Received 20 December 2025, accepted 27 May 2026, date of publication 30 June 2026
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.25.2.4656

Ensuring Continuity of Office IT Infrastructure Operation in Crisis Situations

OLEKSANDR KORCHENKO[1], YULIIA KHOKHLACHOVA[2], DMYTRO PROKOPOVYCH-TKACHENKO[3], TETYANA RUDYANOVA[3], ROSTYSLAV PALAHUSYNETS[3], DMYTRO SHCHYTOV[3]

[1]State University of Information and Communication Technologies, 03110, Kyiv, Ukraine
[2]Department of Software Engineering and Cybersecurity State Universityof Trade and Economics, 02156, Kyiv, Ukraine
[3]Department of Computer Science and Software Engineering University of Customs and Finance, 49000, Dnipro, Ukraine
(e-mail: agkorchenko@gmail.com, yuliiahohlachova@gmail.com, omega2417@gmail.com, rudyanova@umsf.edu.ua, palachros@umsf.edu.ua, Schitov@umsf.edu.ua)

Corresponding author: Yuliia Khokhlachova (e-mail:yuliiahohlachova@gmail.com)

ABSTRACT Blackouts have transformed office electronic communications into a system in which power loss immediately causes degradation of access to documents, services, and coordination channels. The purpose of this study is to substantiate and validate a network reconstruction architecture capable of maintaining business-critical functions during prolonged outages.

A comprehensive solution is proposed based on a self-healing Mesh topology, a dual-WAN configuration with primary GPON access and Starlink backup, and a local solid-state low-power edge server providing DNS/DHCP, authentication, file services, and event logging (minimal SIEM/IDS).

The power subsystem is implemented using a 12 V $LiFePO_4$ battery with a Battery Management System (BMS) and a simple timer mechanism for disconnecting non-critical loads during off-hours, thereby reducing average power consumption and depth of discharge.

Evaluation metrics include autonomy duration, WAN failover time, availability of local services, and energy consumption. Calculated scenarios and experimental tests were conducted for GPON failures and individual Mesh node outages.

For a 2000 Wh battery, the projected autonomy is 22.99 hours in daytime mode and 31.75 hours in nighttime mode, with energy savings of 240 Wh during a 10-hour disconnection of Group B loads. Failover to Starlink required 10–20 seconds, while Mesh route reconstruction took less than 3 seconds.

The practical contribution lies in the load-segmentation rules (Groups A/B), hop-count minimization, and preparation for future Zero Trust segmentation of critical services. Unlike UPS-centric approaches ("power everything"), the proposed design manages priorities: network core, routing, VPN, and local data remain available, while peripheral consumers are disconnected in a controlled manner.

The study demonstrates reduction of single points of failure and provides recommendations for rapid communication recovery in small and medium-sized offices. Additional requirements for logging and basic segmentation are introduced to simplify operation and resilience auditing in crisis conditions.

KEYWORDS blackout, office network, mesh relay, dual-WAN, GPON, Starlink, low-power edge server, $LiFePO_4$, energy management, fault tolerance, Zero Trust.

I. INTRODUCTION

Negative macro-level impacts on the country's energy sector (large-scale damage to generation, transmission nodes, power deficits, emergency repairs, and forced consumption limitation schedules) transform power supply from a "background" condition of ICT functioning into a dominant risk factor. Under such conditions, a blackout becomes not a singular event, but a recurring mode in which organizations must plan network operations in categories of autonomy hours, charging windows, and service prioritization. The humanitarian consequences of prolonged outages and their systemic nature, particularly due to strikes on energy

infrastructure, are documented by international institutions; it is separately emphasized that new waves of attacks can cause prolonged emergency blackouts with severe consequences for the civilian population and critical services.

Electronic communications in such scenarios are the "nervous system" of management and recovery: without communication channels, the coordination of emergency works, logistics, public services, financial transactions, and business process continuity degrade. Therefore, telecommunications energy resilience (hereinafter – network energy resilience) is appropriately interpreted as the ability of network infrastructure to maintain target availability and a minimally acceptable quality of service under conditions of limited/intermittent power supply, ensuring controlled degradation (graceful degradation) rather than chaotic failure.

At the level of the electronic communications sector, dependence on power supply and the need for a minimum level of redundancy and practices to increase resilience to outages are directly viewed as a critical reliability factor. At the same time, emergency experience shows that "installing an Uninterruptible Power Supply (UPS) and forgetting about it" is insufficient, as bottlenecks arise at the intersection of energy and network architecture (single points of failure, inefficient consumption profiles, lack of planned shedding of non-critical loads, dependence on cloud services). International recommendations for emergency telecommunications planning emphasize the necessity of a scenario-based approach, risk assessment, and recovery procedures, where power redundancy and network architecture are considered within a single management contour.

The aim of the study is to develop and substantiate an applied architecture for the restoration of an office network capable of ensuring the continuity of key digital services under conditions of recurring blackouts and communication channel degradation by combining:

- Wireless Mesh topology with route self-healing
- Dual-WAN Internet access redundancy with a primary channel based on Gigabit-capable Passive Optical Network (GPON) and a backup Starlink satellite channel
- A local solid-state low-power edge server as an "island" of basic network and service functions
- Autonomous power supply on a lithium-iron-phosphate ($LiFePO_4$) 12V battery with a simple mechanism for the planned disconnection of non-critical loads.

To achieve this goal, the following tasks must be solved: (1) define architectural requirements for office network resilience in blackout mode; (2) design Mesh coverage minimizing the number of "hops" for critical services; (3) formalize the dual-WAN channel switching policy with quality parameter control; (4) substantiate the energy model, load profiles, and rules for distributing consumers into critical/non-critical groups; (5) set evaluation metrics (autonomy, failover time, service availability, average energy consumption) and verify them in test scenarios.

The scientific novelty of this study lies in the development of an integrated resilience-oriented model for small and medium-sized office IT infrastructure operating under recurring blackout conditions. Unlike approaches that consider backup power supply, Internet channel redundancy, wireless coverage, or local service autonomy as separate technical tasks, the proposed model combines these components into a single managed architecture with coordinated network, service, and energy layers. The main contribution of the paper consists of four interrelated elements:

1. an integrated Mesh + dual-WAN GPON/Starlink + local edge server architecture for maintaining minimum critical services during communication and power degradation;
2. a formalized A/B load-prioritization scheme that separates continuously powered critical components from non-critical consumers disconnected by timer;
3. an energy autonomy model based on $LiFePO_4$ capacity, average power consumption, and controlled load shedding;
4. a validation methodology based on reproducible crisis scenarios, including GPON failure, Mesh node failure, night energy-saving mode, and complete blackout operation.

Thus, the novelty of the research is not only the use of individual known technologies, but their coordinated integration into a practical office infrastructure continuity model with measurable resilience indicators: autonomy duration, WAN failover time, Mesh route recovery time, service availability, and energy savings.

The object of the study is the office network infrastructure of an organization under conditions of recurring power outages and telecommunication channel instability. The subject of the study consists of methods for architectural redundancy, energy management, and controlled service degradation, as well as mechanisms for the self-organization of wireless Mesh fragments and access redundancy (GPON/Starlink) within the resource constraints of a small/medium office

II. OVERVIEW OF EXISTING SOLUTIONS

Office network resilience in a power deficit mode logically relies on two groups of research: (a) network topologies/protocols that reduce dependence on centralized nodes, and (b) energy models and power management methods that ensure predicted autonomy. In the context of wireless mesh networks presented in [1], it was shown that software-defined approaches to the control plane can increase configuration flexibility and route recovery in Mesh systems. The authors demonstrated configuration flexibility but did not account for failure scenarios under power constraints, which is a critical gap for this study. Optimization of router and coverage node placement based on heuristic/evolutionary methods (specifically maximum entropy genetic algorithms), described in [2], allows for improving coverage quality and reducing resource consumption with a limited number of nodes, but this approach assumes static power availability and does not account for scenarios with battery charge limits. The computational costs of the algorithm may be impractical for rapid redistribution during crisis conditions.

Experimental comparisons of routing protocols on practical testbeds (e.g., single-board computers), presented in study [3], demonstrate significant dependence of latency and stability on protocol choice and environmental conditions. The Pi 4 platform is realistic, but this study lacks energy consumption metrics. For scenarios requiring local data processing near the user, reflected in publication [4], the convergence of Mesh with edge computing and approaches like fog architectures is relevant, increasing service autonomy during global backbone degradation. Fog/NDN integration accounts for service locality, but the article did not quantitatively define recovery time after failure and did not confirm performance under degraded global network conditions. Named Data Networking adds protocol complexity, which may hinder rapid recovery. Practically important is also the identification of "critical

edges" and components whose failure disproportionately reduces network reliability, which directly supports the task of minimizing single points of failure described in [5]. Resilience metrics are reliable, but detection algorithms assume network-wide visibility, which may not exist during partial power outages. Real-time application is doubtful when the monitoring infrastructure itself is disrupted. In parallel, research on hybrid data transmission systems under interference conditions demonstrates the feasibility of multi-channel redundancy as a principle (not just for transport, but also for Internet access). The concept of hybrid transmission proposed in [6] confirms dual-channel redundancy, although the study did not address the recovery time of the terrestrial-satellite system or session continuity. Regarding external link redundancy, the role of integrating terrestrial and satellite segments is growing: the analysis of routing challenges and "6G–satellite" integration technologies proposed in study [7] emphasizes the promise of seamless access hybridization. The focus on 6G is future-oriented, extending beyond current Starlink/GPON implementation. There is a lack of empirical data regarding actual recovery performance after failure or operational limitations of existing LEO constellations. Practical cases of satellite Internet application in crisis scenarios (specifically using Starlink) were described in [8], demonstrating the value of a backup channel for management and coordination, but simultaneously pointing to the need for competent switching policy and session management. This study focused on evacuation scenarios rather than continuous office operation. Also, throughput reduction under load was not quantified, and a cost-benefit analysis for permanent redundancy was not provided. For applied backup power systems, optimized energy management models and neural network control in hybrid UPS schemes with renewable sources are important, demonstrating the potential for "smart" consumption profile management in work [9]. Advanced energy management methods were presented here, but the integration of photovoltaic systems and neural network complexity go beyond the proposed simple timer-based approach. Optimization benefits may not justify implementation costs for small/medium offices. Real-time training requirements are impractical during power outages.

Modern reviews of $LiFePO_4$ technology emphasize its suitability for cyclic modes, safer profile, and prospects for improved characteristics. Analysis of battery chemistry justifying the choice of $LiFePO_4$ for cyclic operation proposed in [10] is thorough but does not provide specific discharge curves or temperature dependencies critical for autonomy calculations. Discussion of the safety profile is valuable, but there is a lack of quantitative data on failure rates. Reviews of battery health assessment methods and BMS approaches presented in [11] show that autonomy forecasting depends on correct indicators and degradation models. However, machine learning approaches require historical data unavailable in newly deployed systems. The review summarized methods but did not recommend specific algorithms for resource-constrained edge scenarios. PUE and related metrics were well-established and presented in [12], but they were designed for large facilities. Applicability to small office servers at the edge is limited. Specifically, work [12] did not account for measurement overhead—the instruments themselves consume energy, which matters at this scale. Visualization approaches are relevant for monitoring implementation. However, energy dashboard workloads for high-performance computing proposed in [13] differ fundamentally from office services. A dashboard prototype requires significant development effort, which may not align with rapid deployment needs in crisis conditions. Work [14] presented a multi-layered approach to reliability and security that conceptually aligns with the study's segmentation principles. However, the heterogeneous network model assumes diverse infrastructure that may not exist in small offices. Implementation complexity is thus underestimated. Resource allocation algorithms provided in work [15] are mathematically sound but assume predictable workloads. Dynamic provisioning strategies may be too complex for the proposed timer-based A/B approach. Work [16] proposed edge computing focused specifically on IoT device density rather than service continuity during infrastructure degradation. Edge distribution concepts support the justification for local servers, but IoT-specific optimizations (ultra-low power protocols) cannot be directly transferred to office productivity services. Work [17] addressed fundamental scaling issues but at the levels of computational intensity irrelevant to typical office workloads. The theoretical basis is rigorous, but practical application is limited. Office servers rarely require parallel computing optimization. Resilience to radio interference is becoming increasingly important given the potential for disruption during conflicts. Cluster approaches in work [18] partially align with mesh principles, but WSN energy constraints (battery-powered sensors) differ from powered mesh nodes. Therefore, interference scenarios deserve more attention in the main body of the article. The energy contour of network resilience is closely linked to the choice of storage technology and power management. Issues of capacity sizing and depth-of-discharge modes in microgrids (e.g., wind) were systematized in optimal dispatch and sizing tasks in publication [19]. Issues of LEO segment parameters and their experimental validation on testbeds (multi-constellation) in work [20] are important for correct modeling of latency/availability of satellite backup in real conditions. The measurement campaign provides latency/availability data but does not test degraded conditions or priority traffic shaping. A broad survey presented in publication [21] provides context but lacks specificity for crisis resilience scenarios. Optimization models assume normal operating conditions with performance/energy trade-offs, not emergency triage situations. This precedes the formation of urgent energy resilience. Ultra-low energy LoRa proposed in article [22] demonstrates communication minimums, confirming that connectivity is possible under severe energy constraints. However, LoRa throughput (kbps) is insufficient for office productivity. Resilience principles can be applied even if the technology itself is not. Additionally, interest is growing in assessing the "second life" of commercial $LiFePO_4$ batteries and their applicability after primary use. Capacity fade models presented in [23] help predict autonomy degradation in real-world conditions over multi-year use. But recommendations on when to decommission batteries and when to refurbish them were not provided. Fiber optic network design principles reviewed in [24] are sound but assume stable power on the provider side. Here lies a hidden vulnerability revealed during power outages, and requirements for backup power for ONT and OLT equipment should also be emphasized. Interpretable AI for battery health assessment is valuable for autonomy forecasting, so the generalized additive model in the work combines accuracy and transparency [25]. But it requires training data for all discharge profiles, which accumulate only after repeated outage cycles. Industrial Mesh

network deployment in study [26] is also actively optimized by metaheuristics to improve energy efficiency and link quality. However, an industrial network (stationary installations, harsh conditions) differs from office scenarios. The transient trigonometric Harris Hawks optimizer is computationally resource-intensive for real-time reconfiguration. Work [27] presented cognitive radio concepts (spectrum sensing, dynamic allocation) that improve resilience to interference and jamming, while multicast optimization reduces redundant transmissions. However, cognitive radio hardware requirements exceed typical office equipment capabilities, and licensing restrictions may apply.

Despite a broad scientific base, a gap remains in system design for small and medium offices in the applied plane, which simultaneously combines: (1) Mesh coverage as a mechanism to reduce dependence on central nodes; (2) dual-WAN with an optical main channel (GPON) and satellite backup; (3) a local low-power edge server as an "island" of services during Internet degradation; (4) energy management with load distribution into critical/non-critical groups and planned shedding of non-critical consumers. In the context of national energy instability, such integration is not an "option for comfort," but a condition for maintaining organizational manageability during blackouts, which defines the relevance of the proposed study.

A. METHODS

The article applies a multi-level approach:

1. Architectural decomposition of the solution into access/routing subsystems, wireless coverage, local edge service core, and power supply;
2. Formalization of operation rules and failure modes for each subsystem;
3. Construction of evaluation models (autonomy, failover time, local service availability, average energy consumption);
4. Verification on test scenarios reproducing typical failures (GPON loss, Mesh node failure, transition to night economy mode).

The choice of Mesh topology and self-healing principles is substantiated by the results regarding control flexibility in Mesh networks and the impact of protocols/environmental conditions on latency and route stability [1, 3], as well as approaches to optimizing coverage node placement under resource constraints [2] and an analysis of critical components whose failure disproportionately reduces reliability [5]. The method of constructing the dual-WAN contour relies on the principle of multi-channel redundancy and modern approaches to integrating terrestrial and satellite segments, which allows increasing availability in crisis modes through switching policies and quality control [7, 8], while the basic optical access model (GPON/PON) is considered the main stable channel given power availability [24]. The local solid-state low-power edge core is introduced as a means of reducing dependence on the external backbone (local DNS/DHCP, authentication, files, logging, and a minimal SIEM/IDS contour), which aligns with the edge/fog computing ideology for increasing service autonomy [4]. The energy part of the methods is based on $LiFePO_4$ characteristics for cyclic modes and approaches to battery management/assessment (BMS), allowing for correct modeling of available energy and autonomy forecasting [10, 11]; additionally, principles of energy profile measurability are used as a prerequisite for managed energy management [12].

III. CONCEPTUAL MODEL AND RESEARCH DESIGN

The research methods are developed as an engineering and experimental cycle, focused on achieving controlled degradation of services in the mode of repeated blackouts and degradation of access channels. The conceptual scheme (Fig. 1) captures the cause-and-effect chain: blackouts create a systemic risk for the office infrastructure due to the presence of single points of failure (Single Point of Failure, SPOF), energy inefficiency, lack of a backup external communication channel and excessive dependence on cloud services. The target state is described as network reconstruction with self-healing coverage, access redundancy and a local "island" of services. The methodological framework of the work (Fig. 2) is implemented as a six-stage cycle: problem analysis, architecture design, energy modeling, validation on test scenarios, analysis of the results, and formulation of practical recommendations. The methodological framework of the study is developed as an engineering and experimental cycle, focused on ensuring the continuity of the office network under conditions of repeated blackouts and degradation of access channels.

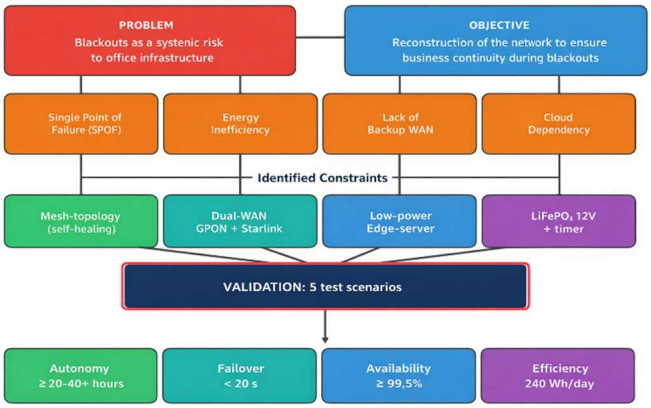


Figure 1. Conceptual diagram of the study of restoring a resilient office network during blackouts.

Within the framework of this approach, the analysis of the problem and infrastructure vulnerabilities, the design of a resilient network architecture, energy modeling and autonomous power planning, validation of solutions on test scenarios, as well as the analysis of the results obtained with the formulation of practical recommendations for implementation are sequentially performed.

Figure 1 shows the logic of the transition from the problem statement to the verified results. The initial premise is blackouts as a systemic risk for the office infrastructure, which manifests itself through typical limitations: the presence of a single point of failure (SPOF), energy inefficiency, the absence of a backup external channel (WAN) and critical dependence on cloud services. The goal of the study is defined as the restoration of the network for continuous operation during a blackout based on a combination of architectural solutions that eliminate the specified limitations: self-healing mesh topology for stable coverage, dual-WAN access (GPON as the main and Starlink as a backup) for fast switching, local energy-efficient edge server as an "island" of critical services, as well as autonomous $LiFePO_4$ 12 V power supply with timer shutdown of non-critical loads. The central element of the scheme is validation on test scenarios, which provides reproducible verification of the architecture's operability. The effectiveness of the solution

is interpreted through target indicators, in particular, autonomy of operation, switching time (failover), achievable availability of services and the energy effect of controlled consumption limitation during non-working hours.

The research methodology is built as a combination of system engineering network design and experimental validation of its stability in power supply and access channel degradation regimes. Such logic is needed to move from problem description to reproducible verification: solutions are not only declared, but also confirmed by measurable metrics and failure scenarios.

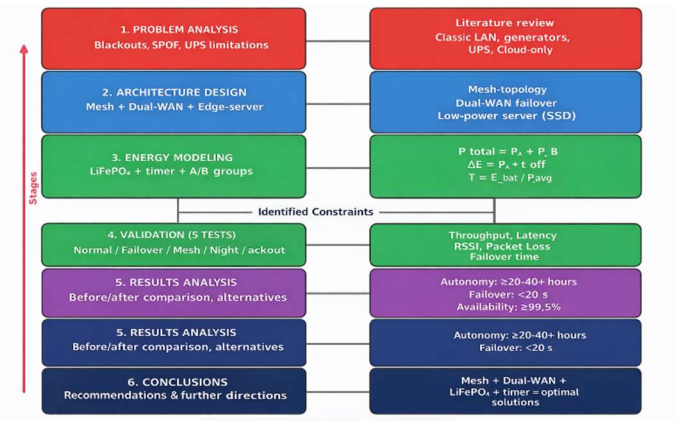


Figure 2. Research methodology (IMRAD)

Figure 2 presents the methodological framework of the work in the IMRAD format as a sequential engineering and experimental cycle of six stages: problem analysis, architecture design, energy modeling, validation on test scenarios, analysis of the results, and formulation of practical recommendations. The diagram shows that the research begins with the formation of the context and requirements (what exactly breaks during blackouts and why), then moves on to the architectural design and energy justification of autonomy, after which the solution is tested for failures, and the obtained measurements are interpreted and converted into applied recommendations for implementation. The IMRAD logic in this scheme provides simple "traceability" from problem formulation to the results: each subsequent stage builds on the previous one and provides artifacts that can be tested, repeated, and used to compare alternative solutions in similar operating conditions.

IV. GENERAL SOLUTION ARCHITECTURE

A. LOGIC DIAGRAM

The architecture is built around the principle of "24/7 core + managed edge disconnection": critical network functions (routing/protection, basic Wi-Fi coverage, local services) operate continuously, while non-critical consumers are switched to a planned shutdown mode to reduce average power. External access is implemented as two channels (dual- WAN): the main one is optical access GPON (Gigabit-capable Passive Optical Network) via an optical network terminal (Optical Network Terminal, ONT), backup – Starlink satellite access; switching is performed by a router/firewall with quality control policies and tunneling (Virtual Private Network, VPN. Inside the office, Wi-Fi coverage and stability is provided by a wireless mesh topology (Mesh) with a minimization of the number of "hops" for critical nodes and the ability to self-recover routes. The architecture of the rebuilt office network is built on the principle of "24/7 core + controlled peripheral shutdown", when critical network functions (routing/protection, basic Wi-Fi coverage, local services) operate continuously, and non-critical consumers can be scheduled to be turned off to reduce average power. External access is implemented as dual-WAN: the main channel is GPON via ONT, the backup is Starlink, and switching and security policies are provided by a router/firewall with VPN, segmentation, and NAT.

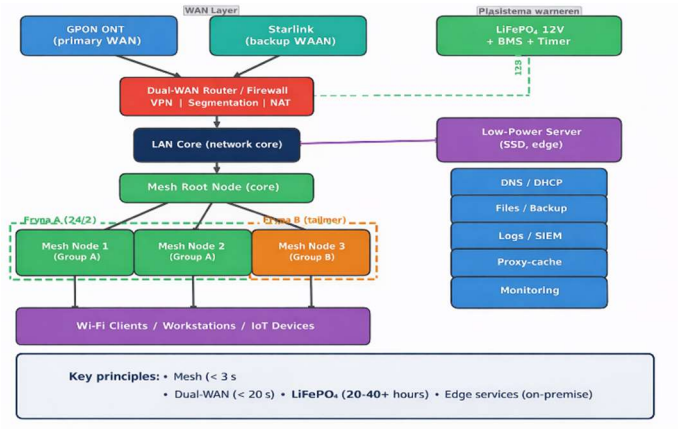


Figure 3. Logical diagram of the solution architecture (GPON/Starlink – dual-WAN – Mesh – edge).

Figure 3 shows the logical connections between the access subsystems, LAN core, Mesh coverage, local edge service core and power loop. At the upper level (WAN), two independent channels operate: GPON ONT as the primary WAN and Starlink as a backup WAN with automatic failover; both are connected to a Dual-WAN Router/Firewall that implemets switching policies, VPN tunneling, segmentation and NAT, after which the traffic is aggregated into the LAN Core. Inside the office LAN Core powers Mesh Root Node, from which a cellular infrastructure of Mesh nodes with relaying and self-healing routes is deployed, supporting Wi-Fi connectivity of clients/workstations/IoT. Energy management is implemented by dividing consumers into groups: group A is critical and operates 24/7 (ONT, Router /FW, Mesh core with 1–2 nodes, server), while group B is non-critical and is turned off by a timer during non-working hours (peripheral Mesh, guest Wi-Fi, PoE consumers). In parallel to the LAN Core, a low-power server (SSD) is connected as a local "island" of services that supports DNS/DHCP, file functions, logging, monitoring, and proxy cache, which reduces dependence on the external Internet during channel degradation. The power subsystem is based on $LiFePO_4$ 12 V with BMS as a long-term reserve, and a timer (time relay) acts as a group B cut-off mechanism to save energy. According to the validation results for this architecture, it was recorded that the failover time on Starlink was 10-20 s, and the Mesh route reconstruction was less than 3 s, which confirms the operability of the approach in crisis modes.

B. FUNCTIONAL ROLES OF COMPONENTS

The roles of the architecture elements are defined from the perspective of ensuring service continuity and minimizing SPOF: the network core implements access, segmentation, and channel switching policies; Mesh ensures coverage preservation in the event of a single node failure; the local

solid-state server forms an "island" of services and event logging for a minimal incident detection loop (Intrusion Detection System, IDS) and security event management (Security Information and Event Management, SIEM).

Table 1. Functional roles of architecture components

Component	Role in architecture	Description / Purpose
GPON ONT	Primary WAN	Stable channel with low latency; requires external power supply from provider
Starlink	Backup WAN	Autonomous satellite channel; automatic failover
Dual-WAN Router/Firewall	Network core	Switching policies, VPN, segmentation, NAT
Mesh nodes (Root+N)	Wireless coverage	Retransmission + self-recovery of routes
Low-power Server (SSD)	Edge services	DNS/DHCP, files, logs, monitoring, proxy cache
$LiFePO_4$ 12 V +BMS	Autonomous power supply	Long-term reserve with controlled charging
Timer (time relay	Energy management	Group B cut-off during non-working hours

Table 1 summarizes the functions performed by each element of the proposed architecture from the perspective of service continuity and single point of failure (SPOF) minimization: the network core is responsible for access policies/segmentation and channel switching, the Mesh maintains coverage in the event of a single node failure, and the local solid-state server forms an "island" of services and event logging for a minimal IDS/SIEM circuit. In the external access (WAN) part, the main channel is the GPON ONT, which provides a stable connection with low latency, but critically depends on the availability of external power supply from the provider. Redundancy is provided by Starlink as an autonomous satellite channel that takes over communication in the event of degradation/loss of the primary channel through automatic failover. The "brain" of this circuit is the Dual-WAN Router/Firewall: it implements the switching logic, VPN tunneling, segmentation and NAT, i.e., it simultaneously supports availability and security control when changing the channel. For internal coverage stability, the table highlights Mesh nodes (Root + N) as a wireless access subsystem: their role is to relay traffic and self-restore routes so that if one node fails, the office does not lose connection "with an entire segment", but only switches to an alternative route. A separate block is allocated to the Low-power Server (SSD) as the edge core of services: it holds local basic functions (DNS/DHCP), file operations, logs, monitoring, and proxy cache. This means that even with WAN problems in the office, a minimally functional "local infrastructure" remains for operation and monitoring of the systems' status. The energy circuit in the table is described by two elements. $LiFePO_4$ 12 V + BMS provides long-term autonomous reserve with controlled charging, i.e., provides predictable autonomy and degrades less in cyclic modes. Timer (time relay) performs the function of practical energy management: it cuts off the non-critical "group B" during non-working hours, reducing average consumption and extending battery life without losing critical network functions.

Table 2. Power subsystem load grouping

Group	Type	Equipment	Regime
A	**24/7 critical**	GPON ONT, Router /FW, Mesh (core, 1-2 nodes), Server	*Never turns off*
B	**By timer**	Peripheral Mesh, guest Wi-Fi PoE consumers	*Turns off during non-working hours*

Table 2 explains the logic of power management by dividing all consumers of the power subsystem into two categories with different operating priorities. It shows that group A is defined as 24/7 critical and includes GPON ONT, router/ firewall, Mesh core (root node and 1–2 nodes) and local server; this group is never turned off, as it is the one that supports the basic network functionality: WAN access (if available), routing and security policies, minimum required Wi-Fi coverage and local services. Group B in the table is marked as operating on a timer: it includes peripheral Mesh nodes, guest Wi-Fi, and PoE consumers, and it is turned off during non-working hours. The point of this distribution is controlled degradation: during periods of limited power supply, the "backbone" of the network is maintained (group A), and everything that does not affect critical functions is planned to be cut off (group B). This reduces the average power consumption and increases the predicted autonomy of the system without losing key services in a crisis mode.

C. MESH WIRELESS COVERAGE SUBSYSTEM

Mesh coverage design methods include: (i) selecting a root node with maximum radio coverage and a minimum number of "hops" to the network core; (ii) limiting the length of the relay chain for critical services (no more than 2–3 hops), which reduces delays and the likelihood of cascading degradation; (iii) checking self-healing routes when one node is lost; (iv) field measurement of signal level and throughput (RSSI/throughput) to identify risk areas. From a resilience perspective, the key factor is not a peak speed, but maintaining the minimum required quality of service (QoS) during partial failures.

D. DUAL-WAN EXTERNAL ACCESS RESERVATION: GPON + STARLINK

The failover algorithm is based on continuous monitoring of the "health" of the main channel (reachability of control nodes, delay, packet loss) and on route switching rules in case of degradation below threshold values. The chosen approach corresponds to the practice of hybridization of terrestrial and satellite segments, where the satellite channel acts as a reserve for crisis modes, and the optical channel as a base during regular power supply.

E. LOCAL EDGE CORE SERVICES AND EVENT LOGGING

A local solid-state low-power server is considered as an element of autonomy: even in the absence of the Internet, basic network functions (DNS/DHCP), authentication/accounting (AD-like mechanisms), local repositories and file services are preserved. A minimum contour of event logging and initial anomaly detection (IDS/SIEM) is separately highlighted, which allows tracking failures/incidents and restoring causal

chains after a blackout.

F. ENERGY MODELING AND POWER SUBSYSTEM

Energy methods are based on the use of $LiFePO_4$ 12 V as a storage medium with cyclic operation and increased safety, as well as a battery management system to control charge/discharge modes and reduce the risk of degradation. Practical energy management is implemented through the division of consumers into groups A/B and timer shutdown of group B during non-working hours, which reduces the average power and increases the predicted autonomy (Table 2).

G. PERFORMANCE EVALUATION METRICS

The assessment of the effectiveness of network restoration is performed based on a group of metrics that reflect both network quality (latency, throughput, RSSI) and service continuity (availability, switching time), and energy suitability (average power, autonomy). The approach is consistent with the principle of measurability as a necessary condition for manageability under resource constraints. The list of metrics is given in Table 3.

Table 3. Performance evaluation indicators

Metrics	Marking	Definition	Target value
Autonomy	T, h	T = E_bat / P_avg	**The more the better**
Failover time	t_sw, s	From GPON loss to stable Starlink	**Target: <20 s**
Availability of services	A, %	uptime / (uptime + downtime) × 100	**Target: ≥ 99.5%**
Power consumption	P, W	Average capacity per day	**The less is the better**
Wi-Fi coverage	RSSI, dBm	Signal level on client devices	**Target: > -65 dBm**
Network throughput	Mbps	Throughput under load	**Measured by iperf3**

Table 3 summarizes the indicators used to evaluate the proposed architecture in terms of energy autonomy, communication recovery, service continuity, and wireless access quality. The selected metrics make it possible to compare normal operation and degraded modes using measurable parameters rather than qualitative assumptions. Autonomy and power consumption characterize the energy suitability of the solution, while failover time and service availability show whether the infrastructure can preserve critical functions during WAN degradation. RSSI and throughput are used to confirm that Mesh recovery does not only restore connectivity formally, but also maintains an acceptable level of wireless service quality.

V. RESULTS

We present a summary of the calculations and experimental measurements obtained during the validation of the proposed architecture on test scenarios; the values presented are interpreted through the given metrics (in particular, the communication quality/recovery indicators, autonomy T and average power P_avg) and compared with the initial state of the infrastructure. Practical testing was performed on an implemented stand deployed on the basis of a training laboratory; the diagrams in Figures 4–6 capture this physically implemented configuration and its decomposition into subsystems. The results are further presented in relation to five validation scenarios (regular mode, GPON loss with switching to Starlink, failure of one Mesh node, night energy saving mode with group B shutdown, complete blackout on battery power), which ensures reproducibility of the test and correct comparison of network operating modes.

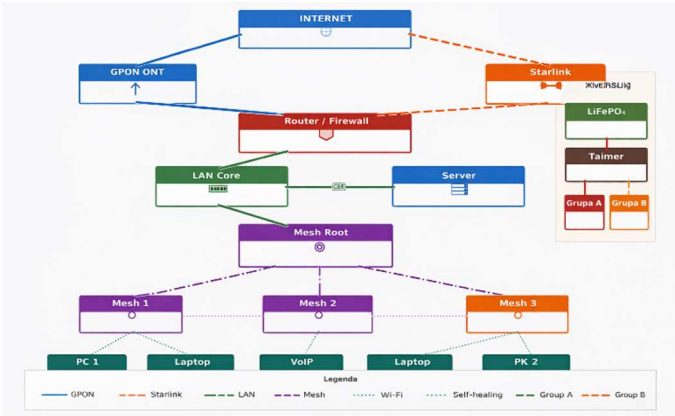


Figure 4. Summary logical network diagram (WAN → Core → Mesh → clients + power).

Figure 4 presents the implemented laboratory configuration as an end-to-end chain from external access to clients and power supply. The diagram shows that the architecture was tested as an integrated system rather than as separate network and energy components. This is important for validation because failures in one layer, for example WAN loss or power limitation, can influence the availability of services in other layers. The figure therefore provides the structural basis for interpreting the subsequent failover, Mesh recovery, and autonomy measurements.

Figure 5 details the top level of the architecture, where external access and network security policies are formed. Two independent WAN channels (main GPON and backup Starlink) are shown, connected to a Dual-WAN Router/Firewall, which performs routing, access control and can apply VPN/traffic segmentation.

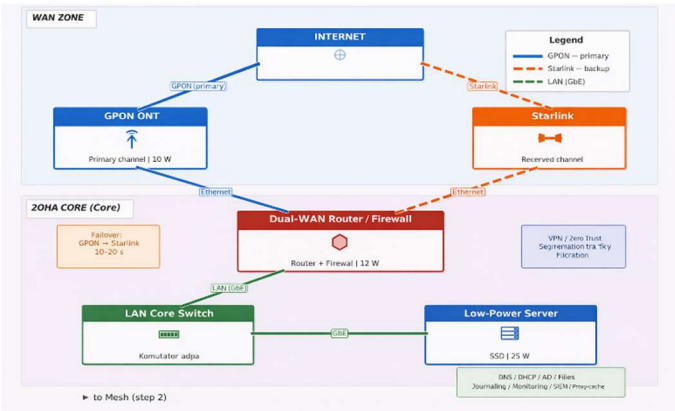


Figure 5. WAN channels and network core (GPON + Starlink → Dual-WAN Router / Firewall → LAN Core + Server).

Figure 5 details the WAN and network-core segment used to evaluate external access continuity. The key point of this configuration is that failover is performed at the router/firewall level, while local services remain available in the LAN core. Therefore, the measured GPON → Starlink switching time reflects not only the presence of a backup channel, but also the ability of the architecture to preserve the operational core during degradation of the primary Internet connection.

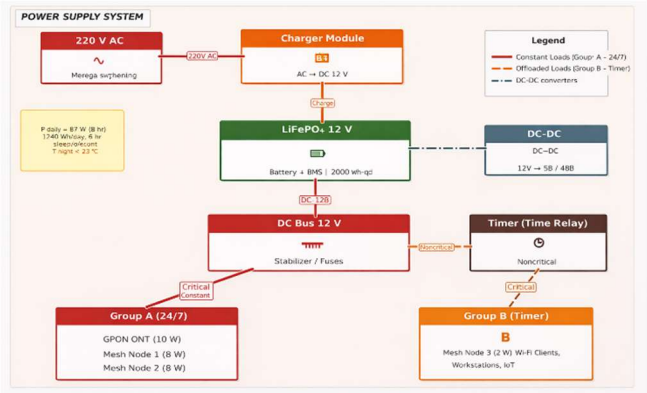


Figure 6. $LiFePO_4$ 12 V power subsystem with a cut-off timer for non-critical loads (groups A/B).

Figure 6 illustrates the power subsystem used for autonomy testing. The scheme separates continuously powered critical loads from non-critical loads disconnected by timer during off-hours. This configuration was used to verify whether controlled load shedding can reduce average power consumption without interrupting core network and local service functions. The values shown in the figure provide the basis for the autonomy calculations and for comparing daytime and nighttime energy profiles.

VI. EXPERIMENTAL PLAN AND VALIDATION

The validation was performed as a set of five test scenarios that reproduce typical failures and operating modes: normal mode, loss of the main channel (GPON), failure of one Mesh node, night energy saving mode, complete blackout on battery power. This scenario structure corresponds to the approaches of emergency planning and assessment of telecommunications resilience during power supply degradation. The experimental plan is given in Table 4.

Table 4. Experimental design/ validation

No.	Test	Conditions	What is measured?
1	**Normal operation**	The network is under load, electricity is available	Baseline throughput, latency, RSSI
2	**GPON discon-nection**	Primary channel unavailable → failover Starlink	t_sw, Starlink channel quality
3	**Mesh node failure**	Shutdown 1 node → rerouting	Recovery time, packet loss
4	**Night mode**	Timer turns off group B	Core availability, energy saving
5	**Complete blackout**	Power supply only $LiFePO_4$	T autonomy, P_avg

Table 4 defines the validation logic of the study. The selected scenarios reproduce the main degradation modes expected in office infrastructure under crisis conditions: loss of the primary WAN channel, local Mesh node failure, planned energy-saving operation, and complete blackout. The purpose of this experimental plan is to check whether the architecture provides controlled degradation rather than uncontrolled service interruption. The measurements obtained in these scenarios allow the network and energy parts of the solution to be evaluated within a single resilience framework.

Table 5. Calculation of power consumption of components

Component	Power (W)	Number	Total (W)
GPON ONT	10	1	**10**
Dual -WAN Router / Firewall	12	1	**12**
Mesh node (core)	8	2	**16**
Mesh node (periphery, timer-based)	8	3	**24**
Low-power Server (SSD)	25	1	**25**
Starlink (active mode)	40	1	**40**
Total (day, Starlink on standby)			**87**
Total (night, group B off)			**63**

Savings under the condition of t_off = 10 h: ΔE = 24 × 10 = 240 Wh per day.

Table 5 provides the power-consumption basis for the autonomy model. The main practical result is that the non-critical peripheral Mesh segment forms a controllable 24 W load that can be disconnected without disabling the network core. As a result, the standard daytime profile is estimated at 87 W, while the nighttime profile decreases to 63 W. For a 10-hour off-hours interval, this produces 240 Wh of daily energy savings, which directly increases the expected battery autonomy.

Table 6. Autonomy on $LiFePO_4$ 12 V battery

$LiFePO_4$ capacity	T_{000} (day), hour	T_{000} (night), hours	Rating
50 A·h (600 W·h)	6.9	9.5	*Short-term reserve*
100 A h (1200 W h)	13.8	19.0	*On a working day*
200 A·h (2400 W·h)	27.6	38.1	*More than a day of autonomy*
300 A·h (3600 W·h)	41.4	57.1	*Maximum autonomy*

Calculation: T = E_bat / P_avg. Day: P_avg = 87 W. Night: P_avg = 63 W (group B off).

Table 6 shows how battery capacity and average power consumption determine the expected autonomy of the reconstructed network. The results confirm a linear relationship between available energy and operating time: increasing $LiFePO_4$ capacity proportionally extends autonomy, while nighttime disconnection of non-critical loads improves the result for every battery size. The calculations also show that

capacities of 200 A·h and higher provide more than one day of operation under the tested load profile, which is sufficient for many prolonged outage scenarios.

Table 7. Failover and Mesh self-healing results

Scenario	Result	Recovery time
Loss of GPON channel	Automatic transition to Starlink	**10–20 s**
Loss of 1 Mesh node	Rerouting through neighboring nodes	**<3 sec**
Night shutdown of group B	Preserving core services	**0 s (planned)**
Complete blackout ($LiFePO_4$ network)	All services of group A are working	**Continuously**
Power restoration	Automatic transition to GPON + battery charging	**<30 s**

Table 7 summarizes the observed behavior of the architecture under failure and recovery scenarios. The results confirm that the main degradation processes remain controlled: GPON loss leads to automatic Starlink failover within 10-20 s, while the loss of one Mesh node is compensated by route reconstruction in less than 3 s. Planned night shutdown does not interrupt core services, and complete blackout operation preserves group A functions on battery power. These values support the conclusion that the architecture reduces the risk of cascading failure.

Table 8. Comparative efficiency before/after reconstruction

Indicator	Before the reconstruction	After reconstruction
Autonomy	Low/unpredictable (UPS 20–40 min)	**Forecast: 20–30+ hours**
Single Point of Failure (SPOF)	Present (switch, AP, WAN)	**Minimized (Mesh + dual - WAN)**
Internet Reserve	Missing	**GPON + Starlink (failover <20 s)**
Energy management	Missing	**$LiFePO_4$ + timer (saving 240 Wh /day)**
Local services when disconnected	Unavailable (cloud-only)	**Available via edge server**
Wi-Fi coverage when AP fails	Loss of zone	**Mesh self-healing (<3 s)**
Availability of services	< 95%	**≥ 99.5%**

Table 8 compares the initial office network state with the reconstructed architecture. The comparison shows a transition from short and unpredictable UPS-based reserve to predictable long-term autonomy, from single-channel Internet access to dual-WAN redundancy, and from cloud-only service dependence to partial local service autonomy. The most important practical effect is that failure of one component no longer causes immediate loss of the whole service chain. The reconstructed architecture therefore changes the operating mode from "working until the first failure" to predictable continuity with measurable recovery and autonomy parameters.

Figure 7 shows a two-dimensional comparison: the vertical line shows a list of threats/ malfunctions (including GPON channel loss, Starlink degradation, Mesh node failure, equipment overheating, deep battery discharge, DNS/DHCP failure, VPN session loss, cloud unavailability, timer failure, hop chain overload), and the horizontal line shows the protective mechanisms built into the architecture (Dual-WAN failover, Mesh self-healing, $LiFePO_4$+BMS, Group B timer, edge server, VPN rekey, monitoring/SIEM, proxy cache). The matrix cells are interpreted according to the legend below: from "no impact" to "high effectiveness".

Figure 7. Correspondence matrix: threats ↔ defense mechanisms.

Visually, this is reflected in the fill color (the "warmer"/greener the tone, the greater the contribution of the mechanism to threat mitigation), as well as in the markers inside the cells: conventionally, marker 1 corresponds to low effectiveness, 2 – medium, 3 – high; a dash means no significant impact. This presentation allows to see immediately not only "what works", but also where a combination of tools is needed. The matrix emphasizes several key dependencies. First, failures or degradation of WAN channels are most effectively covered by dual-WAN switching (preserving external availability), while the edge server and proxy cache act as mechanisms for reducing dependence on the Internet, supporting a local "island" of services and partial operability during degradation of external resources. Second, local Wi-Fi /topology failures (node failure, hop overload) are addressed primarily by Mesh self-healing and the principle of minimizing "hops" for critical services. Thirdly, energy risks (deep discharge, need for economy) are covered by the $LiFePO_4$+BMS combination and timer cut-off of non-critical loads, i.e., controlled degradation without destroying the core of the system. Fourth, service failures (DNS/DHCP, cloud unavailability) are logically "absorbed" by the local edge core, and VPN resiliency violations are absorbed by rekey/session renegotiation mechanisms. Finally, monitoring/SIEM in the matrix has a cross-cutting role: it does not "cure" the failure directly, but provides detection, status confirmation, and post-disaster diagnostics, which is critical for operation in recurring crisis modes. In conclusion, Figure 8 formalizes the recovery outcome as a system of complementary countermeasures: not one "magic" element, but a set of mechanisms that together ensure service continuity and managed degradation during blackouts and channel degradation. To show that the energy stability of the network is measured in watts and hours, Figure 8 summarizes the parameterization of the energy model: the contribution of each component to consumption, the

dependence of autonomy on the capacity of $LiFePO_4$, and the key formulas by which the total power, savings, and autonomy time are calculated.

Part A shows the power consumption of key components of the stand that form the total load profile: GPON ONT (10 W), Dual-WAN Router/Firewall (12 W), Mesh core (2×8 W = 16 W), peripheral Mesh nodes (3×8 W = 24 W), low-power server (25 W) and Starlink (40 W in active mode). It is from this decomposition that the "levers" of autonomy control are visible: peripheral Mesh nodes provide 24 W of controlled load, which can be cut off by a timer without destroying the core.

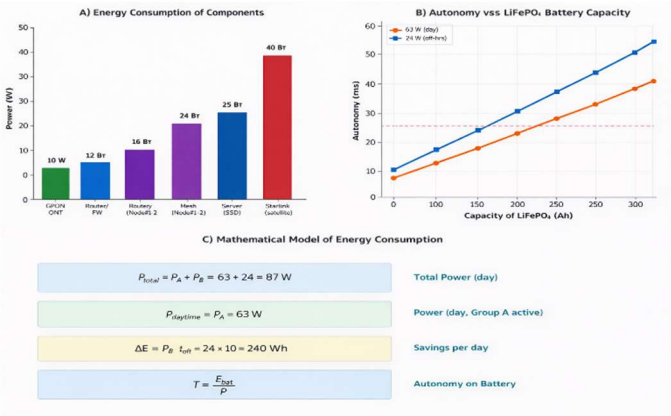


Figure 8. Parameterization of the energy consumption and autonomy model (component energy consumption, autonomy vs battery capacity, mathematical model).

As a result, for the standard daytime mode (Starlink in standby), the total power is 87 W, and in night mode with group B turned off – 63 W. Part B shows how the autonomy increases linearly with increasing $LiFePO_4$ capacity (axes "capacity, A·h" and "autonomy, h"). The calculation is based on the formula T = E_bat/P_avg, where for "day" P_avg = 87 W is taken, and for "night" (group B is turned off) P_avg = 63 W. The graph also sets a benchmark of 24 hours: it clearly shows that for a day of autonomous operation in the daytime profile, a capacity of the order of 200 A·h (≈27.6 h) is required, while in the night profile the reserve is significantly larger (≈38.1 h for 200 A·h), i.e., nightly "cutting off" of non-critical consumers directly brings the system closer to the "over 24-hour operation" mode. The lower block (mathematical model) summarizes the logic of the calculations: the daytime profile corresponds to a total power of 87 W, the night profile – 63 W, and the difference of 24 W at t_off = 10 h forms a daily saving ΔE = 24×10 = 240 W·h.

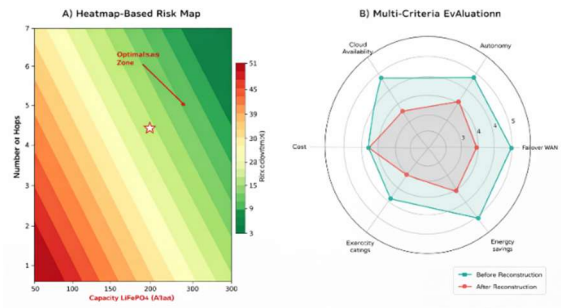


Figure 9. Optimization model: failure risk vs energy efficiency (downtime risk map and multi-criteria evaluation).

This saving is then "converted" into additional hours of autonomy through the same honest formula T = E_bat/P_avg: lower average power means longer operating time from the same battery (no magic – just arithmetic and the discipline of energy management). To move from individual measurements (failover, Mesh self-healing, energy profile) to engineering configuration selection, it is advisable to show the trade-off between downtime risk and energy efficiency in the form of an optimization model (Figure 9).

Figure 9A shows the downtime risk map as a function of two controlled parameters: $LiFePO_4$ capacity (Ah) on the X-axis and the number of Mesh nodes on the Y-axis. The color reflects the level of risk: warm shades correspond to a higher downtime risk (energy shortage and insufficient redundancy coverage), cold/green ones to a lower risk. The highlighted "optimal zone" shows the area in which increasing the battery capacity and the number of nodes gives the most noticeable effect of reducing the risk without excessive "oversizing" the system. The marked point on the field is interpreted as an example of a balanced configuration that is within this zone. Figure 9B shows a multi-criteria assessment in the form of a radar chart that compares the state before and after the restoration according to a set of criteria (service availability, autonomy, WAN failover, Wi-Fi resiliency, energy savings and cost). The area of the test site "after reconstruction" is larger by most criteria, which reflects the increase in stability and controllability of the system in crisis modes; at the same time, the cost criterion naturally does not "improve", but reflects the price of increasing reliability. Taken together, both parts of the figure show that the optimal configuration is determined not by the maximum of one parameter (for example, battery capacity), but by balancing power reserves, coverage redundancy and target availability metrics. The calculations and bench measurements presented have quantitatively confirmed the operability of the proposed architecture in key failure scenarios and energy constraint modes.

VII. DISCUSSION

To compare practical strategies for ensuring connectivity during a blackout, it is advisable to compare not just a single indicator (for example, only autonomy), but a set of metrics: autonomy, WAN switching capability, Wi-Fi resilience to local failures, and service availability. This comparison is presented in Figure 10.

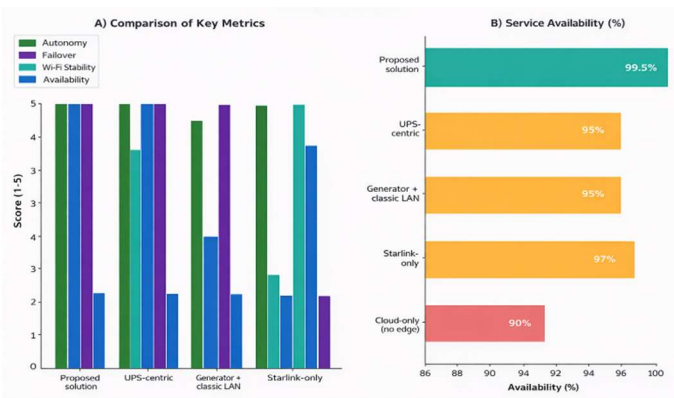


Figure 10. Comparative analysis of approaches to network security during a blackout (assessment of key metrics and service availability).

Figure 10A shows a comparison of five approaches on the scale of 1–5: the proposed solution (Mesh + dual-WAN + edge + $LiFePO_4$ + energy management) demonstrates the highest integral scores for autonomy, Wi-Fi stability and availability, while the UPS-centric approach significantly loses in autonomy and fault tolerance of the network part. The "generator + classic LAN" approach increases autonomy, but does not solve the problems of SPOF and self-healing of coverage, which is typical for centralized topologies without cellular logic. "Starlink-only" gains independence from ground infrastructure, but remains single-point with respect to the channel and does not enhance local autonomy of services. "Cloud-only (without edge)" has the worst availability profile, since when the Internet degrades, the organization loses critical functions regardless of the state of the local network, which conceptually contradicts the ideology of edge / fog approaches to maintain services near the user. In Fig. 10B, this is reflected quantitatively: the proposed solution achieves 99.5% availability, while cloud-only is limited to 90%, and intermediate options (UPS-centric, generator + LAN, Starlink-only) form a "ceiling" of about 95–97%. The advantage of the proposed architecture is explained by the synergy of four mechanisms. First, self-healing Mesh coverage reduces dependence on a single access node and maintains routes even in the event of element loss; this is consistent with the results of the research on control flexibility and protocol behavior in Mesh networks, as well as with approaches to optimizing the placement of coverage nodes under resource constraints and the importance of identifying critical components/links, the failure of which disproportionately reduces reliability. Secondly, dual -WAN (GPON as a basic channel + satellite backup) corresponds to the trend of hybridization of terrestrial and satellite segments, which increases availability in crisis modes due to switching policies and quality control, while GPON/PON remains a stable basis in normal mode. Thirdly, the local edge core reduces dependence on the cloud and allows supporting basic services during Internet degradation, which directly corresponds to the logic fog / edge architectures. Fourth, $LiFePO_4$-reserve with BMS and consumption profile management enhances the predictability of autonomy and reduces the risks of battery degradation in cyclic modes, and measurability power profile (P_avg, T, ΔE) corresponds to modern approaches to energy efficiency metrics as a basis for manageability. In contrast, UPS-centric solutions are effective as a "buffer" for short power sags, but in long blackouts they quickly go into power deficit mode and do not eliminate architectural SPOFs (WAN, AP, switch). Even optimized UPS approaches with intelligent control demonstrate that the key factor is energy management and load prioritization, not "simple power duplication". The generator approach increases autonomy, but adds logistical and operational risks (fuel, start/maintenance, noise, generator failure itself) and still requires network mechanisms for SPOF reduction and self-healing, which emphasizes the importance of scenario planning and recovery procedures. "Starlink-only" is appropriate as a fast channel in crisis conditions, but without a second channel and without a local "island" of services it does not provide the target continuity in the event of satellite segment degradation or energy constraints. "Cloud-only" in blackouts is structurally vulnerable due to dependence on Internet access and external data centers; a practical alternative is to transfer the minimum necessary functions to the edge circuit. At the same time, the interpretation of Figure 10 should take into account the limitations. The score 1–5 in the metrics section is aggregated and depends on the weights of the criteria, the type of office and the load profile; therefore, for industrial implementation, it is advisable to formalize the weights and translate the scale into measurable indicators (t_sw, RSSI, throughput, A, P_avg, T) with constant monitoring and logging. Additionally, in real conditions, one should take into account the threats of the radio environment (interference/jamming) and the corresponding resilience mechanisms, as well as the further development of security policies (segmentation, access control) as a component of service continuity in crisis modes. Thus, Figure 10 not only demonstrates the advantage of the proposed approach, but also sets a framework for the engineering choice of configuration: maximum resilience is achieved not just by one "strong" element, but by a coordinated combination of Mesh self-healing, dual-WAN redundancy, edge autonomy and managed power consumption.

VIII. CONCLUSIONS

The paper solves the applied problem of ensuring the continuity of office services in conditions of repeated blackouts by moving from a "monolithic" network with critical dependencies to an architecture that supports managed degradation. The scientific contribution of the study is expressed in the proposed integrated model of office IT infrastructure resilience, where network redundancy, local service autonomy, and autonomous energy supply are considered within a single engineering framework. The main novelty is the coordination of Mesh self-healing, GPON/Starlink dual-WAN failover, low-power edge services, and $LiFePO_4$-based power management through a formal A/B load-prioritization scheme. This makes it possible to evaluate office infrastructure continuity not only by the presence of backup equipment, but by a set of measurable indicators: autonomy time, failover delay, Mesh recovery time, service availability, and energy savings from controlled shutdown of non-critical loads.

In addition, the paper proposes a reproducible validation procedure for assessing office infrastructure resilience in crisis conditions. The procedure includes testing of the main operational failure scenarios: loss of the primary GPON channel with transition to Starlink, failure of a Mesh node with route reconstruction, night disconnection of non-critical loads, and complete blackout operation from $LiFePO_4$ power supply. This validation logic can be transferred to other small and medium-sized office environments by substituting their own power consumption profiles, number of nodes, local service set, and target availability requirements. The key result is that resilience to power outages is achieved not by a single component (UPS/generator/backup Internet), but by a coordinated combination of network and energy mechanisms: WAN redundancy, coverage self-healing, local service autonomy, and energy consumption discipline. The proposed architecture implements the principle of "24/7 core + planned peripheral shutdown". Critical network and service elements operate continuously (router/ firewall, basic Mesh coverage, local low-power edge server), while non-critical consumers are transferred to a managed mode by a timer. This approach simultaneously minimizes the risks of a single point of failure and provides predictability of autonomy, which is crucial for operation during long outages. Experimental Validation on the bench confirmed the operability of the access reservation model: in case of loss of the main channel, automatic switching

to the reserve channel with a recovery time of 10–20 s is provided. For the internal segment, the network's ability to maintain operability during local failures is shown: self-recovery of the route in the Mesh network when one node is disconnected occurs in less than 3 s. This means that the degradation becomes manageable and does not turn into a cascading scenario of "all coverage falls" due to a single failure. The obtained results of the energy model and their parameterization demonstrate that energy management is the same engineering "lever" as increasing battery capacity. For the daytime consumption profile, the total power is 87 W, and for the night profile with group B disconnected – 63 W. The difference of 24 W with 10 hours of cutoff per day creates savings of 240 Wh / day, which is directly converted into additional hours of autonomy. For batteries of different capacities, autonomy increases linearly, and nightly cut-off of non-critical loads systematically increases operating time without losing key functions. A comparative analysis of typical approaches to network provision during a blackout shows that "UPS-centric" solutions are suitable as a short-term buffer, but do not cover the needs of long-term outages and do not eliminate network SPOFs. The "generator + classic LAN" option increases the duration of power supply, but without topological stability and local autonomy of services remains vulnerable to node failures and WAN degradation. The "Starlink-only" approach provides independence from ground infrastructure, but without a second channel and edge circuits does not guarantee stable availability of services in the event of satellite segment degradation or power restrictions. The "cloud-only (without edge)" approach is the riskiest in crisis modes, since if Internet access is lost, the organization loses functions regardless of the performance of the local network. Thus, the practical value of the proposed solution lies in a reproducible set of engineering rules that can be transferred to other office facilities: external access reservation according to the dual-WAN scheme, limiting the "relay chain" for critical services, minimizing SPOF due to Mesh coverage, transferring the minimum necessary services to the local edge circuit, as well as formalized load division into critical and non-critical groups with timer control. Together, this transfers the network from the "working until the first failure" mode to the mode of predictable operation during outages, with transparent recovery metrics and energy autonomy. A limitation of the study is that part of the estimates depends on the specific office profile (area, radio environment, number of clients, work scenarios) and on the configuration level of implementation (types of Mesh nodes, router policies, composition of local services). At the same time, the architecture logic and validation methodology itself are universal: it allows to repeat testing for another site, substitute own consumption parameters, and verify the achievement of target indicators of autonomy, switching time, and service availability.

References

[1] H. Elzain, Y. Wu, "Software defined wireless mesh network flat distribution control plane," *Future Internet*, vol. 11, no. 8, art. 166, 2019. https://doi.org/10.3390/fi11080166.

[2] N. Ussipov, A. Mukhambetova, M. Moldaganova et al., "MEGA: maximum – entropy genetic algorithm for router nodes placement in wireless mesh networks," *Sensors*, vol. 24, no. 20, art 6735, 2024. https://doi.org/10.3390/s24206735.

[3] D. Turlykozhayeva, G. Absadykova, A. Imashev et al., "Experimental performance comparison of proactive routing protocols in wireless mesh network using Raspberry Pi 4, *Telecom.*, vol. 5, no. 4, pp. 1008–1020, 2024. https://doi.org/10.3390/telecom5040051.

[4] R. Glazkov, A. Gorodetskiy, O. Solovyov at al., "Provisioning of fog computing over named – data networking in dynamic wireless mesh systems," *Sensors*, vol. 24, no. 4, art. 1120, 2024. https://doi.org/10.3390/s24041120.

[5] N. Akram, O. Ugurlu, İ. Kocabaş, O. Dagdeviren, "Detection of critical links for improving network resilience," *Electronics*, vol. 14, no. 14, art. 2904, 2025. https://doi.org/10.3390/electronics14142904.

[6] S. Kurdiuk, Y. Boichuk, S. Zlotskiy et al., Development of a high – reliability hybrid data transmission system for unmanned surface vehicles under interference conditions," *Drones*, vol. 9, no. 3, art. 174, 2025. https://doi.org/10.3390/drones9030174.

[7] F. Aktas, Y. Yayla, N. Erbass et al., "Routing challenges and enabling technology for 6G– satellite network integration: towards seamless global connectivity," *Technologies*, vol. 13, no. 6, art. 245, 2025. https://doi.org/10.3390/technologies13060245.

[8] S. Shaffiee Haghshenas, M. Scalvenzi, N. Elia, A. Bruzzone, "The potential of satellite internet technology for crisis management during urban evacuation: a case study of Starlink in Italy," *Information*, vol. 16, no. 10, art. 840, 2025. https://doi.org/10.3390/info16100840.

[9] R.R. Boros, V. Motuzienė, A. Janulevičius at al., "Optimized real-time energy management and neural network-based control for photovoltaic – integrated hybrid uninterruptible power supply systems," *Energies*, vol. 18, no. 6, art. 1321, 2025. https://doi.org/10.3390/en18061321.

[10] T. Chen, M. Li, J. Bae, "Recent advances in lithium iron phosphate battery technology: a comprehensive review," *Batteries*, vol. 10, no. 12, art. 424, 2024. https://doi.org/10.3390/batteries10120424.

[11] M. Li, Y. Wei, X. Xie et al., "State of health estimation and battery management: a review of health indicators, models and machine learning," *Materials*, vol. 18, no. 1, art. 145, 2025. https://doi.org/10.3390/ma18010145.

[12] A. Safari, J. Rabb, Z. Suleiman at al., "A systematic review of energy efficiency metrics for optimizing cloud data center operations and management," *Electronics*, vol. 14, no. 11, art. 2214, 2025. https://doi.org/10.3390/electronics14112214.

[13] K. L. Veigas, M. Zhou, N. Degirmenci et al., "Towards energy efficiency of HPC data centers: a data-driven analytical visualization dashboard prototype approach," *Electronics*, vol. 14, no. 16, art. 3170, 2025. https://doi.org/10.3390/electronics14163170.

[14] S. Qi, H. Pan, L. Guo, S. Yin, "Dual-network layered network: a method this improve reliability, security, and network efficiency in distributed heterogeneous network transmission," *Electronics*, vol. 13, no. 23, art. 4749, 2024. https://doi.org/10.3390/electronics13234749.

[15] J. Fang, Y. Miao, S. Xu, M. Zhao, "Energy-efficiency resource provisioning strategy for reduced power consumption in edge computing," *Applied Sciences*, vol. 10, no. 17, art. 6057, 2020. https://doi.org/10.3390/app10176057.

[16] S. Algarni, F. E. Abd El-Samie, "Energy-efficient distributed edge computing this assist dense Internet of things," *Future Internet*, vol. 17, no. 1, art. 37, 2025. https://doi.org/10.3390/fi17010037.

[17] A. Lastovetsky, R.R. Manumachu, "Energy-efficiency parallel computing: challenges this scaling," *Information*, vol. 14, no. 4, art. 248, 2023. https://doi.org/10.3390/info14040248.

[18] C. Del-ValleSoto, M. Reyes-Robledo, L. Candela at al., "A resilient energy-efficient framework for jamming mitigation in cluster-based wireless sensor networks," *Algorithms*, vol. 18, no. 10, art. 614, 2025. https://doi.org/10.3390/a18100614.

[19] M. M. Hosen, M. S. U. Chowdhury, S. Islam et al., "Optimized economy dispatch and battery sizing in wind microgrids: a depth of discharge perspective," *Electricity*, vol. 6, no. 3, art. 51, 2025. https://doi.org/10.3390/electricity6030051.

[20] M. Fernández-Temprado, M. Galera Monfort, A. Rodríguez-Cela et al., "Experimental testbed and measurement campaign for multi-constellation LEO positioning," *Engineering Proceedings*, vol. 126, no. 1, art. 12, 2026. https://doi.org/10.3390/engproc2026126012.

[21] N. Zahri, S. Bektaş, H. Luque et al., "Survey on optimization models for energy-efficient computing systems," *Energies*, vol. 15, no. 19, art. 7073, 2022. https://doi.org/10.3390/en15197073.

[22] P. Manzoni, S.E. Merzougui, C.E. Palazzi, P. Pozzan, "A resilient LoRa -based solution this supports pervasive sensing," *Electronics*, vol. 12, no. 13, art. 2952, 2023. https://doi.org/10.3390/electronics12132952.

[23] Z. Cao, W. Gao, Y. Fu, et al, "Second-life assessment of commercial $LiFePO_4$ batteries retired from EVs," *Batteries*, vol. 10, no. 9, art. 306, 2024. https://doi.org/10.3390/batteries10090306.

[24] F. Sapundzhi, B. Zarev, S. Georgiev at al., "Design and implementation of a passive optical network for a small town," *Engineering Proceedings*,

vol. 100, no. 1, art. 40, 2025. https://doi.org/10.3390/engproc2025100040.

[25] J. Qi, P. Li, Y. Dong, et al., "Remaining available energy prediction for energy storage batteries based on interpretable generalized additive neural network," *Batteries*, vol. 11, no. 7, art. 276, 2025. https://doi.org/10.3390/batteries11070276.

[26] H. Abdulrab, F. A. Hussin, I. Ismail at al., "Energy efficient optimal deployment of industrial wireless mesh networks using transient trigonometric Harris Hawks optimizer," *Heliyon*, vol. 10, no. 7, art. e28719, 2024. https://doi.org/10.1016/j.heliyon.2024.e28719.

[27] I. Baig, N.U. Hasan, P. Valsalan, M. Zghaibeh, "Energy efficient multicast communication in cognitive radio wireless mesh network," *Sensors*, vol. 22, no. 15, art. 5601, 2022. https://doi.org/10.3390/s22155601.

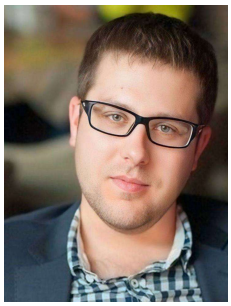
OLEKSANDR KORCHENKO *in 1983 graduated from the Kyiv Institute of Civil Aviation Engineers (now the National Aviation University). In 2004 defended received the degree of Doctor of Technical Sciences. In 2005 was awarded the title of Professor of the Department of Information Technology Security. At the present time is working as an first vice-rector at the State University of Information and Communication Technologies (Kyiv, Ukraine). Corresponding Member of the National Academy of Sciences of Ukraine (specialty – cybersecurity), Prof., Dr Hub (Eng), Laureate of the State Prize of Ukraine in the field of science and technology, Honored Worker of Science and Technology of Ukraine. Scientific interests: cybersecurity and information protection.*

YULIIA KHOKHLACHOVA *in 2004 graduated from the National Aviation University with a degree in Radioelectronic Devices, Systems and Complexes. In 2015 defended her dissertation for the degree of Candidate of Technical Sciences. In 2023 received a diploma as a professor of the Department of Information Technology Security. At the present time is working as a professor at the Department of Software Engineering and Cybersecurity of the State University of Trade and Economics. Scientific interests: cybersecurity and information protection.*

DMYTRO PROKOPOVYCH-TKACHENKO *is a PhD in Technical Sciences and Associate Professor, serving as Head of the Department of Cybersecurity and Information Technologies at the University of Customs and Finance and Senior Research Fellow at the State Scientific Institution "Institute of Information, Security and Law" of the National Academy of Legal Sciences of Ukraine. His professional background combines academic leadership with seniorgovern- mental and security service positions, including executive roles within the State Service of Special Communication and Information Protection of Ukraine. Research interests include cryptography, steganography, technical information protection, cybersecurity, and cybersecurity standards.*

TETYANA RUDYANOVA *is an Associate Professor with a Candidate degree in Physical and Mathematical Sciences (01.05.01 – theoretical foundations of informatics and cybernetics). She graduated in Applied Mathematics from Novocherkassk Polytechnic Institute, specialising in mathematical support for automated control systems. Also undertakes academic advising and leads a student research group focused on mathematical modelling and optimisation in technical, information, and economic systems Research interests include information technologies, mathematical modelling, computer graphics, and artificial intelligence.*

ROSTYSLAV PALAHUSYNETS *graduated from the National University of Uzhgorod in 2004 with a degree in International Economic Relations. In 2012, he defended his dissertation for the Candidate degree (Ph.D.) of Economic Sciences, and in 2021 he defended his dissertation for the Doctor of Science (Dr. Sci.) degree in Public Administration. In 2025, he obtained the title of Associate Professor of the Department of Sociology and Social Work at Uzhhorod National University. Currently, he is the Deputy Permanent Representative of Ukraine to the International Organisations in Vienna and concurrently works as an Associate Professor of the Department of Sociology and Social Work at Uzhhorod National University. Scientific interests: energy security, intellectual capital, etc.*



DMYTRO SHCHYTOV *graduated from the Academy of the Customs Service of Ukraine in 2007 with a degree in "Management of Foreign Economic Activity". In 2015, he defended his dissertation for the degree of Candidate of Economic Sciences on the topic "Implementation of the Export Potential of EU Countries in the Global Market of High-Tech Services". He worked as an associate professor at the Department of International Relations and Tourism at DNU; as an associate professor at the Department of International Economic Relations, Regional Studies and Tourism at the University of Customs and Finance (UCF); as a senior lecturer at the Department of Management and Administration of the Dnipro Faculty of Management and Business of the Kyiv University of Culture. In 2024, he received his second higher education at UCF (majoring in Computer Science). He is currently a doctoral student at UCF. Scientific interests: e-commerce, cybersecurity, high-tech services, artificial intelligence, etc.*