoring points across network interaction layers.

It then defines a hybrid cyber-energy risk model for SOHO access networks that reflects the interaction between blackout conditions and compromise of management or firmware-related components, while firmware attacks, SNMP weaknesses, and SSL/TLS misconfigurations are considered representative technical scenarios used to parameterize and interpret the general risk model.

This study also compares Ethernet- and GPON-based SOHO access architectures with respect to active-node dependency, backup-power requirements, availability, and resistance to cascading failures. In addition, the proposed survivability framework defines an integrated monitoring profile in which IDS/SIEM and machine-learning analytical components are used only as supporting mechanisms for incident detection and localization. Finally, practical implementation recommendations for SOHO environments, including segmentation, management access control, firmware update discipline, and human-factor-aware operational procedures, are created.

The article is organized as follows: Section 2 describes the research methodology. Section 3 develops the architecture's component composition. Section 4 develops the hybrid risk model, analyzes its elements. Section 5 describes the cases study. Section 6 discusses the results of the research and development, and Section 7 summarizes the study and develops proposals for further research.

2. Methodology

The authors propose an integrated methodology to simultaneously engineer the survivability of SOHO access during blackouts and formalize cyber resilience against hybrid attacks that combine power failures, control compromise, and targeted firmware impacts.

The methodology integrates the GPON access architecture, a centralized survivability core, and multimodal monitoring. In this context, the GPON architecture is used not only as a transmission technology but also to reduce active-node dependency during blackouts. The minimum communication backbone that must remain powered and manageable under degraded energy conditions is defined by the centralized survivability core. Multimodal monitoring extends this architecture by combining network events, device logs, optical-channel telemetry, configuration changes, and firmware-related indicators in the IDS/SIEM profile. Therefore, the proposed methodology combines links physical survivability, operational manageability, and cyber-incident detection within a single framework.

The methodological formulation is based on the principle of "one architecture - two assessment profiles". This means that the energy-reliability profile assesses the autonomy of the UPS and the availability of the critical active circuit, while the cyber profile describes the probabilistic structure of the incident risk, in particular for SNMP and SSL/TLS-dependent attack scenarios on firmware and management interfaces. The IDS+SIEM monitoring profile reduces both profiles to a single operational result, enhanced with machine learning models for telemetry time series and firmware artifacts. As an initial architectural reference, a GPON access scheme based on a mini OLT with one PON port, a passive 1:32 PLC splitter and subscriber ONUs (Fig. 1) was used, which allows us to clearly separate active nodes that require power and form risk points during a power outage from passive elements that do not create a load on the UPS, but can be a source of installation failures.

An integrated survivability criterion is introduced to connect the energy-reliability, cyber-risk, and monitoring profiles into a single assessment procedure. The criterion is defined as a normalized function that combines UPS

autonomy, active-chain availability, hybrid cyber-energy risk, and detection capability:

$$S_{int} = \alpha T_{norm} + \beta A_{chain} + \gamma D_{mon} - \delta P_{hybrid},$$

where S_{int} is the integrated survivability score of the SOHO access system; T_{norm} is the normalized UPS autonomy time for the critical communication core; A_{chain} is the availability of the critical active service chain; D_{mon} is the normalized monitoring and detection capability of the IDS/SIEM profile; P_{hybrid} is the probability of a hybrid event combining blackout-induced degradation and cyber compromise; and α, β, γ, and δ are weighting coefficients selected according to the operational priorities of a specific SOHO deployment.

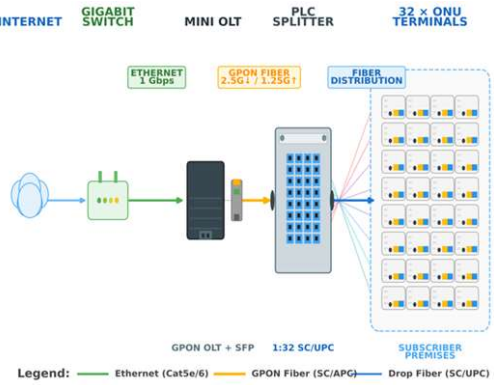

Fig. 1. GPON network architecture:
Gigabit Ethernet → Mini OLT with GPON SFP → 1:32 PLC splitter → 32 ONU terminals subscriber

The normalized UPS autonomy component is determined as follows:

$$T_{norm} = \min\left(\frac{T_{UPS}}{T_{req}}, 1\right),$$

where T_{UPS} is the estimated UPS autonomy time of the critical communication core, and T_{req} is the required autonomy time for the considered blackout scenario. This normalization limits the contribution of the autonomy component to the interval $[0,1]$, so that the integrated score does not distort when the autonomy exceeds the required threshold.

The UPS autonomy time is calculated as follows:

$$T_{UPS} = \frac{C_{bat} U_{bat} \eta}{P_{load}},$$

where C_{bat} is the battery capacity, U_{bat} is the battery voltage, η is the efficiency coefficient of the backup power system, and P_{load} is the total power consumption of the critical communication core's active nodes.

The active-chain availability component is defined as

$$A_{chain} = \prod_{i \in N_{crit}} A_i,$$

where N_{crit} is the set of active nodes whose failure leads to loss of the considered access service, and A_i is the availability of the i-th active node. The availability of an individual active node is calculated as follows:

$$A_i = \frac{MTBF_i}{MTBF_i + MTTR_i},$$

where $MTBF_i$ is the mean time between failures of node i, and $MTTR_i$ is the mean time to recovery of node i.

The hybrid cyber-energy risk component is represented as follows:

$$P_{hybrid} = P(E \cap C) = P(E) P(C \mid E),$$

where E denotes an energy-related degradation event, such as blackout-induced loss of external power, and C denotes a cyber-related compromise event affecting the management plane, firmware, or access-control components. The conditional probability $P(C \mid E)$ reflects the fact that blackout conditions may increase cyber risk by degrading monitoring, requiring emergency

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

configuration changes, simplifying access procedures, or reducing administrative visibility.

The monitoring capability component is normalized as follows:

$$D_{mon} = w_1 F_1 + w_2 AUC + w_3 \left(1 - \frac{MTTD}{MTTD_{max}}\right),$$

where F_1 is the generalized detection quality metric, AUC is the area under the ROC curve, $MTTD$ is the mean time to detection, $MTTD_{max}$ is the maximum acceptable detection time for the considered SOHO scenario, and w_1, w_2, and w_3 are weighting coefficients satisfying $w_1 + w_2 + w_3 = 1$.

This component characterizes the IDS/SIEM profile and analytical detection components' ability to identify and localize incidents within an operationally acceptable time.

Thus, the integrated criterion can be expanded as follows:

$$S_{int} = \alpha \min\left(\frac{C_{bat} U_{bat} \eta}{P_{load} T_{req}}, 1\right) + \beta \prod_{i \in N_{crit}} \frac{MTBF_i}{MTBF_i + MTTR_i} + \gamma \left[w_1 F_1 + w_2 AUC + w_3 \left(1 - \frac{MTTD}{MTTD_{max}}\right)\right] - \delta P(E) P(C \mid E).$$

In this formulation, UPS autonomy reflects how long the critical communication core can remain operational during a blackout. Active-chain availability reflects the probability that the required active nodes will remain operational as a service chain. Hybrid risk reflects the probability that energy degradation and cyber compromise occur jointly or reinforce each other. The monitoring capability reflects the ability of IDS/SIEM and analytical components to reduce the time required to detect and localize an incident. Therefore, the proposed criterion enables comparison of Ethernet and GPON architectures not only by power consumption or availability alone, but also by their combined contribution to blackout- and cyber-resilient operation.

The weighting coefficients are selected according to the operational priorities of a specific SOHO deployment as follows:

$$\alpha + \beta + \gamma + \delta = 1, \ \alpha, \beta, \gamma, \delta \geq 0.$$

For example, in a security-camera or emergency-communication segment, the weights of UPS autonomy and active-chain availability may dominate. In a management-intensive SOHO network with high cyber-risk exposure, the weights of hybrid risk and monitoring capability may be increased. This makes the criterion adaptable while preserving a single structure for architectural scenario comparison.

Next, Ethernet and GPON architectural scenarios are formalized for scales of 5–20–32 connections, assumptions are made regarding the criticality of nodes and their redundancy rules, and equations are introduced for assessing UPS autonomy and integrated service availability under serial criticality of the active circuit.

Simultaneously, a probabilistic model of a hybrid event is defined as a combination of an energy event and a cyber event, given that control procedures often change, access is simplified, and observability degrades in blackout modes, which can increase the risk of compromise. The practical applicability of the methodology is ensured by the fact that the results of probability/availability calculations are directly linked to the monitoring profile. IDS events and network element logs are normalized in SIEM. Two complementary ML components generate additional features and anomaly assessment. AE+LSTM is used to analyze telemetry time series (flows, errors, re-registrations, optical R_x / T_x levels). CNN+LSTM is used to analyze firmware in a Byte2Image representation, focusing on structural changes that can serve as early indicators of a firmware attack, even in the absence of obvious network symptoms. The detection quality and operational efficiency of the methods are evaluated using metrics such as MTTD (Mean Time to Detection), FPR (False Positive Rate), and generalized classification quality indicators, and the output is a formalized set of procedures and models suitable for the comparative analysis of Ethernet and GPON architectures and for forming practical implementation recommendations in Zero Trust logic.

Zero Trust is not a fully implemented standalone security architecture with a complete formal specification of identities, access policies, policy decision points, policy enforcement points, and continuous authorization workflows. Instead, it is used as a set of engineering constraints for SOHO network survivability and manageability. These constraints include separation of management, subscriber, guest, IoT, and security-device segments; least-privilege access to management interfaces; restriction of SNMP and web-management access to trusted administrative sources; inventory of firmware versions and configuration states; mandatory logging of administrative actions; and continuous correlation of device events in SIEM. Therefore, this paper applies Zero Trust as a practical control logic that supports the proposed survivability framework rather than as an independently formalized security model.

The computational profile required for AE+LSTM

and CNN+LSTM inference is treated as logically connected to, but energetically separate from, the communication survival core. Accordingly, the UPS autonomy calculations refer only to the communication backbone elements required to maintain connectivity and centralized manageability during blackouts. The availability of ML-enhanced monitoring relies on a separate protected computation point, such as a low-power edge node or externalized analysis host, and is therefore not included in the access architecture's baseline power budget.

3. GPON network architecture

3.1. Construction GPON access in SOHO

This section defines the GPON access architecture only to the extent necessary for the subsequent survivability, availability, and hybrid-risk modeling. For this reason, the description focuses on the distinction between active and passive elements, critical communication core location, and the impact of passive optical branching on UPS requirements and cascading-failure risk. Detailed reference descriptions of GPON hardware are intentionally minimized because the paper's scientific results focus on the survivability-oriented architecture rather than the technical specifications of individual devices.

The GPON path components are considered only from the standpoint of their influence on the proposed survivability model. In this context, the mini OLT is treated as the central active node of the survivability core, the passive PLC splitter is treated as a branching element that does not increase the UPS load, and the ONU is treated as an endpoint that may require selective backup only for critical subscriber segments. Therefore, the architectural value of the GPON scenario is determined by the reduction of distributed active dependencies in the access zone and the concentration of control, telemetry, and redundancy in a limited number of manageable nodes rather than by the description of individual components.

The component composition of the architecture is defined to ensure the correct modeling of two interconnected circuits: energy survivability during blackouts and cyber resilience to hybrid attacks.

The most important distinction in the proposed architecture is between active elements that require power and passive elements that do not create additional load on the UPS. The mini OLT and backbone router form the minimum survivability core that must remain powered during a blackout to preserve connectivity and manageability. The passive PLC splitter distributes the optical signal without power consumption and therefore does not increase the number of critical energy-dependent nodes. ONUs are treated as active subscriber-side endpoints; only those serving critical functions require selective backup. This structure directly supports the paper's main methodological idea: survivability is improved by reducing distributed active dependencies and concentrating redundancy and monitoring in a centralized core.

Fig. 1 shows the logic of constructing GPON access in SOHO as a serial chain from the external channel to the subscriber segments. Internet traffic is fed to a gigabit switch, which then transmits it to the mini OLT via Ethernet. The Mini OLT acts as a centralized access node. Connection management, service profiles, and the overall network control point are concentrated in this area. The signal then transitions to the optical medium and enters a passive PLC splitter, which physically divides one optical path into multiple subscriber branches. ONUs that convert the optical signal into local Ethernet for end devices are at the ends of these branches. An important practical conclusion from the diagram is that no active elements in the distribution area require power. Because branching is performed passively, critical redundancy points during blackouts are concentrated in the core (switch and mini OLT) rather than distributed throughout the facility. Figs. 2–4 show the key physical elements of the GPON path and their roles in practical operation, detailing the architecture's component structure.

Fig. 2 shows the core access equipment. This is a compact mini OLT/media converter and a GPON SFP transceiver, class B+, which sets the optical channel characteristics in the directions to and from subscribers.

Fig. 2. Mini OLT GPON equipment for SOHO network deployment: (a) compact media converter (P=18W) with LC duplex optical connector for connection to PLC splitter 1:32; (b) GPON SFP OLT transceiver (Class B+, downstream 2.488 Gbps at λ=1490 nm, upstream 1.244 Gbps at λ=1310 nm)

These active components determine the power requirements, form the optical channel, and are the main control points. These elements are considered as basic elements of the network core and the initial parameters for further modeling of survivability and controllability.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Fig. 3. Passive optical PLC splitter 1:32

Fig. 3 shows a passive PLC splitter 1:32 as a branching element that does not require power and provides subscriber branch connection without additional UPS dependencies. Fig. 4 shows the ONU subscriber terminal as an access point that connects the optical line to the user's local network and is a practical point of micro-segmentation and local diagnostics of the connection status. The optical signal is converted into local Ethernet for connecting user equipment. This node concentrates the active part of the access and determines the power backup requirements during a blackout. Together, these components provide centralized access construction and reduce the number of active elements in the distribution area, which simplifies service support during power outages and increases network manageability.

The cassette module has 32 SC/UPC ports (blue connectors) for connecting subscriber ONUs. Since the splitter is a passive element and does not require power, it does not create additional redundancy points during blackouts, but provides physical distribution of the optical signal from the mini OLT to up to 32 subscriber terminals in the access area.

Fig. 4. ONU subscriber terminal (P=5W) for connecting the subscriber to the GPON network.

The device (Fig. 4) has an SC/UPC optical port for connection to a passive PLC splitter and an RJ-45 Ethernet port for connecting the ubscriber's end network. The ONU is an active element in the access area; therefore, its operation depends on the local power. For critical segments in blackout scenarios, providing on-site redundancy is advisable. In the methodological part, the ONU is considered a point of micro-segmentation and access control. In this case, it is most convenient to delimit subscriber domains and record line status parameters, which is important for operational diagnostics and further correlation of events in the monitoring profile. The defined component composition of the architecture and the distinction between active and passive elements provide a methodological basis for further comparison of access solutions. Active nodes form a critical service chain and require power redundancy, whereas passive elements do not load the UPS, but can be a source of installation failures and optical budget degradation. Considering the above components, the next step is to formalize the compared architectures in the form of two generalized scenarios and a set of modeling assumptions. Therefore, the Ethernet and GPON scenarios are further specified, the analysis scales (5–20–32 connections), critical nodes for each scenario and the basic prerequisites necessary for further calculations of survivability, availability and hybrid risk are determined.

3.2. Architectural scenarios and modeling assumptions

This paper considers two generalized access scenarios for a SOHO facility requiring up to 32 wired connections.

1. Ethernet scenario (Ethernet everywhere). The components include a backbone router, one or more access switches, additional intermediate switches/PoE injectors depending on the premises' layout. Active elements are spatially distributed.

2. GPON scenario (mini OLT + passive splitter). The components include a mini OLT as a centralized GPON node, a passive optical splitter (typically 1:8, 1:16, 1:32 as expansion options), ONUs at subscriber points. Optical branching does not require power.

The scenarios with 5, 20, and 32 connections are used as representative scaling points for SOHO access networks rather than as the only possible configurations. The 5-connection scenario corresponds to a minimal SOHO environment with some workstations, network devices, or service endpoints. The 20-connection scenario represents an expanded SOHO or small-office environment with several functional segments, including user workstations, Wi-Fi access, video surveillance, VoIP, IoT, and security devices. The 32-connection scenario corresponds to the upper practical boundary of the considered one-port mini OLT GPON configuration with a 1:32 passive splitter. Therefore, these three values reflect the selected architecture's lower, intermediate, and upper scaling points.

The scenarios are analyzed from the standpoints of

(i) survivability during a blackout, (ii) manageability and diagnostics, and (iii) resilience to hybrid cyberattacks. Formally, the following sets are distinguished:

- V_a are active nodes (requiring power to support the service): router, switches, OLT, ONU, access points (if necessary).
- V_p are passive elements (not requiring power): cable lines, optical splitters, passive crossovers, detachable connections.

Passive elements can fail (e.g., due to installation errors), but they do not create additional load on the UPS backup. This is a fundamental difference of the GPON scenario.

To strengthen the comparison between Ethernet and GPON architectures, additional topological survivability indicators are introduced. The access network is represented as a graph:

$$G = (V, E),$$

where V is the set of network nodes and E is the set of communication links. The set of active nodes that require power is denoted as follows:

$$V_{act} \subset V,$$

and the set of passive elements is denoted as follows:

$$V_{pas} \subset V.$$

The most important subset for survivability analysis is the set of critical active nodes

$$V_{crit} \subseteq V_{act},$$

where the failure of any node $v_i \in V_{crit}$ leads to the loss of the considered access service or the disconnection of a critical subscriber segment.

The first indicator is the active dependency coefficient:

$$K_{AD} = \frac{|V_{crit}|}{|V_{act}|}.$$

This coefficient characterizes the share of active nodes that are critical for service maintaince. A higher value of K_{AD} indicates that the architecture is more sensitive to active powered element failures.

The second indicator is the critical-node density:

$$K_{CN} = \frac{|V_{crit}|}{|V|}.$$

This metric reflects how strongly the entire topology depends on nodes whose failure can interrupt the service. In the Ethernet scenario, this value usually increases as the number of intermediate switches or PoE elements increases. In the GPON scenario, passive optical branching limits the growth of V_{crit}, because the splitter does not require power and is not included in the active service chain.

The third indicator is the coefficient of redundancy load:

$$K_{RL} = \frac{\sum_{v_i \in V_{crit}} P_i}{\sum_{v_j \in V_{act}} P_j},$$

where P_i is the power consumption of the i-th active node. This coefficient shows the share of the total active-node power that must be backed up to preserve the critical communication service. In the GPON scenario, K_{RL} is lower when the survivability core includes only the mini OLT, the backbone router, and selected critical ONUs.

The fourth indicator is the node criticality index:

$$C_i = \frac{N_{lost}(v_i)}{N_{total}},$$

where $N_{lost}(v_i)$ is the number of subscriber endpoints that lose connectivity when node v_i fails, and N_{total} is the total number of subscriber endpoints in the scenario considered. This index allows ranking nodes by their impact on service continuity.

For the entire architecture, the average node criticality can be estimated as follows

$$\overline{C} = \frac{1}{|V_{act}|} \sum_{v_i \in V_{act}} C_i .$$

A lower value of $\overline{C}$ indicates that the topology is less dependent on individual active nodes and has better structural survivability.

Only active nodes are considered candidates for UPS backup, because passive elements do not create additional power demand.

The set of required services is denoted as

$$S = \{s_1, s_2, ..., s_m\}.$$

Each service s_k is associated with a minimum acceptable service level L_k^{min}, which may include connectivity, manageability, monitoring visibility, subscriber availability, or access to a critical segment. For each node $v_i \in V_{act}$, the service-impact function is introduced as follows:

$$I(v_i, s_k) = \begin{cases} 1, \text{if failure } v_i \text{ causes violation of } L_k^{min}, \\ 0, \text{otherwise} \end{cases},$$

A node is classified as critical if it affects at least one required service:

$$v_i \in V_{crit} \Leftrightarrow \sum_{k=1}^{m} I(v_i, s_k) \geq 1.$$

Thus, the set of critical nodes is defined as

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

$$V_{crit} = \left\{ v_i \in V_{act} \mid \sum_{k=1}^{m} I(v_i, s_k) \geq 1 \right\}.$$

For a more detailed prioritization, the criticality score of node v_i is calculated as follows:

$$CS_i = \sum_{k=1}^{m} \omega_k I(v_i, s_k),$$

Where ω_k is the importance weight of service s_k, and

$$\sum_{k=1}^{m} \omega_k = 1, \omega_k \geq 0.$$

A higher value of CS_i means that the node has greater influence on the preservation of critical services and should receive higher priority for UPS backup, monitoring, and access-control protection.

4. Hybrid risk model

4.1. Energy profile redundancy and autonomy

The survivability core is defined as a set of redundant nodes that must be guaranteed to maintain the network backbone, i.e., mini OLT and backbone router, and if necessary, one key ONU (e.g., security/VoIP segment). The redundancy autonomy is estimated using the following formula:

$$T = \frac{C \cdot U \cdot \eta}{P} \quad (1)$$

where T is the battery backup time (h), C is the battery capacity (A·h), U is the voltage (V), η is the efficiency coefficient, P is the total active load power (W). This approach corresponds to the practice of preliminary selection of UPS and battery modules, followed by refinement based on passport characteristics [8].

4.2. Active profile availability model

The availability model should be interpreted as a first-level engineering approximation for comparing SOHO access architectures. It assumes serial criticality of the selected active service chain and does not explicitly model failures, common-cause failures, repair-resource contention, or partial service degradation states. Failures of active nodes may be statistically dependent under real blackout conditions because they can be caused by the same external event, such as a prolonged power outage, battery degradation, overheating, or emergency configuration changes. Therefore, the obtained availability values should be treated as comparative architectural assessment indicators rather than as a complete stochastic description of network behavior.

Each active node $i \in V_a$ is characterized by the mean time between failures $MTBF_i$ and the mean time to recovery $MTTR_i$. The node availability is calculated as follows:

$$A_i = \frac{MTBF_i}{MTBF_i + MTTR_i}$$

Assuming serial criticality of the active chain (failure of any of the critical nodes terminates the access service), the integral availability is as follows:

$$A_{series} = \prod_{i \in V_a^*} A_i \quad (2)$$

where $V_a^* \subseteq V_a$ is a subset of nodes without which the service is unavailable. In the Ethernet scenario $|V_a^*|$ is usually larger due to the intermediate active elements. For the GPON scenario, the critical ones are the mini OLT, the backbone router, and, depending on the service, individual ONUs [9, 12].

4.3. Probabilistic hybrid risk model with a focus on firmware

The hybrid service degradation event D is interpreted as a combination of energy event E (no power outside the UPS) and cyber event C (compromise of the control plane or firmware). The probability is calculated as follows:

$$P(D) = 1 - \left(1 - P(E)\left(1 - P(C \mid E)\right)\right) \quad (3)$$

The term $P(C \mid E)$ emphasizes that during a blackout, temporary policy changes, simplified access to restore services, and monitoring degradation are often observed, which can increase cyber risk [16,17,21]. For SOHO, it is important to highlight firmware attacks as subclass C, where an attacker (or a malicious update package) modifies the firmware of an ONU, router, or auxiliary device. The main vectors are:

SNMP vector. These include weak community strings, incorrect ACLs to the SNMP agent, and protocol implementation vulnerabilities [5, 7].

SSL/TLS vector. These are outdated protocol versions, weak cipher suites, and certificate validation problems in web management interfaces and update mechanisms [19, 20].

Supply chain/updates. This includes the substitution of update files, lack of signature verification, and source compromise [18].

The proposed hybrid risk model is based on a simplified probabilistic representation. It captures the relationship between an energy-related event and a cyber-related compromise event, but it does not fully describe the stochastic temporal dynamics of blackouts, repeated outage cycles, recovery processes, or time-dependent changes in the probability of compromise. In addition, the model does not yet include a multi-state representation of service degradation, where the network may remain partially available for some segments while other services are unavailable. These aspects are outside the scope of this present engineering model and are identified as important directions for future development.

4.4. Optimization of reservation and prioritization of critical segments

To formalize the choice (which nodes to backup first), a binary variable $x_i \in \{0,1\}$ is introduced, which means connecting the node i to a UPS or local backup power supply. Let P_i be the node power. To limit the available UPS power P_{max}, the problem is posed:

$$\max_{\{x_i\}} E[A] \quad \text{if} \quad \sum_{i \in V_a^*} x_i P_i \le P_{max} \tag{4}$$

The SOHO interpretation is as follows: in a GPON scenario, the basic solution always includes $x_{OLT} = 1$ and $x_R = 1$. Only critical ONUs are added later, whereas in an Ethernet scenario, it is often necessary to reserve several intermediate switches at once, otherwise the topology becomes fragmented.

The survivability core is defined as the minimum subset of active nodes $V_{core} \subseteq V_{act}$ that satisfies the required service constraints under blackout conditions:

$$\forall s_k \in S : L_k(V_{core}) \ge L_k^{min}.$$

Simultaneously, the total power consumption of the selected nodes must not exceed the available UPS power budget:

$$\sum_{v_i \in V_{core}} P_i \le P_{UPS},$$

where P_i is the power consumption of node v_i, and P_{UPS} is the maximum available UPS-supported load.

Therefore, the selection of the survivability core can be described as an optimization problem:

$$V_{core}^* = \arg_{V_{core} \subseteq V_{act}} \sum_{v_i \in V_{core}} P_i,$$

subject to

$$\forall s_k \in S : L_k(V_{core}) \ge L_k^{min},$$

$$\sum_{v_i \in V_{core}} P_i \le P_{UPS},$$

$$V_{core} \supseteq V_{mgmt},$$

where V_{mgmt} is the subset of nodes required to preserve centralized management and monitoring visibility. This additional condition is important because no node may directly provide subscriber traffic, but it may still be necessary for configuration control, event logging, or incident localization.

For practical implementation, a binary decision variable is introduced as follows:

$$x_i = \begin{cases} 1, \text{if node } v_i \text{ is included in the survivability core,} \\ 0, \text{otherwise} \end{cases}$$

The optimization problem can then be written as

$$\min \sum_{v_i \in V_{act}} x_i P_i,$$

subject to

$$\sum_{v_i \in V_{act}} x_i P_i \le P_{UPS},$$

$$\forall s_k \in S : L_k(x_1, x_2, ..., x_n) \ge L_k^{min},$$

$$x_i = 1, \quad \forall v_i \in V_{mgmt}.$$

If several feasible variants satisfy these constraints, the preferred variant is selected by maximizing the weighted criticality coverage:

$$\max \sum_{v_i \in V_{act}} x_i CS_i.$$

The practical algorithm for selecting the minimum survivability core is as follows. First, the required services and critical segments are defined, including Internet access, management access, security-camera traffic, VoIP, alarm systems, or other services that must remain available during blackout conditions. Second, the network topology is represented as a graph, with active and passive nodes separated. Third, for each active node, the service-impact function $I(v_i, s_k)$ is calculated. Fourth, the set of critical nodes V_{crit} is determined. Fifth, each critical node is assigned a criticality score CS_i according to the importance of the services it affects. Sixth, the minimum subset V_{core} is selected under the UPS power constraint. Seventh, if the UPS budget is insufficient for all critical nodes, the nodes are prioritized according to the ratio

$$R_i = \frac{CS_i}{P_i},$$

where R_i reflects the criticality gained per unit of power consumption. Nodes with higher R_i values are included first, provided that the required service constraints are preserved.

In the GPON scenario, this procedure usually includes the backbone router and mini OLT in the

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

mandatory survivability core, because they provide centralized connectivity, manageability, and monitoring visibility. ONUs are added selectively only when they serve critical subscriber segments. The passive PLC splitter is not included in the UPS-backed core because it does not require power. However it remains part of the physical topology and must be considered in fault localization. In the Ethernet scenario, several intermediate switches are often selected as critical nodes because their failure disconnects downstream subscribers. This increases the required backup load and increases the size and distribution of the survivability core.

Thus, the revised methodology provides a strict rule for selecting the survivability core: the core must include the minimum set of active nodes that preserves required services, centralized manageability, and monitoring visibility under the available UPS power budget.

4.5. Integrated IDS+SIEM profile with AE+LSTM and CNN+LSTM (Byte2Image)

The AE+LSTM and CNN+LSTM components are used as representative analytical model classes within the proposed IDS/SIEM monitoring profile. They are intended to demonstrate how telemetry-oriented anomaly indicators and firmware-oriented structural indicators can be incorporated into a multimodal monitoring loop. However, the study does not provide a fully reproducible ML training protocol. In particular, it does not fully specify dataset provenance, sample volumes, labeling rules, train/validation/test partitioning, feature preprocessing, epoch schedules, optimizer parameters, hyper-parameter search procedures, or the use of pre-trained weights. Therefore, the ML-related results should be interpreted as indicative comparative metrics within the proposed methodological framework rather than as a complete independently reproducible benchmark.

A multi-layered profile is used to enhance the detection of hybrid attacks.

IDS captures traffic anomalies, scans, exploit attempts, and suspicious patterns at the network layer.

SIEM collects event logs (router, mini OLT, ONU, servers, Wi-Fi controllers), correlates them with rules, and adds analytical features.

Machine learning models assess the typicality of events for two data classes: telemetry and firmware.

AE+LSTM is applied to telemetry time series of x_t features (e.g., error counts, NetFlow aggregates, ONU re-registration rates, R_x / T_x jitter, packet loss rates). The autoencoder compresses the features into the latent space, and the LSTM models the dynamics of the latent representations to detect "slow" attacks and degradations [12].

CNN+LSTM is applied to the Byte2Image representation of the firmware: the byte dump is converted into a two-dimensional fixed-width luminance matrix (Byte2Image), the structural features are extracted by the CNN, and the sequence of updates (versions/time) is tracked by LSTM [16].

AE+LSTM and CNN+LSTM components are introduced at the methodological level of the analytical model classes.

A combined loss function is introduced for simultaneous training/scoring:

$$L = \lambda_1 \cdot L_{cls}(y, \hat{y}) + \lambda_2 \cdot \|x - \hat{x}\|_2^2, \quad (5)$$

where L_{cls} is the classification loss (e.g., cross-entropy) for CNN+LSTM, $\|x - \hat{x}\|_2^2$ is the autoencoder reconstruction error for AE+LSTM, λ_1, λ_2 are the weights. The output scores (anomaly score, firmware drift score) are passed to SIEM as enriched event fields, after which correlation rules and scenario checks are performed according to ATT&CK [17].

AE+LSTM and CNN+LSTM should be interpreted as representative model families within the proposed analytical profile rather than as fully specified neural architectures. A complete implementation-level description, including the exact number and type of layers, latent-space dimensionality, hidden-state sizes, convolutional configuration, and training hyper parameters, is not yet provided and therefore remains outside the present level of reproducible detail.

In addition, AE+LSTM and CNN+LSTM components should be interpreted as representative analytical model classes within the proposed multimodal IDS/SIEM monitoring profile. In this study, AE+LSTM denotes a telemetry-oriented model family intended for detecting deviations in time-series network and device indicators, while CNN+LSTM denotes a firmware-oriented model family intended for analyzing Byte2Image representations and temporal changes in firmware artifacts. However, this study does not claim to provide a complete implementation-level specification of these neural architectures.

A fully reproducible implementation would require explicit description of the autoencoder's encoder and decoder structure, latent-space dimensionality, LSTM hidden-state size, number of recurrent layers, sequence length, convolutional kernel sizes, number of filters, pooling strategy, classifier head, loss functions, optimizer settings, learning rate, batch size, number of epochs, early-stopping criteria, regularization parameters, and train/validation/test partitioning. Because these parameters are not fully specified, the AE+LSTM and CNN+LSTM components are used as methodological

analytical profiles rather than as final reproducible neural implementations.

5. Case Study

Quantitative and qualitative verification of the proposed methodology is provided for two scenarios. The presented materials focus on indicators that are practically significant. These indicators directly follow from the methods, namely, the number of critical active nodes and the nature of cascading failures in a blackout, the autonomy of the backup for the "survival core" and selectively critical subscriber segments, and the integral availability of the service as a function of the active chain composition.

5.1. Comparative structural assessment and failure points

Table 1 compares the architectures in terms of the number of critical active nodes, redundancy nature, and behavior during a blackout. In GPON, the key element of fault tolerance is passive branching.

The architecture # 1 is Ethernet everywhere.

The architecture # 2 is GPON (mini OLT + 1:32).

The architecture # 3 is GPON + selective ONU redundancy.

Table 1

Comparison of architectures by node criticality, branching scheme, and cascading failure resistance

#	Critical active nodes	Passive branching	UPS logic	Risk of cascading failure
1	3--6	No	Distributed (multiple points)	Increased
2	2 + ONU	Yes	Centralized (core)	Reduced
3	2 +	Yes	Core + critical ONUs	Minimized

An integrated topological survivability score is introduced to compare Ethernet and GPON scenarios:

$$S_{top} = 1 - \left(\lambda_1 K_{AD} + \lambda_2 K_{CN} + \lambda_3 K_{RL} + \lambda_4 \overline{C}\right),$$

where $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ are weighting coefficients satisfying $\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 = 1$, $\lambda_i \geq 0$.

The value of S_{top} increases when the number of critical active nodes, the share of power-dependent critical elements, and the average impact of node failures decreases. Therefore, this indicator is suitable for comparing access architectures in terms of structural survivability.

In the Ethernet scenario, the number of active intermediate devices increases as the number of subscriber connections grows. As a result, the sets V_{act} and V_{crit} usually expand simultaneously, increasing the number of powered failure points and the probability of cascading service degradation. The passive splitter increases the number of subscriber branches in the GPON scenario without increasing the number of active nodes in the distribution zone. Therefore, the growth of subscriber connections does not proportionally increase $|V_{crit}|$, which improves S_{top} and reduces the access topology's structural vulnerability.

Thus, the comparison of Ethernet and GPON architectures is strengthened by quantitative topological indicators. These indicators confirm the main engineering conclusion of the study: the GPON scenario's survivability advantage is driven not only by lower power consumption but also by reduced distributed active dependencies and the concentration of critical functions in fewer manageable nodes.

The obtained results should be interpreted not as isolated values for only three fixed configurations, but as a scaling trend. In Ethernet-based access, increasing the number of connections increases the number of distributed active elements, such as switches, PoE injectors, or intermediate powered nodes. This increases the number of UPS-dependent failure points and may increase cascading vulnerability. In GPON-based access, the number of subscriber branches can grow to the splitter limit without a proportional increase in the active distribution elements. Therefore, the advantage of GPON becomes more evident as the number of connections approaches the medium and upper SOHO ranges.

5.2. Numerical examples of UPS autonomy and redundancy scenarios

Consider a typical example of a preliminary engineering calculation. Let the power of the mini OLT be $P_{OLT} = 18\text{W}$, the power of the backbone router $P_R = 12\text{W}$. For the core, the power is $P = 30\text{W}$. For the battery $C = 18\text{A}\cdot\text{h}$, $U = 18\text{V}$, $\eta = 0.85$ from (1), the redundancy autonomy is equal to the following:

$$T \approx \frac{18 \cdot 12 \cdot 0.85}{30} \approx 6.12$$

Next, the prioritization strategy is evaluated: if 4 ONUs of 5 W are to be critically supported, then $P = 50\text{W}$ and $T \approx 3.67$. If an entire floor or sector (10 ONUs) is to be supported, $P = 80\text{W}$ and $T \approx 2.30$ (Table 2).

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Table 2

UPS autonomy assessment for different power scenarios

Scenario	P, W	C, A · h	η	t
Core (OLT + Router)	30	18	0.85	6.12
Core + 4 critical ONUs	50	18	0.85	3.67
Core + 10 ONU (critical sector)	80	18	0.85	2.30

GPON allows us to separate the concepts of "network backbone" and "subscriber periphery". The backbone is maintained centrally, and the periphery is selectively reserved, which is consistent with problem (4). In the Ethernet scenario, a similar strategy often does not work, since intermediate switches are both periphery and part of the backbone.

5.3. Availability assessment: impact of number of active nodes

To illustrate (2), consider the simplified but indicative values of node availability under normal conditions: $A_R = 0.995$ (router), $A_S = 0.993$ (typical switch), $A_{OLT} = 0.995$, $A_{ONU} = 0.992$. For the Ethernet scenario, assume that the router and two switches are critical $\left(V_a^* = \{R, S_1, S_2\}\right)$:

$$A_{Eth} = 0.995 \cdot 0.993 \cdot 0.993 \approx 0.981.$$

For a GPON scenario, the router and mini OLT are critical $\left(V_a^* = \{R, OLT\}\right)$:

$$A_{GPON} = 0.995 \cdot 0.995 \approx 0.990.$$

The percentage point difference in availability is significant over the annual interval, and in blackout conditions the effect is amplified as the proportion of MTTR increases in the Ethernet scenario due to the larger number of locations where power needs to be restored and connectivity checked [9, 12].

5.4. Hybrid attack detection. SIEM rules and ML models

The numerical comparison of detection profiles should be interpreted with caution because the neural components are not specified at the full architecture and training-protocol level. The reported AE+LSTM and CNN+LSTM profiles illustrate the potential contribution of telemetry-oriented anomaly detection and firmware-oriented structural analysis to SIEM-level correlation. They should not be treated as final benchmark results of completely disclosed neural models. A strict experimental validation would require a complete architecture table for each model, dataset description, class distribution, preprocessing pipeline, training protocol, validation procedure, test protocol, and statistical reporting of results.

Three profiles were compared within the simulation (Table 3):

1. A basic IDS+SIEM rule-based correlation profile using IDS events and system logs.

2. An AE+LSTM-based profile for event/flow telemetry, aimed at detecting deviations from the usual operating profile [12].

3. A CNN+LSTM-based profile for firmware analysis in Byte2Image representation, aimed at detecting suspicious structural changes/drift [16].

The rule-only approach strongly depends on the completeness of logging and the quality of correlation rules, whereas AE+LSTM is better suited for previously unseen telemetry anomalies [12], and CNN+LSTM adds a specific signal for firmware-oriented analysis through Byte2Image-based structural representation [16], even when network traffic may appear normal in the early stages.

The comparative profiles summarized in Table 3 should be interpreted as a methodological comparison of detection profiles rather than as a fully documented cyber-range benchmark or as a strict benchmark based on one fully documented unified dataset. A complete description of the cyber threat simulation workflow, including the exact attack-generation toolchain, scenario timing, traffic generation logic, firmware manipulation procedure, and event collection instrumentation, is not yet provided in reproducible detail, and the complete training workflow for the ML-based profiles, including exact dataset sources, sample sizes, epoch counts, hyperparameter settings, and pretraining status, is not yet documented. Therefore, the values in Table 3 for AE+LSTM and CNN+LSTM should be interpreted as indicative comparative results within the proposed monitoring framework rather than as fully reproducible ML benchmark outcomes.

Table 3

Comparison of approaches for detecting hybrid cyberattacks based on quality metrics and detection time

Approach	F1	ROC-AUC	MTTD, min
IDS+SIEM rules	0.78	0.84	18.5
AE+LSTM (events/flows)	0.88	0.92	7.4
CNN+LSTM(Byte2Image, firmware)	0.91	0.94	6.2
AE+LSTM + CNN+LSTM (SIEM integration)	0.93	0.95	5.9

The quantitative indicators are used to illustrate the relative contribution of telemetry-based anomaly detection, firmware-oriented structural analysis, and SIEM-level multimodal correlation within the proposed monitoring framework.

IDS+SIEM approach depends on rules and logs. AE + LSTM approach is strong for detecting unknown anomalies. CNN+LSTM approach detects changes in the structural firmware. In the AE+LSTM + CNN+LSTM approach, modality correlation reduces FPR and may shorten the effective MTTD by triggering SIEM-level alerts earlier from heterogeneous evidence sources.

The F1 values reported are comparative indicators within the proposed monitoring framework. However, the exact averaging scheme used for the F1-score (macro-, micro-, or weighted) and class-wise confusion statistics are not yet specified. Therefore, the reported F1 values should be interpreted as indicative comparative metrics rather than as fully specified benchmark indicators under a documented class-distribution protocol.

The operational delay between the emergence of a suspicious event pattern and its detection by the corresponding monitoring profile is characterized by MTTD.. Therefore, the reduction of MTTD from 18.5 min to 5.9 min should be interpreted as an improvement in detection and triage speed within the monitoring loop, rather than as a standalone guarantee of full real-time attack prevention.

MTTD values reflect detection and triage speed within the monitoring profile and should not be interpreted as a direct standalone guarantee of full attack prevention without considering the response mechanism. The quantitative values within the proposed monitoring framework should be interpreted as comparative indicators.

This comparison is conducted at the level of methodological detection profiles and not at the level of exhaustively documented neural architecture instantiations. Therefore, AE+LSTM and CNN+LSTM should be read as architectural classes used to structure the monitoring concept, while a full layer-by-layer specification remains a task for future reproducible implementation reporting.

From the deployment perspective, these ML components should not be interpreted as being executed directly on all low-power SOHO network elements. In the considered methodological profile, AE+LSTM and CNN+LSTM represent analytics functions assigned to a separate monitoring computation point, which may be implemented as an edge device, protected local server, or externalized analysis node. Therefore, their computational and energy requirements are outside the baseline UPS calculations for the communication survival core. This distinction is important for correctly interpreting the practical applicability of the proposed architecture under blackout conditions.

Accordingly, the values reported in Table 3 should be treated as indicative comparative metrics within the proposed IDS+SIEM/ML analytical framework. They are intended to illustrate the relative behavior of rule-based, telemetry-based, firmware-oriented, and multimodal correlated detection profiles, rather than to claim a fully self-contained experimental benchmark documented at the level of a complete attack-emulation protocol.

Additionally, it was found that for SOHO it is important not only to "catch the attack", but also to quickly localize its plane: optics/installation, service configuration, ONU compatibility (GPON/EPON/XPON), or management compromise. The centralized visibility of the mini OLT (ONU statuses, optical R_x / T_x levels, registration history) combined with SIEM correlation gives the greatest operational effect [1,4].

The results of cyberattack detection should be interpreted in light of the current level of experimental disclosure. The comparison of IDS/SIEM rules, AE+LSTM telemetry analysis, CNN+LSTM firmware-oriented analysis, and the integrated monitoring profile illustrates the relative behavior of the different detection profiles in the proposed framework. Simultaneously, the study does not yet provide a complete cyber-range description that would be required for strict replication of the reported metrics. The exact attack-generation toolchain, traffic-generation procedure, attack timing, malicious firmware manipulation workflow, event collection instrumentation, SIEM parsing rules, and the mapping between generated cyber events and detection labels are not yet sufficiently detailed.

F1, ROC-AUC, and MTTD values should be interpreted as indicative comparative metrics within the proposed monitoring framework. This version of the study does not yet provide a complete metric-reporting protocol. In particular, the averaging scheme for the F1-score, such as macro-, micro-, or weighted averaging, is not fully specified. The class balance, the number of normal and attack samples, and the class-wise confusion statistics are also not reported in sufficient detail. Therefore, the reported values should not be interpreted as final benchmarks for fully reproducible ML performance.

The evaluation protocol should include the confusion matrix for each detection profile, including true positives, false positives, true negatives, and false negatives, for strict interpretation of the ML-based detection results. It should also report precision, recall, F1-score with an explicitly defined averaging scheme, False Positive Rate, False Negative Rate, ROC-AUC, and MTTD. In cyberattack detection tasks, where class imbalance is usually significant, macro-F1 and class-wise recall are especially important, because a high aggregated score may hide poor detection of rare but critical attack classes.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

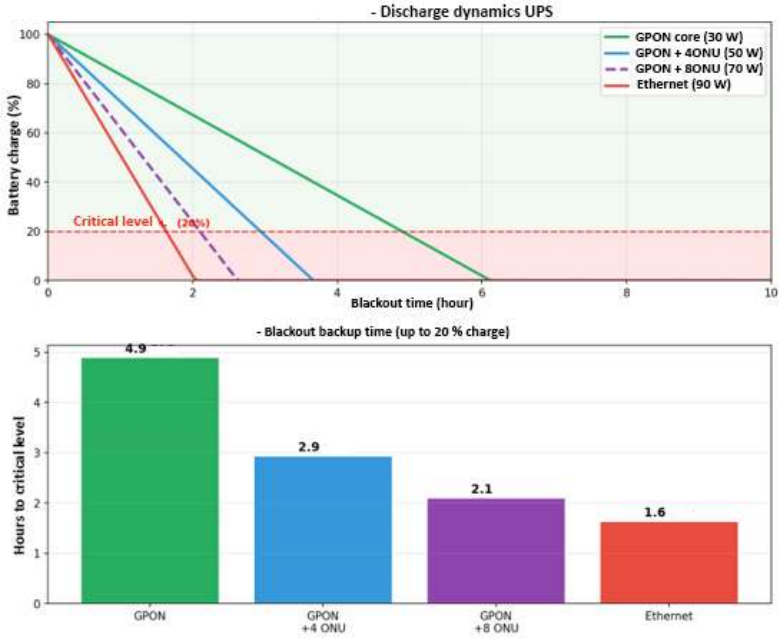

Fig. 5. Blackout simulation for SOHO network

5.5. Operational diagnostics

The visualizations bring the calculated estimates of autonomy, power consumption, and blackout survivability to a format suitable for a quick SOHO engineering solution. Each graph answers the applied question of "what will we get" for a given load, battery capacity, and redundancy scenario, and simultaneously demonstrates how the GPON approach's advantage over Ethernet changes as connections scale.

Fig. 5 shows the result of a blackout simulation for SOHO network as a visual comparison of how quickly the UPS discharges under different architectural scenarios and redundant load composition.

The upper part of the figure shows the UPS discharge dynamics over time. The dotted line indicates the critical level of 20%, which is accepted as the threshold for safe operation (below it, the risk of incorrect node shutdown and communication loss increases). The graph compares scenarios with redundancy of only the GPON "core" (least load), the GPON "core" with additional power supply for some subscriber ONUs (intermediate options), and an Ethernet scenario with a higher total load. As the redundant load increases, the curves become steeper, indicating that the UPS reaches the critical threshold faster. In addition, GPON configurations with lower redundancy exhibit slower discharge than Ethernet.

The lower part of the figure aggregates the same result in the format of "backup time up to 20%." For the GPON core it is 4.9 hours, for GPON with 4 ONU redundancy - 2.9 hours, for GPON with 8 ONU redundancy - 2.1 hours, while for Ethernet - 1.6 hours. Thus, Fig. 5 shows two practical patterns. First, centralized redundancy of the minimum GPON "core" provides the largest autonomy margin. Second, extending the redundancy to subscriber terminals is a manageable compromise between service coverage and autonomous operation duration, and even with extended redundancy, GPON scenarios maintain a better profile than Ethernet for a comparable access scale.

Fig. 6 presents a general result of a comparative analysis of SOHO access energy efficiency for two architectural scenarios – GPON with a mini OLT and classic Ethernet – across connection scales.

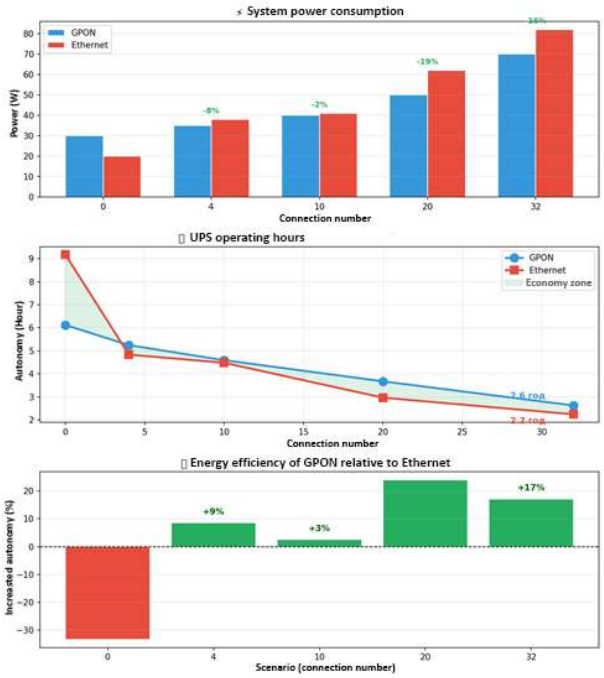

Fig. 6. SOHO GPON Mini OLT. Energy efficiency

Fig.6 top graph shows the total system power (W) for different numbers of connections. For small configurations, the differences between architectures may be insignificant or even favor Ethernet, since GPON core costs are fixed regardless of the number of connections.

However, with increasing scale (10–20–32 connections), a noticeable trend toward a better energy profile for GPON is observed, which is explained by a decrease in the number of distributed active nodes in the access field and by a greater concentration of controllability in a single node. The middle graph shows UPS autonomy as a function of the number of connections: as load increases, autonomy naturally decreases in both scenarios, but the GPON and Ethernet curves diverge at medium and large configurations. The "economy zone" shows the range in which GPON provides more UPS runtime with the same battery capacity, i.e. creates an additional margin of stability during blackouts. The lower graph aggregates the comparison by relative gain in GPON autonomy compared to Ethernet across the given scenarios. Positive values correspond to situations where GPON provides longer UPS operation time, and the maximum effect is manifested in scaling scenarios, when the number of active intermediate elements and the total power increase in the Ethernet architecture.

Figure 7 shows a UPS configuration selection matrix that summarizes the energy modeling results as a "solution map" for SOHO. Its purpose is purely practical: to quickly determine the expected autonomy for a given battery capacity and total load, and to compare typical operating points for Ethernet and GPON scenarios.

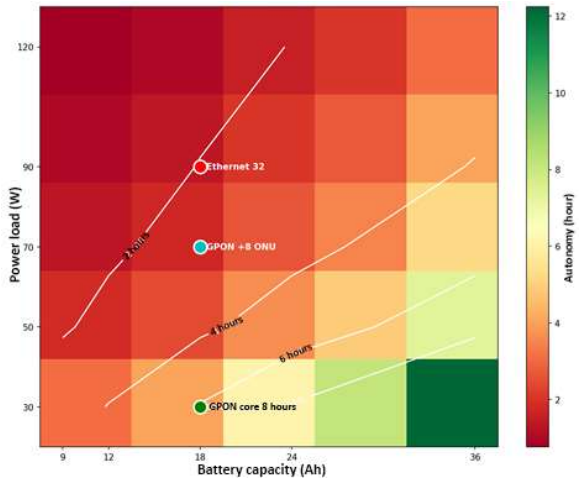

Fig. 7. UPS configuration selection matrix

The color of the cells corresponds to the autonomy (hours): the "greener" the longer the UPS provides power, while the red areas correspond to a short operating time. The plotted isolines (approximate contours of equal autonomy) allow us to read the matrix not only by cells, but also as a continuous dependence: increasing the battery capacity or reducing the load shifts the system into a zone of greater autonomy. The points on the graph indicate typical scenarios: Ethernet for 32 connections, as the case with the highest total load, GPON-"core" as the minimally redundant option with the lowest load, and GPON with additional redundancy of part of the ONU as a compromise between service coverage and uptime.

It is advisable to choose a UPS in SOHO not "by device power", but by the battery-load pair of parameters, where the GPON architecture gives a practical advantage precisely due to the lower critical power of the redundant core.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

The key application conclusion shows that the advantage of GPON in energy efficiency is most pronounced not in minimal configurations, but in typical SOHO scenarios of growth to dozens of connections, where autonomy during a blackout becomes a critical metric.

The results of modeling and experimental and computational examples confirmed that the determining factor for SOHO in blackout conditions is not the nominal bandwidth but the number of critical active dependencies in the access chain and the ability to centrally maintain the "core" of the network under UPS. A comparative structural evaluation showed that the GPON scenario based on a mini OLT with passive branching reduces the risk of cascading failure by removing power from the distribution zone (passive splitter), while the Ethernet scenario with dozens of connections increases the number of intermediate active elements and increases the requirements for distributed redundancy. Numerical examples of UPS autonomy and visualization confirmed the practical advantage of the "core redundancy + selective redundancy of critical ONUs" approach. The minimally redundant GPON variant provides the largest time margin to the critical charge level, and extending the redundancy to subscriber terminals predictably reduces autonomy, but provides a manageable compromise between uptime and service coverage. From the perspective of cyber resilience and operational monitoring efficiency, the rule-only IDS+SIEM profile is found to be sensitive to logging completeness and rule quality, while the addition of AE+LSTM for telemetry and CNN+LSTM for firmware artifacts in the Byte2Image representation provides more robust anomaly detection and reduces time to detection, especially in firmware attack scenarios where early network symptoms may be weak.

The practically significant result is also the strengthening of diagnostics due to centralized visibility of ONU states and optical channel parameters, which allows for faster separation of installation errors and physical degradations from configuration failures and cyber compromise. Therefore, the results obtained demonstrate that the architectural transition to GPON in SOHO provides a reproducible gain in survivability during power outages and lays better foundations for manageability and the detection of hybrid attacks through centralization of control and a reduction in the number of critical active nodes.

6. Results and Discussion

The results confirm that the decisive parameter in the SOHO segment is the number of active dependencies in the critical access chain, rather than peak speed or nominal bandwidth. The GPON scenario minimizes critical active nodes via passive branching, thereby increasing availability and simplifying redundancy. Importantly, this is a consequence of the architectural organization, namely, active elements are concentrated in one controlled point (core), where they can be realistically protected by UPS and organizational controls, while the number of intermediate nodes increases in distributed Ethernet logic, thereby increasing the probability of cascading failure and operational complexity of recovery.

The results should be interpreted with regard to the proposed models' simplified assumptions. The availability assessment is suitable for comparing the structural effect of active-node reduction in Ethernet and GPON scenarios, however, it does not yet account for dependent node failures or common-cause degradation mechanisms. Similarly, the hybrid risk model is useful for formalizing the interaction between blackout conditions and cyber compromise, but it does not model blackout duration as a stochastic process or represent service availability as a set of multiple degraded states. Therefore, the practical value of the models lies in supporting architectural comparison, backup prioritization, and preliminary survivability assessment rather than in providing a complete probabilistic simulation of SOHO network behavior under all possible outage and attack scenarios.

The use of combined AE+LSTM and CNN+LSTM (Byte2Image) models as a multimodal mechanism to reduce blind-spot detection is methodologically justified. AE+LSTM captures anomalous telemetry dynamics (slow drifts, atypical series of events, changes in the flow profile), which are relevant for "slow" and low-noise attacks and degradations. CNN+LSTM with Byte2Image adds an independent signal of structural changes in firmware, which can be an early indicator of compromise even when network manifestations are still weak or disguised as normal activity. The practical effect of integration into SIEM is the time required to localize the incident plane. In the reported case study, a lower MTTD measured in minutes also reflects this effect; however, this indicator should be interpreted as a monitoring-response efficiency metric rather than a universal proxy for guaranteed real-time prevention. The centralized visibility of the mini OLT (ONU statuses, registration history, optical parameters) combined with SIEM correlation provides the greatest operational gain for small support teams. An illustrative example of the "architectural effect" at the manageability level is presented. In a GPON scenario, management and telemetry are naturally centralized in a single node, simplifying access control, logging, and event correlation. In contrast, in a distributed Ethernet scenario, the number of management surfaces (switches, PoE elements, access points) increases, thereby increasing the likelihood of weak links in access policies and configurations. In practice, this means that "fewer different control panels" often provides a greater gain in stability than cosmetic rule enhancements, because the error plane is reduced and change auditing is

simplified.

The lower MTTD observed for the integrated AE+LSTM + CNN+LSTM + SIEM profile should not be interpreted due to lower computational complexity. In contrast, the combined profile is analytically heavier, but it can trigger an incident earlier because SIEM correlates heterogeneous weak signals from telemetry anomalies, firmware drift indicators, and rule-based events. Thus, the gain is achieved through earlier multimodal evidence fusion rather than faster standalone inference. At the same time, the present study does not yet provide a full reproducible dataset specification, which should be considered an important limitation of the reported quantitative metrics.

The quantitative comparison of detection profiles must be interpreted with caution because the metric calculation procedure is not yet fully disclosed. The F1-score strongly depends on the averaging strategy and class distribution. The majority class may dominate micro-averaged F1, whereas macro-averaged F1 gives equal weight to each class and is more informative when rare attack classes are present. Weighted F1 reflects class proportions but may still mask the weak detection of low-frequency attacks. For this reason, future evaluation should report the averaging scheme explicitly and provide class-wise precision, recall, F1-score, FPR, FNR, and a confusion matrix for each detection profile.

The MTTD metric also requires a precise operational definition. The MTTD is interpreted as the average delay between the emergence of a suspicious event pattern and the generation of a corresponding alert by the monitoring profile. However, a fully reproducible evaluation should specify the event start time, alert trigger condition, SIEM correlation window, timestamping procedure, and missed detection treatment. Without these details, MTTD should be interpreted as an indicative operational metric rather than a strictly reproducible timing benchmark.

The limitations of the study require separate fixation, as they determine the portability limits of the obtained numbers and scenarios. First, the numerical parameters of power consumption are generalized and should be specified according to the parameters of specific models of mini OLT, ONU, and routers, as well as considering the real load mode and battery degradation [8]. Secondly, the main emphasis in the availability calculations is on active nodes. Passive defects in the optical installation (quality of connectors, mixed IN/OUT splitter direction, APC/UPC mixing) were not modeled as a separate stochastic process, although in practice they can form the primary "incident background" and affect MTTR indicators due to time spent on diagnostics. Third, training machine learning models in SOHO is complicated by small data volumes and heterogeneity in logging. In such conditions, disciplined event collection, drift control, transfer learning application, and correct validation of local data are critical. Additionally, the cost of operating ML is a practical consideration. Even if the model improves detection, it must be operationally manageable within a small team's resources; otherwise, the effect is nullified.

The scalability of the proposed approach is ensured because the methodology does not depend on fixed values of 5, 20, and 32. These values are used only as reference points to demonstrate the behavior of the compared architectures. The same procedure can be repeated for another SOHO configuration by specifying the actual number of endpoints, the set of active nodes, the power consumption of each node, the required service chains, the number of critical subscriber segments, and the available UPS capacity. Thus, the proposed approach can be applied to smaller or larger SOHO variants, provided that the selected access technology's architectural constraints are taken into account.

The ML part of the proposed monitoring profile is a methodological component of the survivability framework rather than a fully disclosed machine-learning experiment. AE+LSTM and CNN+LSTM were introduced to show how heterogeneous signals, such as telemetry time series and firmware structural representations, can be integrated into IDS/SIEM correlation. However, the current manuscript does not provide sufficient implementation detail to independently reproduce the neural models. Therefore, within the proposed framework, the ML-related metrics should be treated as indicative comparative values. This limitation does not affect the paper's architectural contribution, but it limits the ML component's reproducibility and requires additional experimental disclosure in future work.

Simultaneously, the study has an important deployment limitation. The exact hardware profile, power demand, and inference latency of the AE+LSTM and CNN+LSTM components in a real SOHO installation are not quantified. Therefore, the communication survivability gains reported for the GPON-based architecture should not be interpreted as automatically guaranteeing the blackout-resilient operation of the full intelligent monitoring stack. The design of low-power edge AI platforms capable of supporting such analytics under strict power constraints remains a separate engineering task, but a further limitation is the absence of a complete AI training protocol. The manuscript does not yet report, in a reproducible experimental format, the training dataset sizes, epoch counts, optimization settings, hyper parameter configuration, or the use or non-use of pre-trained weights for the neural components. For this reason, the ML-related part of the work should presently be interpreted as a methodological design framework rather than as a fully disclosed experimental training-and-evaluation pipeline.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

In addition, an important limitation of the study is the lack of a full technical description of the simulation environment for cyber threats. In particular, the manuscript does not yet document, in a reproducible end-to-end form, the exact attack tools, attack-injection logic, scenario sequencing, malicious traffic generation procedure, and firmware-manipulation workflow that would be required for strict replication of the reported metrics. For this reason, the quantitative values in Table 3 should be interpreted as comparative methodological indicators rather than final deployment-grade benchmark results.

Another limitation of the current quantitative evaluation is that the F1-score reported in Table 3 is not yet accompanied by an explicit averaging definition or by class-wise confusion analysis. In cyber-attack detection tasks, where class imbalance is often substantial, strict interpretation of the metric is restricted. For a rigorous future evaluation, the reporting should include the averaging scheme for F1, the False Negative Rate (FNR), and preferably a full confusion matrix or equivalent class-wise performance breakdown.

Another limitation of the present study is that the ML components are not yet described at the exact implementation architecture level. In particular, the manuscript does not specify the precise number of convolutional and recurrent layers, hidden dimensions, latent-space size, or detailed hyper parameterization. Therefore, the ML part of the work should be interpreted as a methodological design framework rather than a fully disclosed neural implementation ready for direct replication.

The ML-related part of the study has an important limitation in terms of reproducibility. Although the reported values demonstrate the potential contribution of telemetry-based anomaly detection and firmware-oriented structural analysis to reducing detection time, they should not be treated as a fully documented experimental campaign's final benchmark results. A rigorous reproducible evaluation would require explicit disclosure of dataset sources, data volumes, class distribution, labeling methodology, preprocessing procedures, train/validation/test splits, model architectures, layer parameters, latent-space dimensionality, recurrent block settings, optimizer configuration, learning rate, number of epochs, stopping criteria, and hardware/software environment. A complete cyberattack simulation protocol, including attack tools, scenario sequencing, traffic generation, firmware manipulation, event logging, and SIEM correlation rules, would also be required. These elements are now identified as limitations of this study and as mandatory components of future experimental validation.

Moreover, it should be emphasized that the provision of telecommunication service continuity during blackouts and ML-based cyberattack detection are analytically distinct, although operationally related, problems. In the present study, the reported UPS autonomy and survivability estimates refer only to the communication survival core, i.e., the minimum set of active network elements required to preserve access service under degraded power conditions. These calculations do not include the computational energy demand of the IDS+SIEM infrastructure and the DL inference components. Therefore, the energy advantage of the GPON-based architecture should be interpreted as an architectural and operational advantage for maintaining connectivity and centralized manageability, rather than as proof of the entire intelligent cybersecurity stack's fully autonomous operation.

However, such architectural centralization and passive optical distribution provide an important practical basis for resilient monitoring, diagnostics, and incident localization under blackout conditions characterized by dynamically reduced access to grid power. In this sense, a common operational environment motivates the integration of survivability and cyber-monitoring profiles rather than identical energy accounting. The development of low-power mobile or edge platforms for neural-network-based security analytics, capable of supporting anomaly- and firmware-oriented detection functions under strict blackout energy constraints, is a promising direction for further research.

The Zero Trust component should be interpreted as a practical control layer rather than as a complete formal Zero Trust architecture. This study defines how the GPON-based SOHO access architecture should be operated to reduce the probability and impact of hybrid compromise. In particular, the proposed control layer requires logical separation of administrative and subscriber domains, least-privilege access to the mini OLT, router, and ONU management interfaces, restriction of SNMP and web-management services, logging of configuration changes, firmware version inventory, and SIEM-level correlation of authentication, configuration, telemetry, and firmware-related events. A complete formal model of Zero Trust policy decision, policy enforcement, identity governance, and continuous adaptive authorization remains outside the scope of this article and is identified as a direction for further research.

This approach allows us to reduce false positives through modality correlation, increase the explainability of decisions, and speed up response, which is critical for small support teams and extreme operating conditions. In further work, it is advisable to develop this direction in the form of scenario-oriented correlation pipelines (in terms of tactics and techniques), where the output signals of AE+LSTM and CNN+LSTM are interpreted not in isolation, but as consistent indicators within specific classes of hybrid detection and response scenarios.

The results show that the study's main contribution is not limited to comparing Ethernet and GPON architectures. The key contribution is the proposed integration of

passive GPON branching, a centralized survivability core, and multimodal monitoring into a single operational model for SOHO networks during blackouts. Passive optical branching reduces the number of active elements requiring backup power. The centralized survivability core enables UPS resources to be prioritized and preserve the minimum manageable communication backbone. Multimodal IDS/SIEM monitoring provides correlation of heterogeneous signals, including telemetry anomalies, configuration events, optical-channel parameters, and firmware-related indicators. This integration creates a practical basis for maintaining connectivity, improving incident visibility, and reducing localization time during hybrid cyber-energy degradation.

7. Conclusions

The scientific and practical novelty of the work is the integrated use of GPON-based passive access, a centralized survivability core, and multimodal monitoring for SOHO networks operating under blackout conditions and hybrid cyberattack risks. The GPON component reduces the number of critical active dependencies in the access zone. The centralized survivability core provides an engineering basis for selective UPS redundancy and manageability preservation. The multimodal monitoring component supports detection and localization of hybrid incidents by correlating IDS/SIEM events with telemetry, configuration, optical-channel, and firmware-related indicators. Thus, the proposed approach transforms network survivability from a separate power-backup problem into an integrated architectural, operational, and cyber-monitoring methodology.

This study developed and tested a model for designing SOHO access networks that simultaneously considers two dominant exploitation factors in the Ukrainian context: survivability during blackouts and countermeasures against hybrid cyberattacks. It is shown that the mini OLT GPON architecture with passive optical branching up to 32 ONU subscriber terminals reduces the number of critical active nodes in the access chain, increases availability by (2), and simplifies redundancy by (1). The resulting effect is interpreted as a consequence of the correct architectural organization. Active equipment is concentrated in a managed core, which can realistically be kept under UPS and organizational controls, while the number of intermediate dependencies increases in distributed Ethernet structures, thereby increasing the risk of cascading failure and recovery time. SOHO cyber resilience is formalized in the work through a hybrid probabilistic risk model (3) that focuses on firmware attacks driven by vulnerabilities and control plane configuration errors. SNMP and SSL/TLS are often easy entry points for compromising embedded devices in SOHO. Weak or generic credentials, excessive privileges, and a lack of management segmentation amplify the SNMP vector, whereas the SSL/TLS chain is amplified by outdated cryptographic profiles, incorrect certificate validation, and inconsistent web management settings. Firmware in SOHO should be considered a full-fledged security object with origin and integrity controls, not a technical component updated on an ad hoc basis. An integrated IDS + SIEM circuit is proposed to reduce detection time and increase incident explainability, reinforced by two complementary ML components: AE+LSTM for telemetry time series and CNN+LSTM for firmware analysis in the Byte2Image representation. This combination enables simultaneous capture of anomalous event/flow dynamics and detection of firmware structural changes as an early indicator of compromise. The results of these assessments in SIEM can be used as enriched event fields for incident correlation and localization. This is critical, especially for the SOHO, where the support team is small and time for manual analysis is limited.

It is advisable to begin the practical implementation of mini OLT GPON in SOHO by defining a clear "core of survivability" and reservation rules. The most manageable strategy is centralized redundancy under a single UPS for a minimum set of nodes on which the network backbone depends (mini OLT and backbone router), with subsequent selective redundancy of only critical ONUs according to business process and service priorities. This approach ensures basic connectivity and manageability for as long as possible, expanding power coverage only where it is economically and operationally justified. Standardization of optical connection installation and discipline of initial parameter fixation are critical to reduce incidents and recovery time. It is advisable to implement a unified connector policy, not mix APC/UPC, clearly mark the IN/OUT directions of the splitter, keep an inventory of routes, and record the basic optical R_x / T_x levels as a "zero line" for further diagnostics. This transforms failure localization from a random search to a reproducible procedure and reduces the risk of misinterpreting an installation problem as a cyber-incident. When managing, the priority should be to limit SNMP and management services to the minimum necessary level. In practice, this means using unique credentials, applying access lists, delegating control to a separate segment, limiting access sources, and, if possible, disabling unnecessary control services. Simultaneously, strengthening SSL/TLS management profiles are necessary. It is necessary to avoid outdated protocol versions, ensure certificates are correctly validated in management interfaces, control cryptographic settings, and exclude configurations that allow session interception or spoofing. A firmware policy should be implemented. Firmware management in SOHO should be formalized as a process. Controlling the origin of updates, implementing integrity checks, maintaining a version registry, scheduling update

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

windows, and minimizing manual, unaudited interventions are necessary.

This approach reduces the risk of supply chain compromise and provides a basis for correctly interpreting changes, such as illegitimate updates, potential drifts, or unauthorized modifications. To achieve operational effectiveness from monitoring, it is necessary to integrate not only IDS triggers but also mini OLT/ONU telemetry, registration/deregistration events, configuration changes, and physical layer parameters that allow you to distinguish channel degradation from attacks or policy errors into SIEM. It is advisable to add analytical anomaly assessments with AE+LSTM and firmware drift indicators with CNN+LSTM/Byte2Image to SIEM events as standard parameters to simplify correlation and reduce incident localization time. Consequently, SIEM becomes a decision-making tool within the limited resources of SOHO. Implementing micro-segmentation, applying least privilege for management, ensuring continuous verification of access to management interfaces, and complete logging of administrative actions are recommended. This increases the controllability of changes, reduces the risk of lateral movement if a single segment is compromised, and lays the groundwork for a reproducible incident response even in small networks.

The Zero Trust principles should be understood as implementation-oriented security constraints for SOHO network operation. They support segmentation, least privilege, management-plane isolation, firmware inventory, access logging, and continuous event correlation. However, this work does not claim to provide a complete formal Zero Trust architecture with fully specified identity, authorization, and policy-enforcement mechanisms. The development of such a formal Zero Trust model for blackout-resilient SOHO networks is considered a separate direction for future research.

A limitation of the proposed methodology is that the presented availability and hybrid-risk models are based on simplified engineering assumptions. They do not yet include stochastic blackout dynamics, active node-dependent failures, common-cause failures, repair-process constraints, or partial service degradation states. Future work should extend the proposed framework toward multi-state availability models, Markov or semi-Markov representations of blackout and recovery processes, and dependency-aware risk models that account for correlated failures and gradual service degradation.

A limitation of the current study is the incomplete reproducibility of the ML-based experimental component. The proposed AE+LSTM and CNN+LSTM elements are introduced as analytical model classes within the multimodal IDS/SIEM monitoring profile; however, a complete implementation- and training-level description is not yet provided. Future work should include a fully documented experimental protocol with explicit dataset provenance, sample sizes, class balance, labeling rules, train/validation/test partitioning, feature preprocessing, neural architecture parameters, optimizer settings, hyper-parameters, epoch schedules, stopping criteria, and pre-trained versus non-pre-trained initialization. In addition, a reproducible cyber-range methodology, including attack-emulation tools, traffic-generation scenarios, firmware-manipulation procedures, logging pipelines, SIEM correlation rules, and mapping between simulated events and evaluation metrics such as F1-score, FPR, FNR, ROC-AUC, and MTTD, should be provided.

A separate limitation of the study is that AE+LSTM and CNN+LSTM are presented as analytical model classes rather than fully specified neural architectures. The manuscript does not yet provide complete information on layer structure, latent-space dimensionality, recurrent parameters, convolutional configuration, training hyperparameters, validation procedure, and test protocol. Future work should include a full model specification, preferably in the form of architecture tables, training-parameter tables, dataset documentation, validation methodology, and ablation experiments comparing rule-based IDS/SIEM, AE+LSTM, CNN+LSTM, and their multimodal combination.

A limitation of the current evaluation is the incomplete disclosure of the metric calculation methodologies for F1, ROC-AUC, and MTTD. The manuscript does not yet provide a full class-balance description, F1 averaging scheme, class-wise confusion statistics, or detailed MTTD timing protocol. Future work should include a complete evaluation protocol, including the number of samples per class, the train/validation/test distribution, confusion matrices, macro-, micro-, and weighted F1 values, precision, recall, FPR, FNR, ROC-AUC with confidence intervals, and an explicit procedure for measuring MTTD. This is necessary for the strict interpretation of the effectiveness of the ML-based monitoring profiles and for the independent reproducibility of the reported results.

Future work should include a fully specified evaluation protocol with explicit metric definitions, including the averaging scheme for F1-score, FPR, FNR, and confusion-matrix-based analysis for each detection profile and it should include a complete implementation-level disclosure of the neural architectures used in the monitoring profile, including encoder/decoder design, recurrent block structure, latent-space dimensionality, sequence settings, and training hyper parameters for both telemetry-oriented and firmware-oriented models, and, it should include full disclosure of the AI training workflow, including exact dataset provenance, sample sizes, preprocessing procedures, train/validation/test splits, epoch schedules, optimizer and hyper parameter settings, and explicit indication of whether transfer learning or

pre-trained models were used, also a fully described cyber-range methodology covering attack emulation tools, traffic-generation scenarios, firmware-oriented manipulation procedures, logging and SIEM collection pipelines, and explicit mapping between generated cyber events and evaluation metrics should be included.

Moreover, it should focus on the practical realization of low-power computation platforms for ML-based cyber monitoring, including hardware sizing, power budgeting, inference latency, and selective backup strategies for blackout-resilient deployment in SOHO environments.

Contributions of authors: conceptualization, methodology – **Serhii Zybin, Dmytro Prokopovych-Tkachenko;** formulation of tasks, analysis **– Dmytro Prokopovych-Tkachenko, Yuliia Khokhlachova;** development of model, software, verification **– Dmytro Prokopovych-Tkachenko, Rostyslav Palahusynets;** analysis of results, visualization **– Yuliia Khokhlachova, Anton Herasymenko;** writing – original draft preparation, writing – review and editing **– Serhii Zybin.**

Conflict of Interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, author ship or otherwise, that could affect the research and its results presented in this paper.

All the authors have read and agreed to the published version of this manuscript.

Financing

This study was conducted without financial support.

Data Availability

Data will be made available upon reasonable request.

Use of Artificial Intelligence

The authors confirm that they did not use artificial intelligence methods while creating the presented work.

References

1. 1. Wan, Y., & Cao, J. A Brief Survey of Recent Advances and Methodologies for the Security Control of Complex Cyber–Physical Networks. *Sensors*, 2023, vol. 23, no. 8, article no. 4013. DOI: 10.3390/s23084013.

2. Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. A survey of network-based intrusion detection data sets. *Computers & Security*, 2019, vol. 86, pp. 147–167. DOI: 10.1016/j.cose.2019.06.005.

3. Cavalcanti, M. M. L., Teixeira, G. W., Dinarte, H. A., Almeida, R. C., Boutaba, R., & Chaves, D. A. R. Enhancing the Efficiency of Resilient Multipath-Routed Elastic Optical Networks: A Novel Approach for Coexisting Protected and Unprotected Services with Idle Slot Reuse. *Sensors*, 2024, vol. 24, no. 12, article no. 3965. DOI: 10.3390/s24123965.

4. Ashraf, M., Idrus, S., Iqbal, F., Butt, R., & Faheem, M. Disaster-Resilient Optical Network Survivability: A Comprehensive Survey. *Photonics*, 2018, vol. 5, no. 4, article no. 35. DOI: 10.3390/photonics5040035.

5. Shen, G., Guo, H., & Bose, S. K. Survivable elastic optical networks: survey and perspective (invited). *Photonic Network Communications*, 2016, vol. 31, pp. 71–87. DOI: 10.1007/s11107-015-0532-0.

6. Korchenko, O., Korchenko, A., Zybin, S., & Davydenko, K. An approach for classifying sociotechnical attacks. *Radioelectronic and Computer Systems*, 2025, no. 2, pp. 230–252. DOI: 10.32620/reks.2025.2.15.

7. Mushtaq, S., Mohsin, M., & Mushtaq, M. M. A Systematic Literature Review on the Implementation and Challenges of Zero Trust Architecture Across Domains. *Sensors*, 2025, vol. 25, no. 19, article no. 6118. DOI: 10.3390/s25196118.

8. Zybin, S., Khoroshko, V., Khokhlachova, Y., & Kozachok, V. Approach of the Attack Analysis to Reduce Omissions in the Risk Management. *Proceedings of Selected Papers of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems*, 2021, vol. 2923, pp. 318–328. Available at: http://ceur-ws.org/Vol-2923/paper35.pdf (accessed 8 February 2026).

9. Salazar, L., Castro, S. R., Lozano, J., Koneru, K., Zambon, E., Huang, B., Baldick, R., Krotofil, M., Rojas, A., & Cardenas, A. A. A Tale of Two Industroyers: It was the Season of Darkness. *2024 IEEE Symposium on Security and Privacy*, 2024, pp. 312–330. DOI: 10.1109/sp54263.2024.00162.

10. Durumeric, Z., Ma, Z., Springall, D., Barnes, R., Sullivan, N., Bursztein, E., Bailey, M., Halderman, J. A., & Paxson, V. The security impact of HTTPS interception. *Proceedings of the 2017 Network and Distributed System Security Symposium (NDSS 2017)*, 2017. DOI: 10.14722/ndss.2017.23456.

11. Ashfaq, F., Wasim, M., Shah, M. A., Ahad, A., & Pires, I. M. Enhancing Security in 5G Edge Networks: Predicting Real-Time Zero Trust Attacks Using Machine Learning in SDN Environments. *Sensors*, 2025, vol. 25, no. 6, article no. 1905. DOI: 10.3390/s25061905.

12. Huang, J., Chen, Z., Liu, S.-Z., Zhang, H., & Long, H.-X. Improved Intrusion Detection Based on Hybrid Deep Learning Models and Federated Learning. *Sensors*, 2024, vol. 24, no. 12, article no. 4002. DOI: 10.3390/s24124002.

13. Han, D., Li, H., Fu, X., & Zhou, S. Traffic Feature Selection and Distributed Denial of Service Attack Detection in Software-Defined Networks Based on Machine Learning. *Sensors*, 2024, vol. 24, no. 13, article no. 4344. DOI: 10.3390/s24134344.

14. Oyucu, S., Polat, O., Türkoğlu, M., Polat, H., Aksöz, A., & Ağdaş, M. T. Ensemble Learning Frame-

work for DDoS Detection in SDN-Based SCADA Systems. *Sensors*, 2023, vol. 24, no. 1, article no. 155. DOI: 10.3390/s24010155.

15. Talpur, F., Korejo, I. A., Chandio, A. A., Ghulam, A., & Talpur, M. S. H. ML-Based Detection of DDoS Attacks Using Evolutionary Algorithms Optimization. *Sensors*, 2024, vol. 24, no. 5, article no. 1672. DOI: 10.3390/s24051672.

16. Nataraj, L., Karthikeyan, S., Jacob, G., & Manjunath, B. Malware images: visualization and automatic classification. *Proceedings of the 8th International Symposium on Visualization for Cyber Security (VizSec '11)*, 2011, article no. 4, pp. 1–7. DOI: 10.1145/2016904.2016908.

17. Chatterjee, B. C., Sarma, N., & Oki, E. Routing and Spectrum Allocation in Elastic Optical Networks: A Tutorial. *IEEE Communications Surveys & Tutorials*, 2015, vol. 17, no. 3, pp. 1776–1800. DOI: 10.1109/comst.2015.2431731.

18. Chatterjee, B. C., Ba, S., & Oki, E. Fragmentation Problems and Management Approaches in Elastic Optical Networks: A Survey. *IEEE Communications Surveys & Tutorials*, 2018, vol. 20, no. 1, pp. 183–210. DOI: 10.1109/comst.2017.2769102.

19. Bao, B., Yang, H., Yao, Q., Yu, A., Chatterjee, B. C., Oki, E., & Zhang, J. SDFA: A Service-Driven Fragmentation-Aware Resource Allocation in Elastic Optical Networks. *IEEE Transactions on Network and Service Management*, 2022, vol. 19, no. 1, pp. 353–365. DOI: 10.1109/tnsm.2021.3116757.

20. Lira, C. J. N., Almeida, R. C., & Chaves, D. A. R. Spectrum allocation using multiparameter optimization in elastic optical networks. *Computer Networks*, 2022, vol. 220, article no. 109478. DOI: 10.1016/j.comnet.2022.109478.

21. Mehrabi, M., Beyranvand, H., & Emadi, M. J. Multi-Band Elastic Optical Networks: Inter-Channel Stimulated Raman Scattering-Aware Routing, Modulation Level and Spectrum Assignment. *Journal of Lightwave Technology*, 2021, vol. 39, no. 11, pp. 3360–3370. DOI: 10.1109/jlt.2021.3065297.

22. Liu, Y., Feng, N., Shen, L., Lv, J., Yan, D., & Zhao, J. Fragmentation and ISRS-Aware Survivable Routing, Band, Modulation, and Spectrum Allocation Algorithm in Multi-Band Elastic Optical Networks. *Applied Sciences*, 2024, vol. 14, no. 11, article no. 4755. DOI: 10.3390/app14114755.

23. Abuelela, E., Żal, M., & Kabaciński, W. Simultaneous Connections Routing in Wavelength–Space–Wavelength Elastic Optical Switches. *Sensors*, 2023, vol. 23, no. 7, article no. 3615. DOI: 10.3390/s23073615.

24. Rodrigues, E., Cerqueira, E., Rosário, D., & Oliveira, H. Hybrid Routing, Modulation, Spectrum and Core Allocation Based on Mapping Scheme. *Sensors*, 2020, vol. 20, no. 21, article no. 6393. DOI: 10.3390/s20216393.

Received 15.09.2025, Received in revised form 28.05.2026
Accepted date 13.07.2025, Published date 31.07.2026

МЕТОД ПІДВИЩЕННЯ РІВНЯ ЖИВУЧОСТІ МЕРЕЖІ В УМОВАХ ГІБРИДНИХ КІБЕРАТАК ПІД ЧАС ВІДКЛЮЧЕНЬ ЕЛЕКТРОЕНЕРГІЇ

С. В. Зибін, Д. І. Прокопович-Ткаченко, Р. В. Палагусинець, Ю. Є. Хохлачова, А. А. Герасименко

Предметом *дослідження у статті є процеси проєктування SOHO-мереж (Small Office / Home Office) електронних комунікацій на основі компактного GPON (Gigabit-capable Passive Optical Network) mini OLT (Optical Line Terminal) з одним PON-портом (Passive Optical Network) до 32 абонентських терміналів ONU/ONT (Optical Network Unit/Optical Network Terminal).* ***Мета*** *роботи полягає у розробленні та валідації методу підвищення рівня живучості мережі в умовах гібридних кібератак під час відключень електроенергії. Дослідницькі* ***завдання*** *полягають у наступному. Розробити формальну модель живучості SOHO-доступу з урахуванням енергетичного бюджету ДБЖ та структури активних вузлів; формалізувати ризик гібридних подій, в яких збої енергопостачання поєднуються з кіберкомпрометацією; розробити методологію моніторингу IDS+SIEM (Intrusion Detection System+Security Information and Event Management) з машинним навчанням; провести порівняльний аналіз архітектур Ethernet та GPON; сформулювати практичні рекомендації щодо впровадження, діагностики та оптимізації управління відповідно до принципів Zero Trust та вимог управління інформаційною безпекою, враховуючи людський фактор та зручність використання засобів контролю в SOHO. Отримані наступні* ***результати.*** *Розроблено модель живучості, яка поєднує схему резервного живлення (оцінювання автономності ДБЖ), доступність активної схеми та ймовірнісну модель ризику компрометації компонентів управління, включаючи атаки на firmware-прошивку, пов'язані з вразливостями SNMP (Simple Network Management Protocol) та SSL/TLS (Secure Sockets Layer/Transport Layer Security) у вбудованому програмному забезпеченні. Було розроблено методологію моніторингу, яка інтегрує IDS та SIEM з класами аналітичних моделей на основі глибокого навчання і яку було представлено телеметричним аналізом типу AE+LSTM (Autoencoder + Long Short-Term Memory) та аналізом, орієнтованим на прошивку, типу CNN+LSTM (Convolutional Neural Network + LSTM). Було проведено порівняльне моделювання архітектур Ethernet Everywhere та GPON з пасивним розгалуженням для сценаріїв масштабування з'єднань 5–20–32. Наведено числові приклади розрахунків, порівняльні таблиці метрик та практичний алгоритм діагностики типових помилок встановлення (APC/UPC, IN/OUT сплітера,*

несумісність стандартів). Результати інтерпретовано з використанням принципів Zero Trust для малих мереж та визначено перспективи мультимодального ШІ для кореляції подій SIEM з артефактами прошивки та фізичною телеметрією оптичного каналу. Запропоновано практичні рекомендації щодо сегментації, політик оновлення та мінімізації привілеїв для контролю доступу в сегменті SOHO. ***Висновки.*** *Це дослідження визначає, що підвищення живучості мережі є важливим та актуальним завданням. Наукова новизна отриманих результатів полягає в наступному: розроблено інтегровану методологію моніторингу з машинним навчанням, яка забезпечує перехід від складу компонентів та операційних припущень до числових метрик живучості, доступності та виявлення; розроблено формальну модель живучості, що враховує енергетичний бюджет джерела безперебійного живлення та структуру активних вузлів; формалізовано ризик гібридних подій, за яких енергетичні збої поєднуються з кіберкомпрометацією.* ***Напрями подальших досліджень****: методологія локалізації відмов; методології, пов'язані з Zero Trust; мультимодальний аналіз ШІ; підтримка прийняття рішень в умовах обмежених ресурсів SOHO.*

Ключові слова: *кібербезпека; SOHO; блекаут; GPON; mini OLT; IDS, SIEM, Zero Trust.*

Зибін Сергій Вікторович – доктор техн. наук, професор, професор кафедри систем та технологій кібербезпеки, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

Прокопович-Ткаченко Дмитро Ігорович – канд. техн. наук, доц., завідувач кафедри кібербезпеки та інформаційних технологій, Університет митної справи та фінансів, Дніпро, Україна.

Палагусинець Ростислав Васильович – доктор наук з державного управління, кандидат економічних наук, доцент, заступник Постійного представника України при міжнародних організаціях у Відні, Австрія.

Хохлачова Юлія Євгеніївна, канд. техн. наук, професор, професор кафедри інженерії програмного забезпечення та кібербезпеки, Державний торговельно-економічний університет, Київ, Україна.

Герасименко Антон Андрійович, аспірант кафедри управління кібербезпекою та захистом інформації, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

Serhii Zybin – D.Sc., Professor, Professor at the Department of Cybersecurity Systems and Technologies, State University of Information and Communication Technologies, Kyiv, Ukraine,
e-mail: zysv@ukr.net, ORCID: 0000-0002-2670-2823, Scopus Author ID: 57202220667.

Dmytro Prokopovych-Tkachenko – Candidate of Technical Sciences, Associate Professor, Head of the Department of Cybersecurity and Information Technologies, University of Customs and Finance, Dnipro, Ukraine,
e-mail: omega2417@gmail.com, ORCID: 0000-0002-6590-3898.

Rostyslav Palahusynets – Doctor of Sciences in Public Administration, Candidate of Economic Sciences, Associate Professor, Deputy of the Permanent Representative of Ukraine to the International Organizations in Vienna, Vienna, Austria,
e-mail: palachros@umsf.edu.ua, ORCID:0000-0003-1399-7164.

Yuliia Khokhlachova – Candidate of Technical Sciences, Professor at the Department of Software Engineering and Cybersecurity, State University of Trade and Economics, Kyiv, Ukraine,
e-mail: yuliiahohlachova@gmail.com, ORCID 0000-0002-0787-5112.

Anton Herasymenko – PhD student at the Department of Cybersecurity and Information Protection Management, State University of Information and Communication Technologies, Kyiv, Ukraine,
e-mail: anton.hrsmnk@gmail.com, ORCID: 0009-0008-4475-2040.