Multi-layer secured architecture of a local automated centralized alert system*

Volodymyr Hotovych [1,†], Oleh Nazarevych [1,†] , Grigorii Shymchuk [1,†], Liubomyr Matiichuk [1,†] and Yurii Maksymiak [1,*,†]

[1] *Ternopil Ivan Puluj National Technical University, 56, Ruska Street, Ternopil, 46001, Ukraine*

Abstract

The article analyzes typical cyber and physical threats inherent to Local Automated Centralized Alert Systems (LACAS). A multi-layered secured architecture is proposed, combining Zero Trust principles, network microsegmentation, end-to-end encryption of data transmission channels, and redundancy of critical components. The developed architectural model provides for the use of fault-tolerant channels (Ethernet + LTE/5G + satellite communication), multi-factor authentication for control center personnel, and autonomous algorithms for operating alert sirens in the event of a communication loss. To assess the effectiveness of the proposed solutions, a potential risk analysis was conducted, and methods were presented to reduce the likelihood of a successful attack and to shorten the mean time to recovery after an attack. The results of the study demonstrate that implementing the specified technical and organizational measures significantly increases the cyber resilience of LACAS and ensures uninterrupted public alerting even under combined threat conditions.

Keywords

Local Automated Centralized Alert System (LACAS); cyber resilience; Zero Trust; microsegmentation; TLS encryption; data backup

1. Introduction

Local Automated Centralized Alert Systems (LACAS) are hardware and software complexes designed for the urgent delivery of signals and messages about threats or the occurrence of emergencies to government authorities and the public [1]. The operation of public alert systems is one of the key tasks of civil protection, enshrined in the legislation of Ukraine [2]. The organizational foundations for creating and maintaining such systems are defined by several regulatory acts, including the Civil Protection Code of Ukraine and a special regulation approved by Cabinet of Ministers Resolution No. 733 [3].

Historically, alert systems at various levels were based on analog technologies (electromechanical sirens, analog information transmission channels such as radio and television, etc.). However, under modern conditions — especially in connection with russia's aggression against Ukraine — there has arisen a need to modernize these systems by implementing digital technologies and enhancing their level of cybersecurity [4, 5].

2. Literature review

In 2018, the Government of Ukraine approved the Concept for the Development and Technical Modernization of the Alert System [4] and adopted an Action Plan for its implementation [5]. These documents emphasized the need to ensure the system's resilience to cyber intrusions and the

[*] *The 5th International Conference on Information Technologies: Theoretical and Applie (ITTAP-2025) October 22-24, 2025 Ternopil, Ukraine Opole, Poland*

[1*] Corresponding author.

[†] These authors contributed equally.

gotovych@gmail.com(V. Hotovych); taltek.te@gmail.com (O. Nazarevych); gorych@gmail.com (G. Shymchuk); mlpstat@gmail.com (L.Matiichuk); admin@prosto.te.ua (Y. Maksymyak)

0000-0003-2143-6818 (V. Hotovych); 0000-0002-8883-6157 (O. Nazarevych); 0000-0003-2362-7386 (G. Shymchuk); 0000-0001-6701-4683 (L.Matiichuk); 0009-0008-2489-8659 (Y. Maksymyak)

protection of information. In particular, the action plan provides for the creation of a comprehensive information protection system (CIPS) within the nationwide alert system [5]. This approach aligns with the national cybersecurity policy defined in the Law of Ukraine “On the Basic Principles of Ensuring Cybersecurity” [6].

As an important element of critical infrastructure, LACAS is subject to various risks. An analysis of a well-known nationwide project for the creation of LACAS [1] revealed potential “break points” that directly correspond to specific types of threats:

- Unauthorized control and insider risk. The use of a MikroTik RB960 router, node management via 2G/SMS, and a backup satellite channel based on the Viasat SurfBeam RM4100 modem poses significant risks. RouterOS contains vulnerability CVE-2023-30799, which allows a low-privilege administrator to execute arbitrary commands and escalate privileges. Combined with the typical “admin / empty password” setup, this creates a path to seizing control of the control center and broadcasting false alerts [14]. The absence of SIEM logs and patch management procedures for RouterOS makes rapid breach detection impossible.
- Attacks on communication networks (2G/SMS). Controlling sirens via 2G and SMS exposes the system to IMSI-catcher attacks, downgrades to weak A5/1 encryption algorithms, and SS7 message spoofing. Google has already implemented in Android 16 the ability to completely disable 2G to counter such threats [15].
- Malware infection and denial of the backup satellite communication channel. Viasat RM4100 modems have been found to contain a zero-day vulnerability (CVE-2024-6198) enabling remote code execution via the web interface. Compromise of the sole satellite channel paralyzes backup alerting and provides a foothold for further network infection [16].
- False alarms and trust undermining. In February 2023, a few Russian radio stations were compromised, resulting in broadcasted messages about “missile danger,” which caused public panic. A similar scenario in our LACAS threatens both disruption and loss of trust in the alert system [10, 17].
- Physical tampering and lack of multi-layered protection. Documentation [1] does not require TLS 1.3/VPN between the server and local alert control units (BCO) nor does it provide for VLAN segmentation, which contradicts the “implicit deny” principle in Zero Trust. NXDN digital radio supports AES-256 encryption only after installing the KWD-AE30/AE31 board. Unencrypted NXDN traffic can be decoded using DSD + RTL-SDR, enabling passive system monitoring and preparation of a replay attack. Project [1] does not provide for secured telecom equipment cabinets or the use of A/B-class uninterruptible power supplies. In the event of a combined cyberattack and physical power outage or cable damage, alert devices would lose control — moving the risk from IT to the OT security domain [1].
- Dependence on public networks (Internet, mobile operators). If alerting relies on public networks, attackers may carry out DDoS attacks, compromise telecom equipment, or send fake SMS messages on behalf of the alert service. Recent cyber incidents targeting Ukrainian ISPs and mobile operators confirm the reality of this threat. Failures or compromise of communication networks can delay or prevent signal delivery to the public, which is especially dangerous during sudden attacks.

The LACAS system fully falls under the identified types of threats: unauthorized control, network attacks, malware infection, physical tampering, and the human factor (social engineering), as shown in Figure 1. For critical infrastructure, this is unacceptable and requires the urgent implementation of measures such as end-to-end encryption, microsegmentation, MFA, communication channel redundancy, and regular patch management.

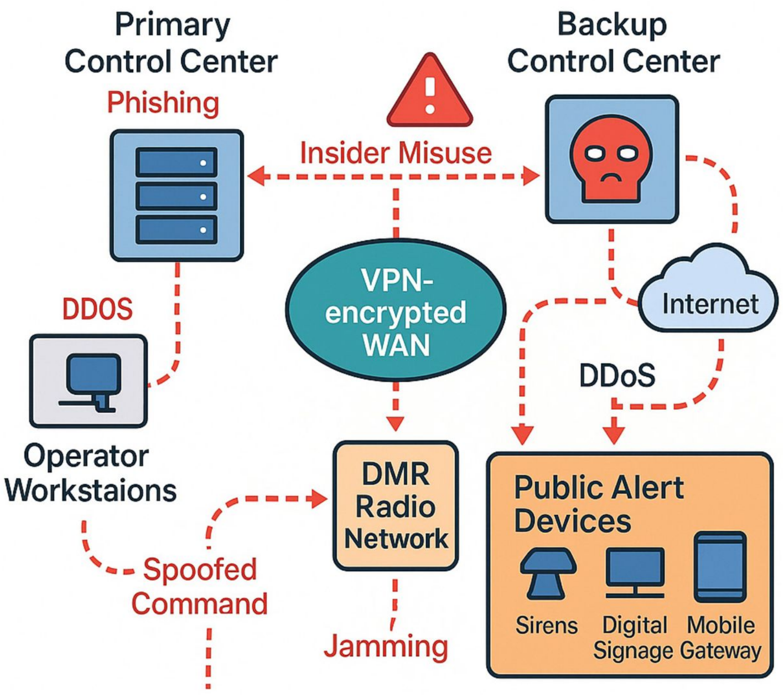

Figure 1: Thread Surface and Attack Vectors.

All these risks make the implementation of comprehensive protection for LACAS an urgent necessity. Vulnerabilities may lie in the software (use of outdated versions, lack of encryption), in the network infrastructure (open ports, weak authentication), and/or in organizational procedures (absence of backup alerting protocols, insufficient staff training, etc.). Alert systems are classified as part of the state's critical infrastructure and therefore fall under the law on critical infrastructure, which requires additional security measures and ensures the operational resilience of such facilities [11].

3. Proposed Solution for the Secured Architecture of LACAS

3.1. Typical Components of LACAS

In the general case, a modern LACAS represents a multi-level infrastructure operating at the national, regional (territorial), and local levels. Figure 2 shows the proposed LACAS architecture. At each level, the system includes several key components:

1. Alert Control Center – the primary and backup control point equipped with an operator's automated workstation (AWS). This is a hardware and software complex through which authorized personnel initiate messages and signals [1]. To enhance reliability, a backup control center is typically provided in case the primary one fails.
2. Communication Channels – networks for transmitting signals from the control center to the end alerting devices. Several types of channels are used: wired (dedicated lines, Internet) and wireless (cellular communication, radio networks). Modern systems implement digital radio networks based on the DMR standard in VHF/UHF bands to transmit commands to alert devices [1]. For reliability, channels are duplicated: for example, the operator's AWS can simultaneously connect via Ethernet, mobile Internet (using two different providers), and even a satellite channel [12]. Such multi-channel communication ensures alerting operation even if certain networks fail.
3. Public Alert Devices – end nodes that directly deliver signals to people. These include alert equipment with loudspeakers, as well as auxiliary means such as electronic information

boards, devices for transmitting messages to TV and radio channels, and mass messaging systems (SMS, Cell Broadcast) [1]. Modern alert devices are equipped with slot loudspeakers capable of covering large open areas and can transmit not only the "Attention Everyone" signal but also voice messages.

4. Integration Components – software and interfaces that ensure interaction between the system levels (national – regional – local) and with other civil protection information systems. For example, a local system can be linked to regional and national systems to receive and relay higher-level signals when necessary.

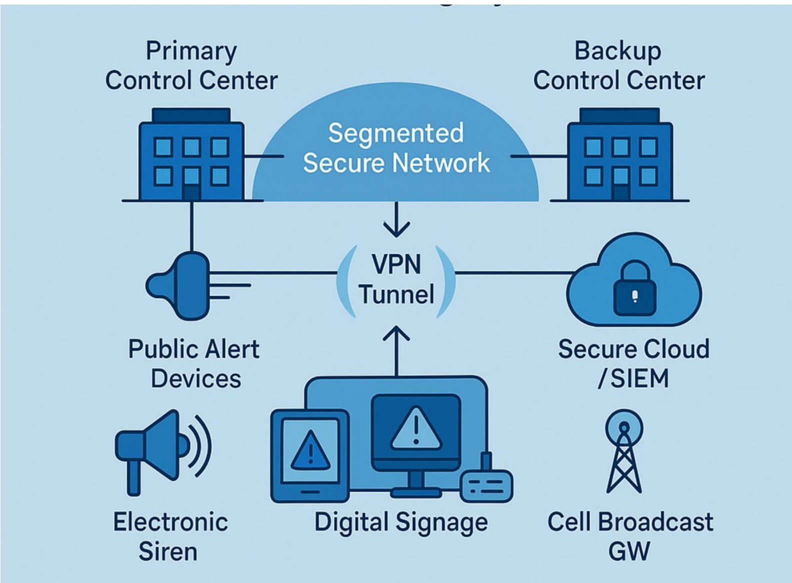

Figure 2: Layered Architecture of a Resilient LACAS System.

Let us formulate the fundamental principles on which a secured architecture LACAS should operate.

3.2. Fundamental principles for implementing a secured LACAS architecture

Based on the analysis of known solutions and the regulatory framework currently relevant to Ukraine, the authors of this work propose a secured and cyberattack-resistant architecture for LACAS. The proposed architecture is grounded in the Law of Ukraine "On Critical Infrastructure" (2021), the Law "On the Basic Principles of Ensuring Cybersecurity" (2017), DSTU ISO/IEC 27001:2022 and DSTU ISO/IEC 27032:2016 (defining requirements for ISMS and network interaction cybersecurity), Cabinet of Ministers Resolution No. 733 (2013) [3], and the recommendations of NIST SP 800-207 (Zero Trust Architecture) as a modern access model.

The fundamental principles of the proposed architecture are defined by modern concepts of Zero Trust, microsegmentation, and end-to-end encryption. Within these approaches, each interaction between system elements begins with mandatory authentication and authorization procedures, and the absence of pre-trusted zones imposes stricter access control requirements. Logical network separation is implemented through dedicated VLAN or SD-WAN segments that isolate the control center, the transport layer, and field devices. Data transfer between nodes is encrypted using TLS 1.3 or IPSec IKEv2, while radio channels employ AES-256. To prevent account compromise, all operators and service accounts use multi-factor authentication, while fault tolerance is ensured by independent communication channels of different technologies and autonomous power supplies for critical nodes. Continuous event monitoring is performed by a SIEM platform with network threat detection and automated DDoS traffic filtering.

The logical system model encompasses three layers, as shown in Figure 3.

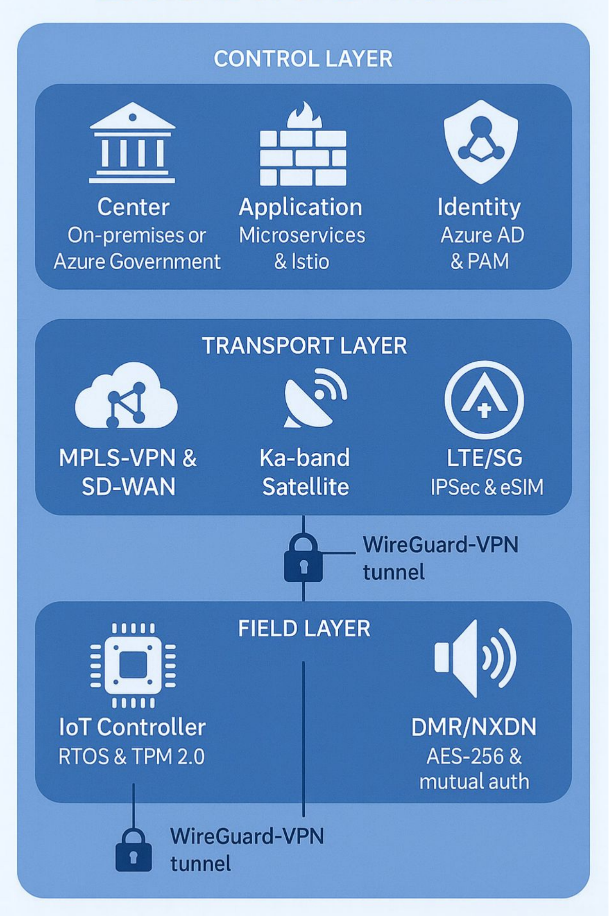

Figure 3: Three-layer logical model of the system.

In the control layer, the center is deployed in a state data center or in Azure Government cloud infrastructure, with access restricted to private networks and protected by Azure Firewall. The software is built on microservices in an environment with Istio service mesh infrastructure, providing mutual traffic encryption and policy-based routing. Identity management relies on Azure AD (Entra ID) with conditional access, and privileged access is handled via a PAM-class solution with Just-In-Time mode. Secrets are stored in Azure Key Vault with an HSM module, accessed via managed identities. The transport layer uses terrestrial MPLS-VPN or SD-WAN channels over optical networks with IPSec encryption; backup is provided by Ka-band corporate-grade satellite lines, as well as LTE/5G mobile gateways with eSIM, IPSec tunnels, IMEI verification, and APN whitelisting. The field layer consists of IoT siren controllers based on MCU with TPM 2.0, a dedicated RTOS, and connections via WireGuard VPN; radio communications are implemented using DMR or NXDN with AES-256 enabled and mutual terminal authentication. Each alerting device can autonomously activate using the last valid configuration in case of channel loss.

Protection against common threats involves a set of organizational and technical measures. Uncontrolled control attempts are neutralized by an RBAC role model supplemented with ABAC attribute-based control, immutable change logging, and PAM session recording in Vault. Denial-of-service and traffic spoofing are countered by combining WAF with cloud-based DDoS mitigation service , while DNSSEC ensures the integrity and authenticity of domain records along with QUIC (HTTP/3) for public mobile apps. The risk of malware infection is mitigated by container isolation with gVisor, mandatory digital signature verification, SBOM scanning at the CI/CD stage, and deployment of EDR agents using the MITRE ATT&CK taxonomy. Physical protection is provided by IP-65 rated enclosures, unauthorized access sensors, and backup batteries with at least seventy two hours of autonomy; geo-distributed replication of the control center and a “hot” backup operator in a remote region eliminate single points of failure. Regarding the human factor, a dual confirmation rule for mass alerting is enforced, along with regular staff training and Red-/Blue-Team sessions.

Incident response and recovery procedures are based on NIST SP 800-61 guidelines, covering all phases of the incident lifecycle from detection to post-incident analysis. Thanks to a backup message queue hosted in a Kafka cluster with triple replication, the recovery point objective does not exceed thirty seconds, and the recovery time objective is no more than five minutes, ensured by automatic activation of the backup site via DR orchestration platform (site-recovery automation) . This combined solution forms a comprehensive architecture capable of ensuring the uninterrupted operation of the Local Automated Centralized Alert System even under complex cyber and physical impact conditions.

3.3. Modern cybersecurity methods for a secured LACAS architecture

Information protection in LACAS requires a multi-layered approach that combines organizational, technical, and cryptographic measures. The main principles of ensuring cybersecurity and information resilience in LACAS, which must be implemented in a secured LACAS architecture, are presented below.

3.3.1. Access control and user authentication.

The system must grant access to its functions only to authorized individuals in accordance with their official duties. Each operator is assigned an individual account with defined permissions. The requirements of the official Instruction (Order of the Ministry of Internal Affairs No. 93) [7] stipulate blocking any attempts at unauthorized modification or deletion of information if the actions are performed by a user without the appropriate rights or by an entirely unauthorized entity.

Authentication technologies — from passwords and hardware keys to multi-factor methods (for example, token and password) — are implemented to make account compromise as difficult as possible [7]. An important principle is role-based access separation. The regulatory framework defines several categories of LACAS users: operator (on-duty personnel directly initiating alerts), administrator (a specialist with the rights to configure the system and manage users), and developer/technical specialist (responsible for modernization and technical maintenance) [7].

Accordingly, access levels are established: a basic level (viewing system status without the ability to interfere), operator level, administrator level, and the highest — developer level. Access to a higher level is possible only through the lower one (for example, a developer can log in only after signing in as an administrator) [7].

3.3.2. Data and communications protection

Information transmitted and stored in LACAS must be protected from unauthorized access, forgery, and destruction. To achieve this, cryptographic measures are implemented, including encryption of communication channels, digital signing of commands and messages, and data integrity control. Information in the system must be transmitted using interference-resistant encoding, and all data must be protected from corruption and unauthorized access [7].

In practice, this means applying encrypted protocols (VPN tunnels for Internet connections, TLS for IP traffic, hardware encryption in DMR radios, etc.) and regularly backing up critical data (such as system configurations, event logs, and more). It also involves implementing differentiated access to information for different categories of users [7].

According to the Law of Ukraine “On Information Protection in Information and Communication Systems” [8], state information systems (including the alert system) must have a comprehensive information protection system with confirmed compliance (CIPS) [7]. In practice, implementing CIPS entails using certified cryptographic protection tools, intrusion detection and prevention systems, and adhering to national cybersecurity standards. For example, communication channel encryption may employ algorithms certified by the State Service of Special Communications and Information Protection of Ukraine, while access control may rely on hardware-software complexes (routers, firewalls) configured in accordance with a defined security profile. The entire system must undergo a state examination to confirm compliance with information protection requirements [8].

3.3.3. Monitoring, attack detection, and response

The multi-layered protection of LACAS is shown in Figure 4.

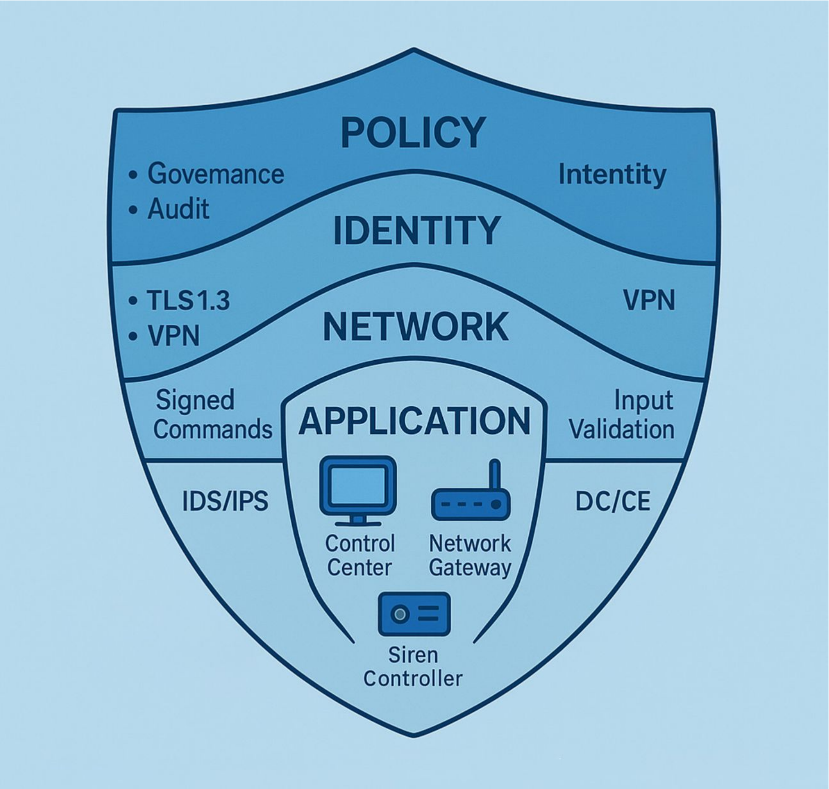

Figure 4: Multi-level protection of LACAS.

The resilience of the system to cyberattacks is ensured not only by preventive measures but also by its ability to quickly detect incidents and restore operations. In modern LACAS projects, tools for monitoring network traffic and node status are integrated — such as intrusion detection systems (IDS), centralized event logs (SIEM) for analyzing suspicious activity, and mechanisms for automatically notifying administrators of malfunctions.

According to international recommendations for protecting industrial and operational systems, it is advisable for such critical complexes to apply the concept of “defense-in-depth” and continuous security monitoring [9]. This means that even if one line of defense is breached (for example, an operator’s password is compromised), other mechanisms (privilege restrictions, anomalous activity analysis, backup alerting scenarios) will prevent the attacker from disrupting the system’s operation.

3.3.4. Physical security and infrastructure redundancy

Cybersecurity cannot be separated from the physical protection of LACAS components. Server rooms of alert centers are equipped with access control systems, backup power supplies, and fire suppression systems to minimize the risk of being disabled through physical impact. Communication lines (cables, repeaters) should preferably be routed along different paths with redundancy. The installation of sirens also takes physical security into account: equipment is placed at inaccessible heights, inside sealed cabinets with locks.

Redundancy also applies to software resources: regular backups of system configurations, the availability of spare server equipment, and backup communication channels (for example, a radio network in case of Internet unavailability) significantly increase the survivability of the system during an emergency.

As part of the modernization of Ukraine's alert system, a number of these measures have already been implemented. In particular, the technical requirements for the nationwide LACAS (Order of the Ministry of Internal Affairs No. 884) mandate compatibility of equipment across different levels, the use of secured communication channels, and redundancy of nodes [12]. The State Emergency Service has issued recommendations for calculating siren coverage zones and designing local alert systems [13] — this is also part of the overall security strategy, as proper signal coverage minimizes the risk of missed messages in the event of localized failures of individual devices.

3.4. Designing a secured LACAS in Ukraine today

Based on the principles discussed, a typical LACAS configuration with enhanced security can be designed for a medium-sized Ukrainian city.

The primary center should, for example, be located at the municipal state administration, with a backup center at a regional State Emergency Service (SES) office or another facility connected to backup power. Both are equipped with identical operator workstations (AWS) synchronized with each other. Data on siren status, event logs, and similar information are replicated between centers in real time over secured channels. Each center has a certified Comprehensive Information Protection System (CIPS) attested in accordance with the established procedure [7], ensuring that cryptographic and technical means comply with state requirements.

The LACAS network is isolated from the public Internet: all connections to external networks pass through firewalls with strict rules. Communication between centers and remote alert devices uses virtual private networks (VPN) with encryption. For example, if alert devices are connected via cellular networks (GSM/3G/4G), VPN tunnels are established over the mobile network, or an operator's private APN is used with traffic encryption. Digital DMR transmitters are configured with encryption keys, preventing eavesdropping or spoofing of activation signals for alert devices. All commands from the control center to execution devices are digitally signed or include a cryptographic authentication code verified by the receiver. Thus, third-party signals or jamming attempts will not cause false or missed alarms.

In the event of a large-scale cyberattack on one communication channel (e.g., the Internet), alternative paths are provided — radio networks, backup satellite links, or local networks. Each electronic siren can receive multiple types of signals: via the primary channel (e.g., IP over Ethernet or 4G), the backup channel (DMR radio), and even autonomously by timer or sensor (as part of an early warning system). Siren power nodes are equipped with uninterruptible power supplies so that operation continues even during mains outages.

Within the LACAS network segment, a hardware–software complex is deployed to track suspicious activity. It monitors traffic for indicators of common attacks (port scans, password-guessing attempts, anomalous command sequences to sirens) and, upon detection, immediately notifies administrators and automatically switches the system into a safe mode. Safe mode may include temporarily blocking remote commands and switching to local control (for example, the duty SES officer can activate the alert directly on site upon a command over a secured voice channel).

When designing a secured system, lifecycle support processes are built in: periodic penetration tests (simulated attacks to find vulnerabilities), scheduled software updates (security patches for server OSs, siren controller firmware), and log analysis for anomalies. These measures allow proactive identification of weak points and strengthening of defenses before adversaries can exploit them.

The proposed architecture aligns with current trends in building cyber-resilient systems. It is consistent with NIST recommendations for protecting operational technology, which call for combining access control measures, network segmentation, secured network protocols, and continuous risk monitoring [9].

4. Evaluation and analysis of the results obtained

The implementation of the described set of measures makes it possible to largely neutralize current threats to LACAS:

- First, strict authentication and user rights separation virtually eliminate accidental or intentional unauthorized control of alerts by personnel.
- Second, encryption and multi-level command verification ensure the integrity and authenticity of signals: a foreign or altered signal will simply not be accepted by the execution devices.
- Third, the presence of redundancy — both in infrastructure (duplicate servers, channels, transmitters) and in procedures (alternative alerting scenarios)—ensures continuity of operation even under emergency conditions. Monitoring and response capabilities minimize the time from attack detection to containment, which is crucial in fast-moving cyber incidents.

However, it should be taken into account that the field of cybersecurity is dynamic—the methods of carrying out attacks are constantly evolving. Therefore, the security level of LACAS requires regular review and enhancement. One area for improvement is the implementation of the Zero Trust concept in future alert systems Figure 5.

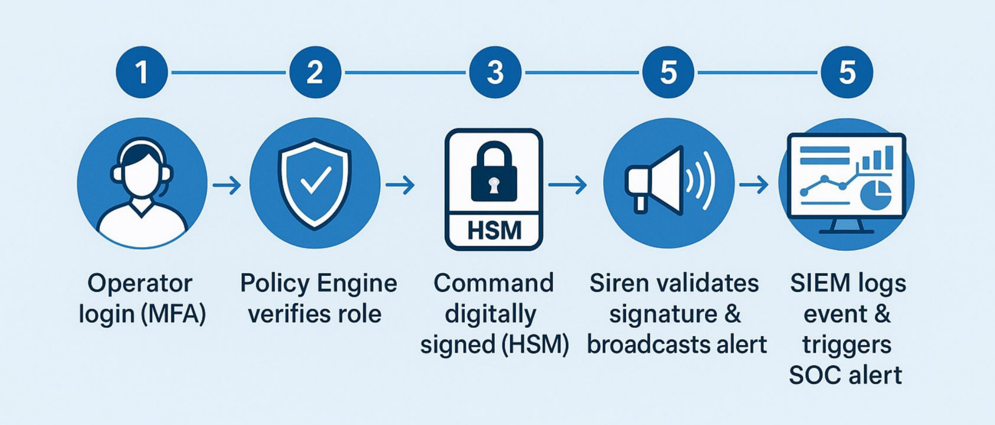
1
2
3
5
5
HSM
Operator login (MFA)
Policy Engine verifies role
Command digitally signed (HSM)
Siren validates signature & broadcasts alert
SIEM logs event & triggers SOC alert

Figure 5: Zero-Trust alert dispatch process with multi-factor authorization and cryptographic validation.

This means that no network element trusts another by default: every action must be verified and authorized, even if it originates from a “secured” segment. For LACAS, this could include such measures as additional confirmation of critical commands (for example, initiating a nationwide alert) by two different responsible persons, the use of hardware security modules (HSM) for storing encryption keys, and tokens or biometrics for operator login, among others.

While individual security techniques (Zero Trust, mTLS, microsegmentation) are known, our contribution is the wartime-grade adaptation to public alerting: (i) a sovereignty-preserving hybrid control layer; (ii) an integrated cyber-kinetic threat model with spatial redundancy; (iii) offline-capable execution of pre-authorized alert scenarios; and (iv) a vendor-neutral stack blueprint suitable for municipal deployment.

5. Discussion

This work focuses on design choices, operational constraints, and limitations from the authors' perspective. The primary objective is rapid and reliable implementation under wartime conditions with minimal human and financial resources, while maintaining compliance with national cybersecurity requirements and enabling continuous operation amid degraded connectivity.

Regarding the hosting of the management layer, Azure is used here solely as a reference implementation platform to illustrate compatibility with widely adopted cloud security frameworks (e.g., Zero Trust) and international standards (e.g., NIST SP 800-82/207). The proposed model is vendor-neutral and can be implemented on any provider, including a sovereign, government-operated data center, or a localized Azure Stack instance deployed with national operators (e.g., Kyivstar) within the territory of Ukraine. As soon as a state-controlled sovereign cloud becomes available, the control layer can be migrated there to ensure full data sovereignty.

Physical survivability and redundancy are addressed beyond backup power. In this work, we emphasize spatial overlap of alerting zones: each device's coverage is partially duplicated by neighboring units so that audibility is preserved even if one or several nodes are destroyed. In addition, the alerting devices have a modular design that enables field technicians to replace or repair damaged modules within approximately 30 minutes (excluding travel time), which significantly reduces downtime during recovery operations.

In this work, we do not report detailed quantitative validation (e.g., latency distributions, RTO/RPO under controlled failover, or MTTR under simulated faults), as such evaluation requires a dedicated experimental campaign and thus lies beyond the present scope. These measurements are planned as part of ongoing pilot deployments, which are currently being rolled out and tested across several communities. For security reasons, operational specifics (locations and configurations) are not published at this stage; the current phase focuses on data collection and analytics to inform subsequent publications.

Similarly, certain advanced capabilities—such as AI-assisted anomaly detection for control-plane drift, device-health deviations, or spoofed signaling—are not elaborated here, as they require separate investigation and belong to the prospects for further research. Future work will also include comprehensive, vendor-agnostic comparisons with alternative architectures (e.g., legacy VPNcentric or cloud-only control planes) and the publication of target SLOs with reproducible test harnesses.

Overall, the present design prioritizes immediate operational readiness, spatial redundancy, modular maintainability, and cyber-resilient operation for Ukraine's local alert infrastructure, while keeping a clear roadmap for sovereignty, portability, and rigorous quantitative evaluation in subsequent stages.

6. Conclusions and prospects for further research

In the context of the legal framework, the implementation of the Law "On Critical Infrastructure" [11] should provide additional protection mechanisms for LACAS, as such a system clearly belongs to security-related critical infrastructure objects [11]. This implies state oversight of its cybersecurity status, auditing, and information sharing on incidents at the national level.

In summary, the security architecture for the automated alert system proposed in this study demonstrates a sufficient level of protection at present. A system built on the proposed principles can perform its functions even under targeted cyberattacks. Further enhancement of security should be carried out proactively — by implementing cutting-edge protection technologies, conducting regular penetration testing, and adapting to emerging threat scenarios. Only with continuous development of the cybersecurity system can it be guaranteed that LACAS will reliably fulfill its critical role — timely warning people of danger and saving lives in emergencies.

Another promising research direction is the use of artificial intelligence methods for analyzing the behavior of the alert system. For example, ML algorithms can monitor typical patterns of traffic and operator actions, detecting deviations that may indicate intrusions. The alert system could also be integrated into a unified city or regional cybersecurity platform to exchange threat information with other services (energy, transportation, etc.). This would allow early response to complex attacks that may simultaneously affect multiple sectors. In this context, adopting well-established Smart City IoT data-processing pipelines for stream ingestion, edge pre-filtering, and event aggregation—as documented in [18]—can strengthen scalable telemetry handling and enable timely cross-service correlation.

Prospects for further research. A pilot deployment is currently being rolled out and tested across several communities; operational specifics are intentionally withheld for security reasons. We are presently in the data-collection and analytics phase. Future work will focus on longitudinal SLO tracking across seasons, comparative trials against legacy VPN-centric architectures, and integration of AI-assisted anomaly detection (control-plane drift, device-health anomalies, spoofed signaling) with human-in-the-loop triage.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] INL Company. Creation of a local automated alert and information system for the population in the city of Chernihiv: working project [Electronic resource]. – Kyiv, 2023. – 44 p. – Available at: https://chernigiv-rada.gov.ua/storage/files/22/00/00/03/a30cec24a4ffdceed6463241ca75fb20.pdf (accessed: 31.07.2025).

[2] Civil Protection Code of Ukraine: Code of Ukraine dated 02.10.2012 No. 5403-VI [Electronic resource] // Legislative Database of Ukraine / Verkhovna Rada of Ukraine. – Available at: и (accessed: 31.07.2025).

[3] On approval of the Regulation on the organization of alerting about the threat or occurrence of emergencies and the organization of communications in the field of civil protection: Resolution of the Cabinet of Ministers of Ukraine dated 27.09.2017 No. 733 [Electronic resource] // Legislative Database of Ukraine / Verkhovna Rada of Ukraine. – Available at: https://zakon.rada.gov.ua/go/733-2017-п (accessed: 31.07.2025).

[4] On approval of the Concept for the development and technical modernization of the centralized alert system about the threat or occurrence of emergencies: Order of the Cabinet of Ministers of Ukraine dated 31.01.2018 No. 43-r [Electronic resource] // Legislative Database of Ukraine / Verkhovna Rada of Ukraine. – Available at: https://zakon.rada.gov.ua/go/43-2018-р (accessed: 31.07.2025).

[5] On approval of the action plan for the implementation of the Concept for the development and technical modernization of the centralized alert system about the threat or occurrence of emergencies: Order of the Cabinet of Ministers of Ukraine dated 11.07.2018 No. 488-r [Electronic resource] // Legislative Database of Ukraine / Verkhovna Rada of Ukraine. – Available at: https://zakon.rada.gov.ua/go/488-2018-р (accessed: 31.07.2025).

[6] On the basic principles of ensuring cybersecurity of Ukraine: Law of Ukraine dated 05.10.2017 No. 2163-VIII [Electronic resource] // Legislative Database of Ukraine / Verkhovna Rada of Ukraine. – Available at: https://zakon.rada.gov.ua/go/2163-19 (accessed: 31.07.2025).

[7] On approval of the Instruction on practices or procedures for designing, researching, commissioning, operating and maintaining (supporting) automated centralized alert systems: Order of the Ministry of Internal Affairs of Ukraine dated 08.02.2019 No. 93 [Electronic resource] // Legislative Database of Ukraine / Verkhovna Rada of Ukraine. – Available at: https://zakon.rada.gov.ua/go/z0418-19 (accessed: 31.07.2025).

[8] On information protection in information and communication systems: Law of Ukraine dated 05.07.1994 No. 80/94-VR [Electronic resource] // Legislative Database of Ukraine / Verkhovna Rada of Ukraine. – Available at: https://zakon.rada.gov.ua/go/80/94-вр (accessed: 31.07.2025).

[9] Stouffer K., Pease M., Pillitteri V. et al. Guide to Operational Technology (OT) Security. NIST Special Publication 800-82 Rev. 3 [Electronic resource]. – Gaithersburg, MD: National Institute of Standards and Technology, 2023. – DOI: 10.6028/NIST.SP.800-82r3. – Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf (accessed: 31.07.2025).

[10] Hacking attack prompts Russian regional broadcasters to issue air alert warnings [Electronic resource] // Reuters, 28.02.2023. – Available at: https://www.reuters.com/world/europe/hacking-attack-prompts-russian-regional-broadcasters-issue-air-alert-warnings-2023-02-28/ (accessed: 31.07.2025).

[11] On critical infrastructure: Law of Ukraine dated 16.11.2021 No. 1882-IX [Electronic resource] // Legislative Database of Ukraine / Verkhovna Rada of Ukraine. – Available at: https://zakon.rada.gov.ua/go/1882-20 (accessed: 31.07.2025).

[12] Ministry of Internal Affairs of Ukraine. Order dated 05.11.2018 No. 884 "On approval of the Technical requirements for the nationwide automated centralized alert system" [Electronic resource]. – Available at: https://dsns.gov.ua/upload/1/6/1/9/5/2019-5-22-884-05-11-2018.pdf (accessed: 31.07.2025).

[13] State Emergency Service of Ukraine. Order dated 26.07.2018 No. 438 "On approval of the Recommendations for designing and calculating the zone of confident reception of the danger sound signal 'ATTENTION EVERYONE!'" [Electronic resource]. – Available at: https://zakon.rada.gov.ua/rada/show/v0438388-18/ (accessed: 31.07.2025).

[14] MikroTik. CVE-2023-30799: Elevation-of-privilege in RouterOS. – 27.07.2023. – Electronic data. – Available at: https://mikrotik.com/supportsec/cve-2023-30799 (accessed: 07.08.2025).

[15] Holt S. Android 16 will flag fake cell towers and warn you if someone is spying on your phone // TechRadar. – 12.06.2025. – URL: https://www.techradar.com/phones/android/android-16-will-soon-flag-fake-cell-towers-and-warn-you-if-someone-is-spying-on-your-phone (accessed: 07.08.2025).

[16] GBHackers. Viasat modems zero-day vulnerabilities let attackers execute remote code. – 28.04.2025. – Electronic data. – Available at: https://gbhackers.com/viasat-modems-zero-day-vulnerabilities (accessed: 07.08.2025).

[17] Glover C. Russian radio stations hacked with bogus missile warning // Tech Monitor. – 23.02.2023. – URL: https://techmonitor.ai/technology/cybersecurity/russian-hacktivist-missile-alarm (accessed: 07.08.2025).

[18] Duda O., Kochan V., Kunanets N., Matsiuk O., Pasichnyk V., Sachenko A., Pytlenko T. Data Processing in IoT for Smart City Systems // 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2019), 18–21 September 2019, Metz, France. – Piscataway: IEEE, 2019. – Vol. 1. – pp. 96–99. – DOI: 10.1109/IDAACS.2019.8924262.