Journal homepage: https://itce.vn.ua/en

Information Technologies and Computer Engineering **Vol. 23, No. 1. 2026**

Article's History: Received: 17.11.2025 Revised: 19.02.2026
Accepted: 26.03.2026 Published: 20.04.2026

ISSN 1999-9941; e-ISSN 2078-6387
UDC 621.396.6:355.40
DOI: 10.31649/vitce/1.2026.153

Analysis of the construction of a communication network of the tactical control link based on software-defined radio communication means

Hryhorii Radzivilov
PhD in Technical Sciences, Associate Professor
Kruty Heroes Military Institute of Telecommunications and Information Technology
01011, 45/1 Knyaziv Ostrozkykh Str., Kyiv, Ukraine
https://orcid.org/0000-0002-6047-1897

Dmytro Pavliuk*
Adjunct
Kruty Heroes Military Institute of Telecommunications and Information Technology
01011, 45/1 Knyaziv Ostrozkykh Str., Kyiv, Ukraine
https://orcid.org/0000-0001-8461-3899

Abstract. The purpose of the study was to develop an architectural solution for the construction and management of a tactical communication circuit of the company-battalion-brigade levels based on flexible radio platforms to ensure continuity and reliability of communication in conditions of active enemy counteraction. Methods of structural and functional modelling, scenario and comparative analysis were used. It was established that in conditions of electronic warfare (EW), the communication circuit of the company-battalion-brigade levels should be built as a hybrid multi-level architecture, which at the company level combines separate voice communication and data transmission channels, uses a self-organised Mobile Ad Hoc Network based on software-defined radio systems for tactical exchange, and at the battalion level – a gateway node for traffic aggregation, routing, and integration with higher-level communication channels via Low Earth Orbit satellite backhaul. It was shown that Digital Mobile Radio should be used for the voice loop of the command-and-control minimum, Software-Defined Radio Mobile Ad Hoc Network with Multiple-Input Multiple-Output – for the tactical data transmission layer, and LEO satellite backhaul – as a main or backup communication channel between the battalion-brigade levels. An iterative algorithm for planning and configuring the tactical command link communication network in the presence of electromagnetic interference and limited resources was proposed. The advantages of the model were increased availability of the command-and-control minimum, preservation of controllability, prioritisation of traffic by quality of service and controlled degradation of services. Its effectiveness was determined by the continuity of voice communication, data exchange stability, speed of connection restoration and communication redundancy between the company-battalion-brigade levels. The practical significance lies in the possibility of applying the results by specialists of communication units during planning, deployment and adjustment of the tactical communication circuit of the company – battalion – brigade in field conditions in a complex electromagnetic environment and under active countermeasures

Keywords: communication network; self-organising network; multichannel architecture; gateway node; satellite communication channel; electronic warfare

Introduction

Stable communication of the tactical control link (TCL) (company – battalion – brigade) is a basic condition for effective command and control (C2) in an environment with limited radio resources, high mobility, uneven coverage and the effects of electronic warfare (EW). In this context, Software-Defined Radio (SDR) tools and self-organising ad

Suggested Citation:
Radzivilov, H., & Pavliuk, D. (2026). Analysis of the construction of a communication network of the tactical control link based on software-defined radio communication means. *Information Technologies and Computer Engineering*, 23(1), 153-169. doi: 10.31649/vitce/1.2026.153

*Corresponding author

hoc networks are the basis of flexible TCL networks, where the quality of service and survivability are determined not by the "passport" of radio stations, but by the architecture, control algorithms and information security (IS) measures. However, at the tactical level, communication is built from a combination of different carriers (narrowband voice, packet channels based on SDR, satellite backbone channel), but without a formalised methodology for the integration and control under the influence of EW. As a result, the "passport" characteristics of individual devices do not guarantee stable Key Performance Indicators (KPIs) of the network (C2 availability, delay/variation (oscillation) of the delay, delivery reliability, recovery time) and do not ensure systematic consideration of IS requirements.

Modern scientific discourse has proposed a number of approaches to counteracting interference in Mobile Ad hoc Network (MANET). In the study, J. Kim *et al*. (2021) showed that inherent interference effects can critically degrade MANET connectivity if media access and routing protocols do not take into account interference interaction. This emphasises the need for specialised protocols/policies that reduce network degradation under interference effects and preserve the operability of management services. In a broader review, Z. Patel *et al*. (2023) systematised the technological trends of tactical self-organising (ad hoc) networks and showed that the key benefits are not provided by isolated "radio solutions", but by the coordinated design of the radio signal form – network layer – service policies. This formalises the typical trade-offs "delay/bandwidth/survivability/controllability", which leads to the formulation of the problem of multi-criteria optimisation of the TCL network construction. In the work of N. Chen *et al*. (2025), the network challenges of satellite-ground integrated networks were generalised, in particular the problems of routing, mobility, resource management and Quality of Service (QoS) in heterogeneous topology. Such an approach means that effective integration requires communication carrier selection policies and traffic management mechanisms at the network level, and not only at the "satellite connection" level. For the physical layer and transmission mode selection, A. Mureșan & P. Bechet (2024) found that different radio signal forms provide different transmission modes and balance robustness, bandwidth, and delay differently. The authors' findings are useful for formalising the rules for selecting a communication medium in a TCL depending on the type of environment (Line of Sight (LOS)/ Non-Line of Sight (NLOS)) and traffic priorities.

A separate scientific direction is related to the use of Multiple-Input Multiple-Output (MIMO) as a tool to increase resilience and throughput in interference conditions. K.-P. Hui *et al.* (2024) demonstrated at the prototype level the potential of MIMO with interference suppression for tactical communication, where interference can dominate the "clean" radio channel. This reinforces the thesis that MIMO should not be considered as a "speed option", but as an element of link survivability and QoS stabilisation. Additionally, in the work of C.E. Thornton *et al*. (2023) considered the role of sidelink in 5G/5G-Beyond for multi-hop tactical networks and showed that direct inter-device communication via the PC5 interface can support multi-hop connectivity and reduce dependence on centralised infrastructure. This justifies direct inter-device communication via the PC5 interface as an additional communication medium for the self-organising TCL network and reinforces the concept of multichannel architecture.

For Ukraine, taking into account the experience of the Anti-Terrorist Operation (ATO)/Joint Forces Operation (JFO) and the full-scale war since 2022, the construction of communication networks that are rapidly deployed, adaptable to interference, and support multichannel data exchange is of paramount importance. In the study, M. Masesov *et al*. (2021) found that active traffic queue management using fuzzy logic can stabilise latency and reduce the effects of congestion in tactical radio networks. According to the authors, QoS in TCL should be ensured by traffic management, and not only by choosing a "more powerful" channel. In the work of R. Shtonda *et al*. (2023), the authors demonstrated that small-sized digital tropospheric stations can be used as an alternative communication channel in operational conditions to maintain connectivity with limited availability of other means. This justifies tropospheric communication as an additional carrier/backbone channel in the multichannel TCL architecture, which enhances network survivability in the event of degradation of the ground-based self-organising network or in the absence of infrastructure. Analysing the use of software-defined radio communication systems in mobile radio networks, S.V. Salnyk & P.H. Sydorkin (2024) emphasised the role of SDR as a technological basis for flexible configuration of operating modes and integration of various protocols. This forms the basis for considering SDR not as a separate "device", but as a platform for building network functions and adapting to application conditions.

Despite the existing body of works, there remains a gap between individual technological solutions (radio signal form, MIMO, Active Queue Management (AQM), sidelink, satellite channel integration) and a holistic methodology for building a TCL network, which simultaneously takes into account the company-battalion-brigade hierarchy, multi-bearer architecture, QoS/survivability and basic IS requirements. Therefore, the purpose of the study was to substantiate an engineering approach to building and managing a company-battalion-brigade tactical communication circuit based on flexible radio platforms to ensure the reliable functioning of tactical communication under active countermeasures. To achieve the goal, the following tasks were set: to describe the structure of the TCL network (company – battalion – brigade) to form a reproducible planning/configuration methodology (algorithm) taking into account QoS, managed degradation, Satellite Communication (SAT) integration and KPI verification, to compare the characteristics of the main communication technologies, in particular Digital Mobile Radio (DMR), SDR-MANET networks and Low Earth Orbit Satellite (LEO-SAT), to

determine the functional roles in the TCL and to substantiate the KPI-oriented hybrid multichannel TCL model for the conditions of Ukraine "DMR + SDR(MIMO)-MANET + LEO-SAT backhaul".

Materials and Methods

The study was carried out as an engineering and architectural justification for building a communication network for the tactical command link in conditions of active counteraction. Within the framework of structural and functional modelling, the TCL network was presented as a hierarchical-cluster multi-level system of company – battalion – brigade levels, where at the company level subscriber nodes (infantry units, crews, unmanned aerial vehicle (UAV) operators, tablets/terminals, sensors), data access nodes and, if necessary, relay nodes were considered. At the battalion level, aggregation nodes and gateways were identified that provided unification of company segments, traffic prioritisation, routing, relaying, network control and monitoring. At the brigade level, control nodes were identified, within which C2 services, routing, logging and key management were implemented. The types of communication channels considered were DMR channels for the C2-minimum voice circuit, SDR-MANET channels for tactical packet data exchange, and a satellite backhaul channel for main or backup communication between the battalion and brigade levels. Topologically, the network was described as a combination of local company clusters, united through battalion gateway nodes into a hierarchical structure, where mesh or ad hoc interaction prevailed within the clusters, and gateway and main connections were implemented between the control levels (Fig. 1).

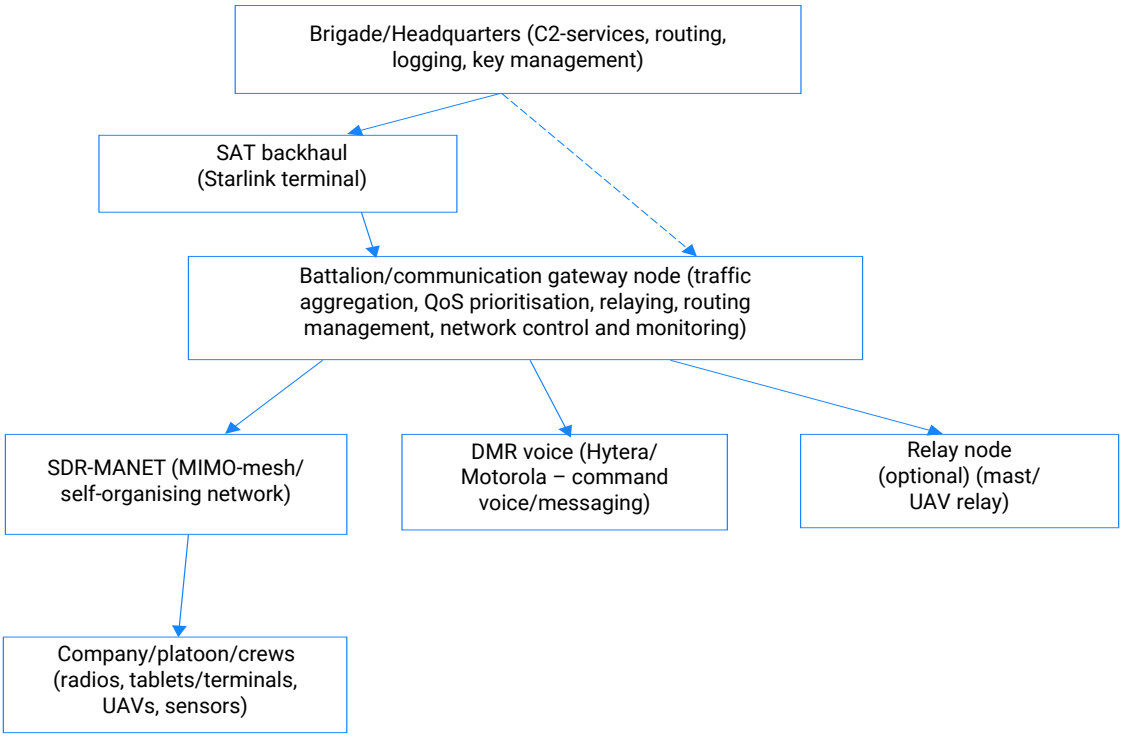

Figure 1. Architecture of the TCL communication network

Source: compiled by the authors based on European Telecommunications Standards Institute (2016), J. Suess (2022), V.H. Sholudko *et al.* (2023), A.A. Hrozdov *et al.* (2024), L. Bojor *et al.* (2024), P.V. Khomenko *et al.* (2025)

The European Telecommunications Standards Institute (2016) standard was used as a regulatory basis for the analysis of the DMR voice circuit, which provided C2 radio exchange, and the architectural model of the company-battalion-brigade circuit was used as an input basis for further analysis of technologies, KPIs and network operation scenarios, in particular for determining the battalion communication node – gateway as a key element of traffic aggregation, routing, QoS prioritisation and route reservation. The described architectural model was used as an input basis for further analysis of communication technologies, determination of KPIs, operation scenarios and formation of the TCL network construction algorithm. Using the method of comparative and system analysis, typical communication means were compared: Hytera (2018) Professional Digital (PD)7i (China) and Motorola Digital Mobile (DM)4000e (USA) (Motorola Solutions, 2026) as typical representatives of DMR for basic voice C2 (Push-To-Talk (PTT)/C2-minimum); Silvus StreamCaster (SC)4400 Enhanced (E) (USA) (Silvus Technologies, 2025) – as a representative of SDR-MANET (MIMO) for tactical broadband data exchange; Starlink (2026) (USA) – as LEO-SAT backhaul/reserve at the battalion-brigade level. These models of communication means as representatives of different technological classes were chosen because such systems were used in real combat missions in the conditions of war in Ukraine during

2022-2025. The comparison was performed according to the engineering-role principle and in conformity with the basic technical parameters: technological class, band/channelling, frequency ranges, power, bandwidth, delay, scalability, MIMO/beamforming, encryption and IS, since it was these parameters that comprehensively characterised deployment, QoS, survivability/scalability and IS in countermeasure conditions.

The method of structural-logical classification systematised the distribution of communication services and technologies in the TCL according to the following criteria: priority services, main technology, reserve/hybrid, sequence of controlled degradation and minimum IS requirements. This approach unified the policy of prioritisation and degradation between levels and the preservation of basic IS mechanisms even in the minimum mode (encryption, key management/zeroize, segmentation of C2/data domains, protection of gateways and control nodes). Using the method of system analytical synthesis, an applied framework for assessing the stability of TCL communication was formed, a set of KPIs focused on the minimum required command and control services was determined, and a field verification protocol was proposed (control pairs of nodes, traffic profiles, measurements in three modes: normal/overload/interference-EW) with fixation of the sequence of service degradation. For this, the National Institute of Standards and Technology standard (2001; 2019) was used as a normative basis, and the AES algorithm was considered as a basic guideline for describing the requirements for traffic encryption in TCL.

Using the method of systematic analysis of the experience of using tactical communication of the Armed Forces of Ukraine in real combat conditions, typical application scenarios for Ukraine (city/NLOS, partial NLOS, LOS with vulnerability to EW, variable LOS) were systematised and translated into engineering requirements for communication media and topology (node density, relay, multichannel mode, readiness for SAT) and modern requirements for TCL were formed. The source base was the analytical report by J. Watling & N. Reynolds (2023), as the context of combat conditions 2022-2023, the annual report of L3Harris Technologies, Inc. (2024), as an indicator of practical relevance on the practical significance of SDR/network solutions. The formed requirements were used as a basis for substantiating the hybrid architecture of the TCL network "DMR + SDR(MIMO)-MANET + LEO-SAT backhaul", determining the functional distribution of roles between its components and further developing an algorithm for its planning and configuration. At the final stage, a logical-algorithmic generalisation of the engineering approach to building a TCL network was applied, within which a step-by-step algorithm was formed, covering the collection of input data, determination of optimisation criteria, design of the C2-minimum and data layer, selection of gateway nodes and relay facilities, QoS settings, integration of SAT, implementation of IS measures and iterative verification of KPIs with correction of network parameters. This was done in order to standardise engineering solutions during planning, deployment and operational management of tactical communication and to ensure guaranteed operability of priority services with limited resources and the influence of EW.

Results and Discussion

Hierarchical architecture and choice of communication technologies for tactical control link under EW conditions

To ensure the effectiveness of tactical communication at different levels of control, it is necessary to take into account not only the technical characteristics of communication facilities, but also the ability of the network to adapt to changing conditions, such as EW and limited resources. In this context, it is important to use such a TCL network that allows for communication stability with minimal loss of connectivity, while optimising the use of technologies to ensure proper controllability and reliability. In the current study, the TCL communication network is considered as a multi-level system of nodes and channels at the company – battalion – brigade levels, where each level has its own functions, services, and requirements for stability under EW conditions. This approach corresponds to the practice of organising military communication, within which communication is considered as an element of the control system, and not as a set of individual radio stations (Sholudko *et al*., 2023).

Within the framework of the analysed model at the company level, the priority is to ensure C2-minimum (command voice, short messages/coordinates) with simple deployment and resistance to local node losses. It is engineeringly expedient to divide the voice control channel and the data channel so that loaded services do not degrade control (Hrozdov *et al*., 2024). To implement the voice control channel, DMR, standardised by the European Telecommunications Standards Institute (2016), is used, which supports basic group services and typical radio exchange organisation modes. At the same time, a local SDR-MANET segment is formed for data transmission and situational awareness (SA), capable of self-organisation and self-recovery of routes during movement and loss of some nodes. Increasing the efficiency of data exchange – increasing the throughput and noise immunity of the MANET segment – is associated with the use of MIMO approaches, in particular in the context of countering jamming, which is relevant for an environment with intensive EW.

The battalion level performs traffic aggregation and routing functions, for which gateway nodes are formed that unite company segments, perform docking of MANET ↔ Internet Protocol (IP) services and implement the QoS traffic prioritisation mechanism, provide redundancy and controlled degradation of services. In addition, these nodes monitor and log the network status taking into account the requirements of electromagnetic discipline (Sholudko *et al*., 2023; Hrozdov *et al*., 2024). Gateway nodes not only perform traffic aggregation and routing, but also have the task of

maintaining network stability, guaranteeing its ability to self-organise and restore routes when the topology changes. This allows the network to function effectively even in the event of malfunctions or losses of some nodes, which is important for ensuring continuous communication in EW conditions or in combat.

At the brigade level, a control backbone is formed that integrates C2 services and provides communication with higher levels via a satellite channel. However, the impact of cyber impacts and jamming on the space and ground communication segments necessitates considering the satellite channel as a managed resource with mechanisms for prioritisation, degradation, and redundancy (Bojor *et al.*, 2024). This allows for the stability of communication between the battalion and brigade levels, even in the event of serious interference. At the brigade level, the satellite channel is the main backbone channel for communication with higher levels, but to ensure reliability and fault tolerance, this channel is supplemented with backup paths, such as SDR-MANET for alternative traffic, which allows for quick switching to other channels in the event of malfunctions or high interference.

Thus, the engineering model of the TCL network should be built as a hierarchical multilayer system: DMR provides reliable command voice communication and short messages at the tactical level; SDR-MANET with MIMO forms a resilient tactical layer for data transmission with self-organisation and self-recovery of routes; and SAT backhaul is used as a backbone channel for communication between the battalion and the brigade, with support for redundancy and traffic prioritisation. Such a hybrid architecture allows maintaining a high level of network adaptability to changes in topology and electromagnetic interference conditions, which makes it resistant to interference and ensures continuous communication at all levels of control. At the same time, the use of different levels of redundancy and degradation of services ensures that even under conditions of high load or failures, key services, such as C2, will remain available.

For the effective practical implementation of the considered TCL network model, it was important to analyse available communication technologies that can be applied in different segments of the tactical architecture. Comparison of technologies is necessary to select the most optimal solutions, taking into account the requirements for resilience, scalability, and QoS in conditions where the network is exposed to EW and changes during combat operations. Since the technologies used belong to different classes and perform specific functions in the network architecture (from portable radios to satellite channels), the comparison was not a direct "one-to-one" comparison. Instead, key technical parameters that directly affect the performance of the TCL network, such as bandwidth, latency, scalability and security capabilities, were considered. This allowed comparing technology classes that represent specific models of real-world communication facilities that can be used in the corresponding TCL circuits (Table 1).

Table 1. Technical characteristics of communication facilities for TCL circuits

Parameter	Hytera PD7i (portable DMR)	Motorola MOTOTRBO DM4000e (automotive DMR)	Silvus SC4400E (SDR-MANET node)	Starlink (LEO satellite channel, backhaul)
Technology/class	DMR (Tier II/III)	DMR (Tier II/III)	SDR-MANET (MN-MIMO)	LEO satellite broadband channel (SATCOM)
Channel bandwidth/ channel spacing	12.5/20/25 kHz (channel step)	12.5/20/25 kHz	20/10/5 MHz (opt. 2.5/1.25)	depends on the service/ terms
Frequency ranges	VHF 136-174; UHF 400-470/450-520/350-400; 210-270; 806-941 (for trunking)	136-174; 300-360; 350-400; 403-470; 450-527 MHz	Available ranges from 300 MHz to 6 GHz	The terminal's RF band is not fixed
Transmitter power	VHF: High 5W/Low 1W	High 25-45 W (depending on range)	"Native transmit power" up to 20 W (depending on configuration/model), efficiency increased by beamforming	Not used as "radio station power" within the scope of TCL role comparison
Bandwidth (class/typical)	Limited to DMR class (voice + basic data services)	Limited to DMR class (voice + data services)	Up to 100 Mbps (adaptive)	25-220 Mbps (downlink), 5-20 Mbps (uplink)
Latency (class/typical)	Suitable for PTT/voice (class)	Suitable for PTT/voice (class)	Average ~7 ms (at 20 MHz)	Typically 25-60 ms on land
Network scalability	Depends on network/relay organisation	Depends on configuration (MOTOTRBO network modes)	550+ nodes	Depends on coverage/load
MIMO/ beamforming	No (as DMR class)	No (as DMR class)	4×4 MIMO, beamforming; spatial multiplexing	Not a "tactical mesh network", the terminal uses an antenna with electronic beam steering within the system

Table 1. Continued

Parameter	Hytera PD7i (portable DMR)	Motorola MOTOTRBO DM4000e (automotive DMR)	Silvus SC4400E (SDR-MANET node)	Starlink (LEO satellite channel, backhaul)
Encryption and IS	AES/ARC4, end-to-end + over-the-air, analogue scrambling	AES-256 (declared in features)	DES56 (standard), AES256 (optional), Zeroize Crypto	Jamming/cyber-impact risks confirmed, service encryption parameters not detailed

Note: AES – Advanced Encryption Standard; ARC4 – Alleged RC4; RC4 – Rivest Cipher 4; DES – Data Encryption Standard
Source: compiled by the authors based on Hytera (2018), National Institute of Standards and Technology (2019), European Telecommunications Standards Institute (2023), D. McCrory (2023), L. Bojor *et al*. (2024), Silvus Technologies (2025), Motorola Solutions (2026), Starlink (2026)

Analysis of the table data showed that DMR technology is appropriate for use as a basic TCL layer, intended primarily for organising PTT communication and transmitting short service messages. Its advantages are relative ease of implementation, energy efficiency, proven solutions and suitability for operation in conditions of limited infrastructure. At the same time, the data transmission capabilities of this class of systems remain limited, which does not allow considering DMR as the main technology for supporting modern situational awareness services, telemetry and other streaming or broadband applications. The bandwidth of DMR is limited by the class of technology, which allows efficiently processing only voice traffic and basic data services, but it cannot support high-speed applications such as video or big data.

SDR-MANET technology fundamentally differs from DMR in that it is focused on broadband tactical data exchange in dynamic network topology. Its key advantages are self-organisation, multi-hop routing, self-recovery of routes, as well as support for MIMO and beamforming mechanisms. Together, this provides higher throughput, greater resilience to changes in the radio environment and better suitability for supporting situational awareness services in a complex electromagnetic environment. The bandwidth of the presented SDR-MANET model (Silvus SC4400E) – up to 100 Mbps (adaptive) – enables the support of broadband services that are critical for modern military applications, such as video surveillance or big data transmission. This makes this technology an ideal solution for tactical networks with high bandwidth and adaptability requirements.

The technical characteristics of the Starlink SAT model (the model's bandwidth ranges from 25 to 220 Mbps for downlink and 5-20 Mbps for uplink) show that LEO-SAT backhaul allows for effective communication between battalion and brigade levels even under difficult conditions with high loads. However, due to the higher latency (25-60 ms), the satellite channel is not suitable for tactical data exchanges in real time. Therefore, within the proposed architecture, LEO-SAT backhaul technology is considered not as an element of a tactical mesh network, but as a backbone or backup channel for communication between higher levels of control. Its use is advisable due to its high bandwidth and acceptable latency, which allows for traffic aggregation and access to a higher-level network. However, the use of such a channel requires a controlled operation mode taking into account the risks of jamming, cyber impact, as well as the dependence of actual service parameters on the system operating conditions.

According to IS criteria, not only encryption algorithms were of crucial importance, but also key management mechanisms, access control, and the ability to quickly reset or destroy cryptographic parameters (zeroize) in case of a threat of compromise. All technologies presented in the table support encryption (AES, DES, ARC4), which provides a basic level of information protection. However, each technology has its limitations, in particular, encryption in LEO-SAT is not detailed, which may create additional risks in the context of cyber threats. Encryption mechanisms can affect data transfer speed and network latency. For DMR, where encryption is used for voice channels, the impact on data transfer speed is insignificant, since such channels are designed to transmit small amounts of data (voice, short messages). However, for SDR-MANET systems with large amounts of data, such as situational awareness, additional encryption mechanisms can lead to increased latency due to processing of large data and high requirements for computing power, which is important to consider when planning a TCL network. Therefore, a hybrid model is technically justified for the TCL, in which DMR is used to provide the minimum necessary control loop, SDR-MANET as the main tactical data layer, and LEO-SAT as a backhaul layer with QoS policies and redundancy. The comparison showed that the DMR channel should be used as a voice C2 loop, which provides minimal system controllability even in the event of degradation or loss of the data network. SDR-MANET should serve as the main tactical data transmission channel, as it provides network self-organisation, multi-hop routing and support for situational awareness services. LEO-SAT backhaul should be used as a backbone or backup battalion-brigade communication channel, designed for traffic aggregation and access to a higher-level network.

The results of the engineering analysis of the roles of communication channels in the tactical control link indicate that at the company level, it is reasonable to divide the voice control channel and the data channel so that loaded services do not cause control degradation. This statement is consistent with Y.W. Lo *et al*. (2024), who analysed the use of DMR in an applied monitoring system and pointed out the need to evaluate the reliability and performance of services under real load conditions. The researchers treat DMR not as a "default channel", but as a technology layer with measurable characteristics. In the context of TCL, this supports the interpretation of DMR given in the current study as a basic C2 loop (voice and short messages) with predictable behaviour, while data exchange and SA should be moved

to a separate SDR-MANET segment to avoid competition for resources within the critical control loop. Accordingly, separating the circuits has not only architectural but also methodological meaning: it allows setting KPIs separately for C2 and for SA/data and checking the performance under conditions of changing load and interference.

In the study by J. Suomalainen *et al.* (2022), tactical mobile networks were considered as isolated tactical segments in which cyber defence and response mechanisms must operate autonomously and cannot rely on the constant availability of a remote Security Operations Centre (SOC). The key conclusion of the authors is that traffic prioritisation must be security-oriented and dynamic: priority decisions are based on traffic analysis and security posture assessment, and as an example of an "intelligent" response to availability threats, dynamic adjustment of live video stream quality parameters is demonstrated. In the current study, these provisions are related to the fact that the criterion for the success of building a TCL network is the implementation of KPIs of priority services with the dominance of the C2-minimum, and at the battalion level, the functions of QoS prioritisation, managed degradation, and monitoring/logging were concentrated in the gateway node, which serves as a practical point of implementation of such dynamic policies under resource shortages under EW conditions.

The functional role of the gateway node at the battalion level is justified by the concentration of aggregation and traffic management functions, which provides MANET ↔ IP docking, QoS prioritisation, redundancy, and managed degradation of services. This approach is conceptually consistent with R. Mahmud *et al.* (2021), who considered SDN-oriented tactical networks as multi-domain systems, where the key condition for supporting heterogeneous services is policy-driven orchestration. The authors proposed a multi-layered Software-Defined Networking (SDN) architecture that provides monitoring and aggregation of network state for orchestrating services in terms of resilience, compatibility, and policy enforcement. In such an architecture, the gateway performs the role of implementing service management policies at the interface of domains, providing monitoring and logging of network state. Therefore, optimality is determined not by the total throughput, but by preserving the operability of priority services by limiting secondary traffic.

According to the analysis of the role of the satellite channel, at the battalion-brigade level it should be considered as a managed backhaul resource that requires prioritisation, degradation, and reservation policies. This statement is consistent with the work of M. Kang *et al*. (2024), which systematises threats to satellite systems in terms of confidentiality, integrity and availability, emphasising the presence of real incidents and the need for not only technological, but also political and organisational countermeasures, which actually leads to the need for "controllability" of the satellite domain at the level of resource access policies. In the study by V.S. Kantheti *et al*. (2023), an anti-jamming approach for cooperative LEO satellite constellations based on distributed combining of received signals (distributed Maximal Ratio Combining (d-MRC), distributed Linear Minimum Mean Square Error (d-LMMSE)) is considered, the effectiveness of which was tested on a hardware and software stand based on SDR. These results are consistent with the current study that satellite backhaul is considered a resource sensitive to EW: the presence of specialised anti-jamming solutions confirms that the interference immunity of the satellite segment is a separate engineering problem. In the proposed TCL architecture of this study, the satellite backhaul channel (LEO/Starlink) must be planned as a managed resource with redundancy and managed degradation/switching modes.

A comparison of communication technologies for the tactical control link showed that for each level of the TCL network it is advisable to use specific technologies – DMR, SDR-MANET and LEO-SAT backhaul, based on the technical characteristics and capabilities. These technologies interact with each other, creating a hybrid architecture in which each of these technologies performs its role, ensuring network stability even in difficult EW conditions. The use of separate circuits for voice control and data transmission allows optimising the network, ensuring continuity and efficiency of operation at all levels of control.

Functional distribution of services and requirements for the TCL network under EW conditions

For the effective operation of the tactical command link network, it is important not only to determine the technical characteristics of the communication means used, but also to configure the functional distribution of services between the TCL levels, taking into account the roles of nodes at each level, which were described in the previous section. Proper organisation of this distribution allows for the optimal combination of different communication technologies, ensuring the priority of important services and creating degradation mechanisms in conditions of limited resources or EW influence. Determining these aspects is critical for ensuring the uninterrupted operation of the TCL network in difficult combat conditions. The functional distribution of technologies and services between different TCL levels, as well as the specified degradation modes and minimum IS requirements for each level are given in Table 2.

Table 2. Distribution of communication services and technologies in the tactical command chain link (company – battalion – brigade) and degradation modes

TCL level/node role	Priority services	Basic technology	Reserve/hybrid	Degradation mode	Minimum IS requirements
Company/ subscriber mode (infantry, crews)	C2-minimum voice, short messages/ statuses	DMR	MANET (via a gateway, if available)	Cutting off "heavy" data → only short messages → C2-minimum (voice)	Encryption; key management/zeroize, minimising open services

Table 2. Continued

TCL level/node role	Priority services	Basic technology	Reserve/hybrid	Degradation mode	Minimum IS requirements
Port/gateway (voice ↔ data)	Voice-data gateway, local routing/ aggregation	DMR + MANET	DMR-only (in degradation)	Video/high bitrates → COP with less frequent updates → short messages + voice	Voice /data key domain separation, gateway authentication, access policies
Battalion/HQ aggregator	C2 data, COP, dispatching, telemetry	SDR MANET (MIMO/mesh)	DMR (voice) + SAT (backhaul if needed)	ISR/video → COP update rate reduction → "control only" (CU/C2 + critical messages)	C2/data segmentation, network management protection, access prioritisation
Battalion/SAT gateway node (if needed)	BLOS/backhaul boot to brigade/senior level	SATCOM (Starlink)	MANET (last mile) + DMR (voice)	Background traffic → C2/service data only → emergency minimum profile	Crypto overlay over the internet channel, access control, endpoint protection
Brigade/ inter-battalion integration node	Stream integration, COP, resource management	MANET + SAT backhaul	DMR (voice C2)	ISR/video → COP with less frequent updates → C2-minimum	Domain-role access model (br/battalion/ company), key distribution, event auditing
Brigade/ strategic backhaul node	Channel to senior level/ interdepartmental interaction	SATCOM	Alternative transport channels (where available)	Non-critical traffic → "management only" → "store and forward" mode for messages	Crypto protection + endpoint control, anti-eavesdropping/ spoofing protection, cyber/EW risk management

Note: ISR – Intelligence, Surveillance, and Reconnaissance
Source: compiled by the authors based on National Institute of Standards and Technology (2001; 2019), European Telecommunications Standards Institute (2016), O. Lavrut *et al*. (2019; 2021), J. Suess (2022), V.H. Sholudko *et al*. (2023), A.A. Hrozdov *et al.* (2024), P.V. Khomenko *et al*. (2025), Silvus Technologies (2025), S. Halwa & L. Harriss (2025), Starlink (2026)

The above matrix confirms the feasibility of a multilayer communication architecture of the TCL according to the primary/fallback bearer principle, where each layer uses the optimal technology for its tasks, taking into account the possibility of degradation when resources are limited. At the company level, the priority is C2-minimum (voice and short messages): DMR provides basic availability, and MANET is used for data transmission in the presence of a gateway. This allows maintaining communication even under limited resource conditions. At the battalion level, where data aggregation and distribution functions (COP, telemetry) are concentrated, SDR-MANET (MIMO/mesh) acts as the main transport layer, and SATCOM acts as a managed backhaul for BLOS and redundancy in case of degradation of the ground topology. At the brigade level, integration between battalions and access to higher levels require a combination of MANET+SAT backhaul with a fixed minimum service profile as a condition for maintaining manageability.

The degradation sequence (limiting high-bitrate ISR/video services, reducing the COP update rate, switching to "control only" mode) supports the prioritisation of critical functions and reduces the risk of network overload. At the same time, degradation should not be accompanied by the abandonment of basic IS mechanisms: encryption, key management/zeroize, C2 segmentation, and protection of control nodes and gateways remain necessary in the minimal mode. Thus, the table formalises the engineering logic of building a TCL network as a hybrid system with many bearers, where MIMO-MANET provides performance and adaptability, DMR provides basic C2 availability at the lower level, and SATCOM provides a backup/transport circuit for BLOS integration between the battalion and the brigade.

The experience of the war in Ukraine has shown that the main problem of tactical communication is not just voice radio exchange, but stable network interaction in conditions of EW, manoeuvre, node losses and the need for operational data exchange between control levels (Watling & Reynolds, 2023). That is why traditional DMR devices, despite the suitability for command voice and short messages, cannot fully meet the needs of TCL, since these devices belong to narrowband systems and are not designed for broadband tactical data exchange and flexible multi-hop networking (European Telecommunications Standards Institute, 2016). In contrast, SDR-MANET platforms with MIMO, such as the Silvus SC4400E, provide higher throughput, spatial immunity to interference, as well as self-organisation and self-healing of routes, which allows more effectively maintaining network connectivity in a complex electromagnetic environment (Silvus Technologies, 2025).

For TCL, performance indicators should characterise not only "channel quality", but also the ability of the network to maintain controllability under conditions of EW, node losses and resource shortages. In applied methodologies,

resilience is considered an integral category related to immunity to interference and cybersecurity, and should be suitable for operational application (Hrozdov *et al.*, 2024). Given the nature of the threats in the war in Ukraine, KPIs should be oriented towards the C2-minimum and managed degradation of services. The recommended set of KPIs for TCL includes: C2-minimum availability between key nodes, end-to-end (end-to-end) delay of delivery of commands and critical messages, latency variation for voice and streaming services, throughput by traffic class (SA/telemetry as priority data, high-bitrate streams, only if resource is available), PTT/group call setup time, recovery time after node/link loss, resilience to EW/cyber impacts, including taking into account combined threats for the satellite segment.

For practical verification of KPI, it is necessary to apply a simple protocol during exercises/deployments: define control pairs of nodes (company ↔ battalion, battalion ↔ brigade, adjacent companies), set traffic profiles (C2-minimum, SA/telemetry, flows "if resource is available") and take KPI in three modes: regular, with resource shortage (simulation of overload) and with interference/EW (simulation of degradation), fixing the sequence of disconnection of services according to the degradation policy. In the TCL, "range" should be interpreted as coverage determined by LOS/NLOS, terrain and buildings, antenna solutions, node density and EW level, respectively, coverage is the result of network organisation (planning, backup routes/frequencies, counteraction to interference), and not a constant passport value (Sholudko *et al.*, 2023). In order to effectively address these challenges in real-world combat environments, it is necessary to properly organise the network topology and technology selection based on signal propagation scenarios in different environments. Table 3 below shows typical signal propagation scenarios and corresponding network topologies for TCL, including changes under EW conditions, manoeuvres, infrastructure changes, and the need to adapt to various geographical conditions.

Table 3. Signal propagation scenarios and corresponding network topologies for TCL

Scenario	Signal propagation conditions	Technologies and network solutions	Degradation mode
City (NLOS, multipath)	"Radio shadows" and unstable links, multipath propagation	SDR-MANET priority for data, DMR for voice, self-healing mesh network, relay.	Cut off "heavy" data → only short messages → C2-minimum (voice)
Forest belts/plantations (partial NLOS)	Coverage fragmentation, reduced signal density over long distances	A denser network of nodes, repeaters, gateways, multichannel network with multiple transport carriers.	Shorter hops, higher node density, thoughtful placement of repeaters/gateways
Open terrain (LOS, EW vulnerability)	Better connectivity, but possible sharp drops under interference under EW conditions	SDR-MANET for data, SAT backhaul for backup, mode adaptation, route backup, readiness for transition to SAT.	Adaptation of modes, reservation of routes
Rough terrain (variable LOS)	Geometric "shadows" and gaps, changes in the line of communication	SDR-MANET for network self-organisation, fast rerouting, alternative routes, local autonomy of subnets.	Fast rerouting, alternative routes/gateways

Source: developed by the authors

All scenarios emphasise the importance of network adaptation to different signal propagation conditions, which makes it possible to flexibly and effectively manage tactical TCL networks in real combat conditions. The experience of combat operations in Ukraine has shown that the TCL communication network degrades under the combined influence of: high density of EW/interference, absence or destruction of infrastructure, rapid topology changes (manoeuvre, loss of nodes), difficult propagation conditions (NLOS), spectrum congestion and cyber risks (compromise of terminals, interception, attacks on gateways/endpoints). Under such conditions, static planning that depends on a single transport medium leads to a decrease in availability and an increase in recovery time, which directly affects the control cycle (company – battalion – brigade) and maintaining COP/data exchange (Halwa & Harriss, 2025). The engineering conclusion is the feasibility of a multilayer architecture in which the tactical data layer is implemented on the basis of a self-organising and self-healing MANET, and maintaining manageability is ensured by QoS prioritisation, managed degradation, and KPI-oriented stability verification.

In the conditions of war in Ukraine, threats to TCL communication are complex and include both electromagnetic and informational and cybernetic influences. The basic risks include interception and eavesdropping due to the use of unprotected or incorrectly configured channels, as well as jamming and electromagnetic incompatibility/mutual noise phenomena at high density of means in the common air. A separate group is made up of influences on navigation components, including spoofing, which complicate the use of modes and services dependent on navigation support. For the backbone component, cyber impacts on the satellite

segment and jamming of satellite terminals are critical, which increases the vulnerability of SAT backhaul and justifies the need for architectural redundancy. Given the above threats, the implementation of command and control (C2) exchange in the TCL should provide for cryptographic protection of traffic and correct organisation of key material at the radio network and terminal levels. As an example of an engineering implementation for tactical SDR-MANET nodes, the Silvus SC4400E specification provides support for DES56 (standard) and AES256 (optional), the presence of the zeroize function and declared compliance with the National Institute of Standards and Technology (2019) as a characteristic of the cryptomodule level. In combat conditions, taking into account the probability of loss/capture of nodes, the availability of procedures for the operational destruction of cryptomaterial and minimising the consequences of potential compromise of a node for the entire network are critical.

Based on the real combat experience of using tactical communication in Ukraine and technological capabilities, the key requirements for the TCL network in conditions of mobility and limited infrastructure were summarised:

1. Mobility and limited infrastructure. The TCL network must support the mobility of units and function in conditions of limited infrastructure capabilities. This includes adaptation to rapid topology changes and the availability of backup channels for communication.

2. Digitalisation and networking. The need for digital means of communication has become urgent, providing not only voice transmission, but also support for various data and integration with other systems, including automation of unit management processes.

3. C2 availability and recovery time. This shifts emphasis away from "passport range" to the availability of minimum C2, in particular voice communication and short messages, during resource shortages or in conditions of electromagnetic effects. Rapid restoration of communication after the loss of nodes or channels.

4. Comprehensive IS. Ensuring network IS, including traffic encryption, key management, domain segmentation, access control, as well as implementing service minimisation policies and operational destruction of cryptographic materials (zeroize) in case of compromise.

5. Adaptation to electromagnetic interference (EW). The network must be resistant to EW and other interference that can disrupt or degrade data transmission. This includes the use of self-organising and self-healing technologies, such as SDR-MANET.

6. Protection against interception and cyber risks. Ensuring protection against interception and compromise of data, especially in tactical networks, where there may be attacks on endpoints and gateways.

7. Flexibility of network topology. Considering various signal propagation scenarios in different conditions (city, forest, open areas), the network must be flexible, with the ability to adapt to topology changes. The important things are the thoughtful placement of repeaters and gateways, support for multichannel networks, and adaptation to EW conditions.

8. Scalability and manageability. The network must have the ability to scale under conditions of increased load and ensure communication stability even with partial loss of nodes or changing conditions.

These requirements determined the basis for the development of an algorithm and engineering model of a communication network for the TCL, which must provide high adaptability, stability, and security in difficult conditions. In general, building a TCL network and planning its deployment requires not only adaptation to changing operating conditions, but also the integration of modern technologies capable of ensuring stability, mobility, and communication security in combat conditions. The proposed criteria and principles, in particular the use of hybrid technologies and controlled degradation of services, are key to ensuring the effective operation of the TCL network in difficult EW conditions, limited resources, and high cyber threats.

Algorithm for designing and configuring a TCL network under conditions of EW and electromagnetic effects

The "DMR + SDR(MIMO)-MANET + LEO-SAT backhaul" model presented in the current study takes into account all the above requirements and is focused on ensuring C2-minimum and maintaining controllability under conditions of EW, node losses and degradation of individual channels. Such a system can help ensure uninterrupted control in complex combat situations. The practical implementation of the proposed model requires a formalised sequence of engineering solutions that connects the choice of network architecture with the procedures for its planning, configuration and verification. For this purpose, a step-by-step algorithm for designing and configuring a TCL communication network under conditions of limited resources and electromagnetic effects is proposed. The algorithm covers input data collection, optimisation criteria definition, C2-minimum and data layer design, gateway and relay node selection, QoS and managed degradation mode configuration, SAT integration, IS implementation, and iterative KPI verification with subsequent network parameter adjustment. A generalised algorithm diagram is shown in Figure 2.

Figure 2 should be interpreted as a detailed algorithm for the phased design, configuration, verification and adjustment of the TCL communication network in the "company – battalion – brigade" loop under EW conditions. The algorithm is focused on ensuring the functional suitability of the network for performing management tasks. The ultimate criterion for its effectiveness is not the maximisation of total throughput, but the guaranteed provision of C2-minimum, communication stability, controlled degradation of services and network recoverability after the loss of nodes or channels.

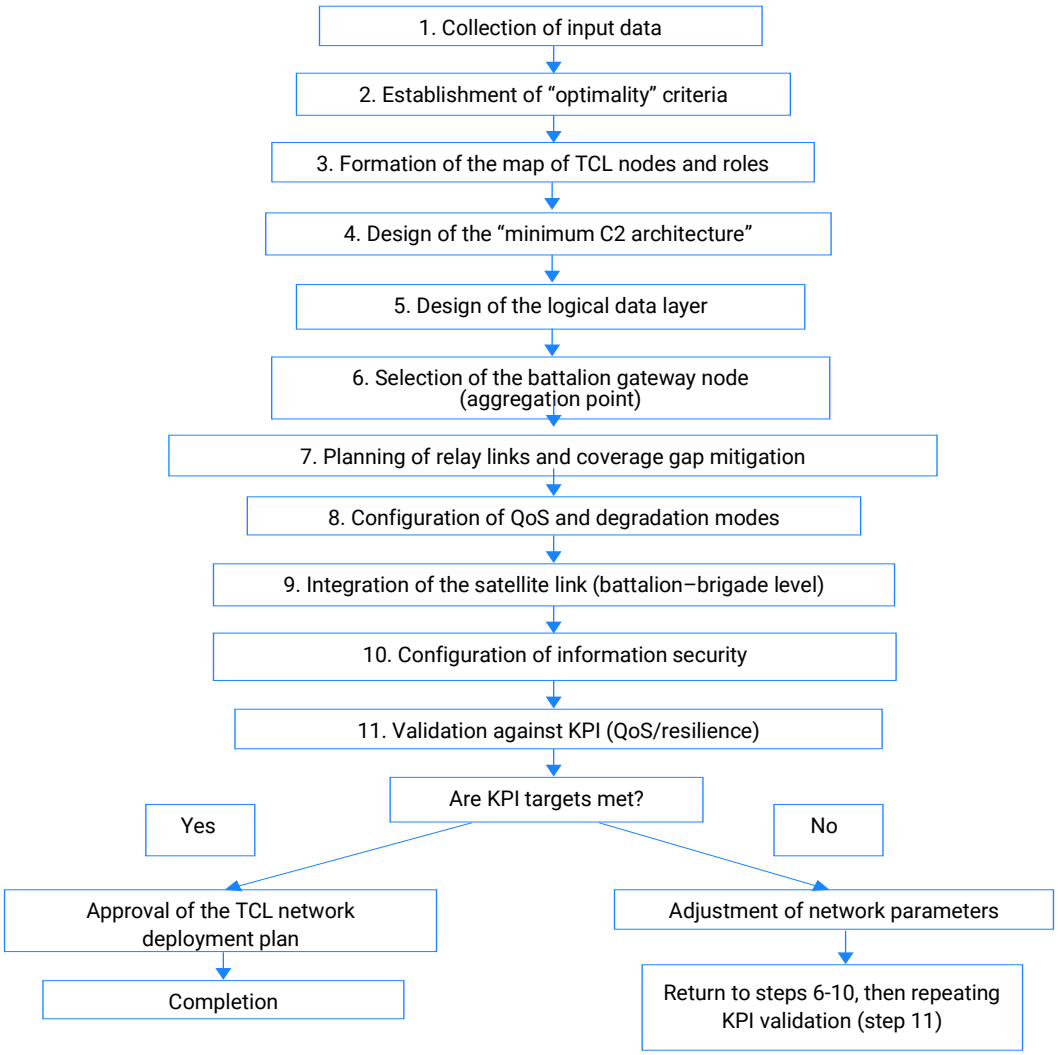

Figure 2. Generalised scheme of the algorithm for designing and configuring a TCL communication network under EW conditions

Source: compiled by the authors based on National Institute of Standards and Technology (2001; 2019), European Telecommunications Standards Institute (2016), O. Lavrut *et al*. (2019; 2021), J. Suess (2022), V.H. Sholudko *et al*. (2023), A.A. Hrozdov *et al*. (2024), P.V. Khomenko *et al*. (2025), Silvus Technologies (2025), S. Halwa & L. Harriss (2025), Starlink (2026)

In step 1 – input data is collected, which determine the initial conditions for building the network. At this stage, the features of the area of operations are analysed, in particular the terrain, the nature of the development, the presence of radio shadow zones, expected radio conditions and probable spatial restrictions for the placement of nodes. Additionally, the composition and number of network elements at the company, battalion, and brigade levels are determined, the presence or need for relaying is assessed, and a list of services that must be supported by the network is formed: command voice exchange, transmission of commands and coordinates, situational awareness data, telemetry and, if resources are available, streaming data. At the same time, EW threats, cyber threats, risks of equipment loss, as well as the probability of degradation or loss of the satellite channel are taken into account. It is at this step that the available technological set of the network is fixed: DMR as the basis for stable voice C2 exchange, SDR-MANET as the basis for a self-organised data layer, and the satellite channel as a main or backup means of communication between the battalion and brigade levels.

In step 2 – the criteria are established according to which the network is considered suitable and meets the requirements for performing the task. At this stage, the network requirements are formalised through coverage, connectivity, survivability, QoS, electromagnetic compatibility, and IS indicators. The priority criterion is the guaranteed provision of the C2-minimum even with partial degradation of services, and lower priority information flows may be limited. Also, requirements are set here for the minimum permissible availability of the command channel, permissible delays, route stability, speed of recovery after node loss, as well as for radio discipline, radiation control, and cryptographic protection modes.

Step 3 – a map of TCL nodes is formed and the roles in the network are determined. At the company level, subscriber nodes and data access nodes are set; at the battalion level, aggregation and gating nodes are allocated; at the brigade level, a control node and an exit point to the main or backup channels are determined. This allows, even before configuring individual technologies, to distribute functions between network levels: local C2 exchange, data aggregation, routing between units, integration with external channels, and redundancy of critical functions. The criticality of this stage is that an error in determining the roles of nodes subsequently leads to inefficient routing, overloading of network reference points, and loss of controllability during degradation.

In step 4 – the company-level C2-minimum circuit is designed. At this stage, DMR technology is introduced, which is used as the basic and most stable channel for voice command communication and transmission of short critical messages. For the company level, channel resources, frequency plan, backup frequencies, operating modes, and the order of transition between these modes are determined in accordance with communication management procedures. This step directly implements the network requirement for continuous management, even under deteriorating propagation conditions or under the influence of EW. If risks of unstable voice coverage are identified at the initial planning stage, this is recorded as a basis for further adjustment of node placement or introduction of relaying.

In step 5 – the company data layer is designed, within which SDR-MANET is introduced as a self-organised multi-hop network. At this stage, the logic of building routes between nodes, the permissible depth of multi-hop connections, the procedure for self-recovery of routes after the loss of individual nodes, and the rules for servicing situational awareness, telemetry, and other service packages are determined. Using SDR-MANET allows meeting the requirements for topology flexibility, distributed control, and adaptability to changes in the tactical situation. The criticality of this step is that it is here that the network's ability to support local data exchange in the event of losses, manoeuvres, and destruction of individual communication sections is formed.

Step 6 – the battalion gateway node is selected, which acts as a point of traffic aggregation and inter-level exchange management. At this stage, one or two reference nodes are determined, for which the position, coverage area, security, power supply, antenna deployment, and redundancy are assessed. This is where the network transitions from local company segments to an integrated battalion structure. The gateway node concentrates the functions of traffic aggregation, message prioritisation, route management, switching between available channels, and preparing data for transmission to a higher level. This is one of the most critical stages of the algorithm, since an incorrectly selected gateway can become a point of overload or the only vulnerability of the entire network.

In step 7 – relay planning and filling of areas of insufficient coverage are carried out. If the previous stages have established the presence of radio shadows, interruption of connectivity between companies, instability of access to the battalion gateway, or insufficient depth of coverage, additional relay nodes are introduced. These can be stationary mast solutions, mobile platforms, or UAV repeaters, depending on the terrain conditions and available resources. In this step, the algorithm directly responds to the network requirement to ensure connectivity and survivability in difficult terrain or with partial loss of infrastructure. If connectivity remains insufficient after the introduction of relaying, this stage is the primary point of correction before re-checking the KPI.

In step 8 – QoS and service degradation modes are configured. This is the stage at which the algorithm establishes a correspondence between traffic types and network functional priorities. The highest priority is given to the C2-minimum: command voice, commands, coordinates, and other critical management messages. The second level of priority is given to situational awareness and telemetry data. Streaming services, additional information exchanges or volumetric data are of lower priority and can be limited, compressed or completely disconnected in the event of a shortage of radio resources or during EW. It is at this step that the mechanism of controlled network degradation is formed, thanks to which the controllability of the unit is maintained even under deteriorating operating conditions.

In step 9 – the satellite channel is integrated into the "battalion-brigade" loop. Here, the satellite segment is not considered as a permanently guaranteed resource, but as a managed backbone or backup channel with predefined usage rules. At this stage, the conditions under which the satellite link is used as the main one for inter-level exchange are established, as well as scenarios for transition to autonomous battalion-level operation in the event of its loss, jamming, or cyber impact. Therefore, this step directly implements the requirement for the network to provide redundancy for inter-level exchange and ensure operability even in the absence of an external backbone channel.

Step 10 – IS setup. At this stage, encryption mechanisms, key material management, delimitation of exchange domains, as well as procedures for rapid resetting of keys and critical settings in the event of a threat of equipment capture are implemented for all involved technological segments. For cryptographic protection, the algorithm uses AES and other provided protection means compatible with the network configuration. Measures to counter radio interception, technical analysis of emissions and compromise of network parameters are separately determined. This means that IS requirements are not considered as an additional component, but are included in the network setup algorithm itself as its mandatory phase.

Step 11 is a network check using KPIs. The availability of C2-minimum, latency and stability of critical message transmission, data throughput, self-healing speed after loss of nodes or channels, as well as the network behaviour under the influence of EW are assessed. Verification at this stage completes the full design cycle and puts the

algorithm into decision-making mode. If the KPIs are met, the network deployment plan is approved as meeting the functional requirements. If the KPIs are not met, the algorithm proceeds to the adjustment of the network parameters, returning first to steps 6-10, i.e., reviewing the gateway configuration, relaying, QoS policies, degradation modes, satellite channel reservation, and protection parameters. This cycle is repeated until an acceptable level of network stability, QoS, and manageability is achieved.

The presented algorithm for phased design, configuration, and verification of the TCL network in EW conditions provides a structured approach to creating and optimising tactical networks. Its main advantage is the integration of many technologies into a single hybrid architecture that includes DMR, SDR-MANET, and satellite channels, which allows not only to ensure communication stability in conditions of high interference and dynamic topology, but also to quickly adapt the network to changes in combat conditions. This algorithm significantly improves network planning and deployment, as it is focused on real-world operating conditions. In particular, it allows clearly defining priorities for each network layer and technology, ensuring optimal resource allocation and minimising the likelihood of failures or degradation in critical situations. The algorithm also implements backup, degradation, and recovery mechanisms that allow the network to remain operational even in the event of loss of nodes or channels. In addition, it includes KPI verification stages that allow directly assessing the effectiveness and reliability of the network under combat and EW conditions, which is important for increasing the overall stability of the system. Thus, the algorithm not only structurally organises the process of network design and configuration, but also allows actively responding to changes in operating conditions, ensuring flexibility, stability, and communication security at all levels of command.

The correctness and efficiency of the proposed model largely depend on the algorithm for its design and configuration. Therefore, it is important to assess how the architectural principles embedded in the algorithm meet the requirements for the TCL network in EW conditions. Although it is not possible to make a direct comparison with other similar algorithms, it is possible to compare the architectural approaches and technologies used in the proposed model. This allows analysing how the choice of technologies, such as DMR, SDR-MANET and satellite channels, affects the stability, adaptability, and efficiency of the network in real conditions.

The results of the engineering analysis of the TCL network architecture showed that it is correctly described not through the "best channel", but through a matrix of services, roles of nodes and carriers and a formalised degradation sequence (ISR/video → COP/SA intensity reduction → "control only" with the dominance of the C2-minimum). This statement is consistent with D. Darsena & F. Verde (2022), who emphasised that the standardised Mission-Critical Push-To-Talk (MCPTT)/Mission-Critical Video (MCVideo)/MCData classes are designed under strict requirements for availability, reliability, latency, security and QoS, i.e., the "criticality" of services sets the priorities of the network resource. At the same time, the authors consider this hierarchy mainly in the context of the 4G/5G ecosystem and standardisation, while in the current study it is translated into operational degradation rules for a heterogeneous stack of communication carriers (DMR/MANET/SAT) and tied to the roles of TCL nodes (subscriber/gateway/aggregator/SAT gateway). S. Yuan *et al*. (2023) show that integrated satellite-ground networks are characterised by limitations in flexibility and adaptability and problems with efficient resource use, in connection with which the authors substantiated the need for SDN and intelligent control approaches. In the current study, these provisions are interpreted for the battalion-brigade level as an engineering requirement to treat SAT backhaul not as an unconditional support of the network, but as a managed resource with traffic prioritisation and degradation modes to the minimum profile ("C2/service data only") and with reservation/switching procedures, which is reflected in the service and carrier distribution matrix.

The results of the engineering analysis of the criteria for selecting the base data layer in the TCL network showed that the use of SDR-MANET at the battalion aggregator level and the inclusion of KPIs of recovery time after the loss of a node or link are methodologically justified, since in TCL the manageability is determined not by the peak speed, but by the network's ability to quickly restore connectivity and delivery of critical messages in conditions of dynamic topology and losses. These conclusions correlate with M. Baumgartner *et al*. (2024), who considered approaches to increasing the resilience of routing in MANETs and showed that the proposed improvements to routing protocols increase the network's resilience in conditions of dynamic topology, which is manifested in improving deliverability and latency indicators. The discrepancy lies in the level of detail: the authors worked at the level of specific protocols/mechanisms, while the current study forms an architectural policy and KPI framework, without fixing specific implementations of routing protocols. The proposed approach to service distribution and degradation policy in this study requires further experimental verification on specific MANET implementations regarding the reachability of the KPI of connectivity recovery time under typical COP/telemetry loads.

D. Falcão *et al*. (2021) substantiate the feasibility of disruption-tolerant networking (DTN) approaches for tactical messaging under conditions of discontinuous connectivity: DTN is considered as an evolution of ad hoc networks for environments with low node density and intermittent connections, where continuous end-to-end (end-to-end) connectivity is absent, and delivery is ensured by buffering and deferred forwarding. In the current study, these results are interpreted for degraded scenarios of the backbone transport (strategic backhaul) in the TCL as an engineering requirement to provide a separate "store and forward" degradation profile for critical messages, which is reflected

in the service and carrier distribution matrix. At the same time, despite the difference in scenarios (marine context in the authors vs. terrestrial TCL in this study), the basic principle is transferred: in the case of backhaul instability, the guaranteed delivery of management messages is ensured by the exchange mode (buffering/prioritisation/TTL), and not by the assumption of constant channel availability. J. Suomalainen *et al*. (2024) analysed the cybersecurity of autonomous rapidly deployable tactical networks and showed that orchestration and autonomous control (in particular, with the use of machine learning methods) simultaneously increase the complexity of the system and expand the threat landscape, as a result of which risk-based approaches, including threat analysis and prioritisation, are necessary for mission-critical applications. This conclusion correlates with the results of the current study that even in the minimum degradation mode, basic IS mechanisms must be maintained, the reduction of services should not be accompanied by the rejection of segmentation, access control and protection of control nodes/gateways and endpoints, which is reflected in the service and carrier distribution matrix. Therefore, IS is a component of system resilience and should be specified through the role of the node and the mode of operation, including degradation modes. Thus, the TCL communication network should be designed as a hybrid multilayer system with primary and backup communication media and managed degradation of services with a C2-minimum priority. Under any degradation profile, it is necessary to preserve the basic IS mechanisms (encryption, key management/zeroize, domain segmentation) and ensure architectural stability through channel diversification.

Conclusions

The paper analyses the model of the tactical command link communication network for the "company – battalion – brigade" loop. The model architecture has three levels: company, battalion and brigade, and includes access nodes, aggregation and gateway nodes, as well as integration and access nodes to main or backup channels. The model was considered under the conditions of unit mobility, limited infrastructure, EW, and possible losses of nodes and communication channels. The study analyses tactical communication technologies, determines the key characteristics for building TCL networks, justifies the distribution of services between network levels and the roles of nodes, taking into account TCL application scenarios. The feasibility of using DMR to ensure C2-minimum, SDR-MANET to build an adaptive data layer, and a satellite channel for inter-level main or backup exchange is shown. Based on real combat experience, the requirements for the TCL network were formulated: resistance to EW, survivability, adaptability, rapid recovery, support for priority services and IS.

The main result of the work was the development of an algorithm for planning the TCL network. It is a step-by-step procedure for deploying, configuring, testing and adjusting the network in changing operating conditions. The algorithm covers the collection of input data, determining performance criteria – coverage, connectivity, survivability and security, distributing node roles, configuring the C2-minimum and data layer, selecting gateway nodes and relay facilities, configuring QoS and redundancy, prioritising traffic and managed service degradation modes. The effectiveness is assessed through KPIs, which allows checking the stability and adaptability of the network in real combat conditions. The results of the study showed that the choice of technologies and architectural approaches, such as DMR, SDR-MANET and satellite channels, significantly improve the efficiency and stability of the TCL network. Ensuring manageability, stability, and high throughput even under EW conditions and channel degradation was one of the key aspects when building such a system. The proposed hybrid architecture allows the network to quickly adapt to changes in topology and conditions, which increases its reliability and security at all levels of command.

The limitation of the study is its theoretical and conceptual nature and the lack of full-scale experimental/field verification of the proposed solutions under real EW and mobility conditions. Future research should focus on developing and improving methods for protecting the TCL network from active interference and attacks. In addition, additional attention is required to study dynamic routing algorithms in conditions of limited resources and variable topology, in particular with the use of artificial intelligence and machine learning methods.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of Interest

None.

References

[1] Baumgartner, M., Papaj, J., Kurkina, N., Dobos, L., & Cizmar, A. (2024). Resilient enhancements of routing protocols in MANET. *Peer-to-Peer Networking and Applications*, 17, 3200-3221. doi: 10.1007/s12083-024-01746-3.

[2] Bojor, L., Petrache, T., & Cristescu, C. (2024). Emerging technologies in conflict: The impact of Starlink in the Russia-Ukraine war. *Land Forces Academy Review*, 29(2), 185-194. doi: 10.2478/raft-2024-0020.

[3] Chen, N., Song, Y., Cao, Y., Sun, Z., Zhao, B., Wang, M., He, D., & Peng, G. (2025). Network-layer perspectives on satellite-terrestrial integrated networks in 6G: A comprehensive review. *Engineering*, 54, 69-92. doi: 10.1016/j.eng.2025.05.012.

[4] Darsena, D., & Verde, F. (2022). Anti-jamming beam alignment in millimeter-wave MIMO systems. *arXiv*. doi: 10.48550/arXiv.2110.08134.

[5] European Telecommunications Standards Institute. (2016). *Electromagnetic compatibility and Radio spectrum Matters (ERM); Digital Mobile Radio (DMR) Systems; Part 2: DMR voice and generic services and facilities*. Retrieved from https://www.etsi.org/deliver/etsi_ts/102300_102399/10236102/02.03.01_60/ts_10236102v020301p.pdf.

[6] European Telecommunications Standards Institute. (2023). *Digital Mobile Radio (DMR) Systems; Part 1: DMR Air Interface (AI) protocol (ETSI TS 102 361-1 V2.6.1)*. Retrieved from https://www.dmrassociation.org/public-downloads/standards/ts_10236101v020601p.pdf.

[7] Falcão, D., Salles, R., & Maranhão, P. (2021). Performance evaluation of disruption tolerant networks on warships' tactical messages for secure transmissions. *Journal of Communications and Networks*, 23(6), 473-487. doi: 10.23919/JCN.2021.000043.

[8] Halwa, S., & Harriss, L. (2025). *Electromagnetic (electronic) warfare*. Retrieved from https://researchbriefings.files.parliament.uk/documents/POST-PN-0749/POST-PN-0749.pdf.

[9] Hrozdov, A.A., Zinchenko, I.A., Hromliuk, M.M., Bilyi, O.A., Ivchenko, M.M., & Tsymbal, I.V. (2024). Method for assessing the sustainability of a military communication system based on troops' combat capabilities. *Systems and Technologies of Communication, Informatization and Cybersecurity*, 5, 64-70. doi: 10.58254/viti.5.2024.05.64.

[10] Hui, K.-P., Phillips, D., Kekirigoda, A., Allwright, A., Zhang, J.A., Zhang, H., Le, A.T., & Jayawickrama, B.A. (2024). Unveiling MIMO potential: A prototype for enhanced tactical communications with interference suppression. In *Proceedings of the IEEE military communications conference* (pp. 1-6). Washington: IEEE. doi: 10.1109/MILCOM61039.2024.10773940.

[11] Hytera. (2018). *PD7i series*. Retrieved from https://www.hytera.us/wp-content/uploads/2023/01/PD7i-Series_20190524-Web.pdf.

[12] Kang, M., Park, S., & Lee, Y. (2024). A survey on satellite communication system security. *Sensors*, 24(9), article number 2897. doi: 10.3390/s24092897.

[13] Kantheti, V.S., Lin, C.-H., Lin, S.-C., & Chu, L.C. (2023). Anti-jamming resilient LEO satellite swarms. In *Proceedings of the military communications conference (MILCOM): Workshop on 5G military communications* (pp. 77-82). Boston: IEEE. doi: 10.1109/MILCOM58377.2023.10356296.

[14] Khomenko, P.V., Radzivilov, H.D., & Ilinov, M.D. (2025). Analysis of the functionality of MANET tactical radio systems. *Systems and Technologies of Communication, Informatization and Cybersecurity*, 7, 222-231. doi: 10.58254/viti.7.2025.20.222.

[15] Kim, J., Biswas, P.K., Bohacek, S., Mackey, S.J., Samoohi, S., & Patel, M.P. (2021). Advanced protocols for the mitigation of friendly jamming in mobile ad-hoc networks. *Journal of Network and Computer Applications*, 181, article number 103037. doi: 10.1016/j.jnca.2021.103037.

[16] L3Harris Technologies, Inc. (2024). *2023 annual report*. Retrieved from https://www.l3harris.com/sites/default/files/2024-02/L3Harris_2023-Annual-Report_web_.pdf.

[17] Lavrut, O., Davidenko, S., Opalynskyi, V., Boichuk, B., & Oliinyk, S. (2021). *Harris: Digital communication means of the tactical command and control of the Armed Forces of Ukraine: Study guide*. Lviv: National Army Academy named after Hetman Petro Sahaidachnyi.

[18] Lavrut, O.O., Lavrut, T.V., Klimovych, O.K., & Zdorenko, Y.M. (2019). New technologies and means of communication in the Armed Forces of Ukraine: The path of transformation and development prospects. *Science and Technology of the Air Force of Ukraine*, 34(1), 91-101. doi: 10.30748/nitps.2019.34.13.

[19] Lo, Y.W., Tsoi, M.H., Chow, C.-F., & Mung, S.W. (2024). An NB-IoT monitoring system for digital mobile radio with industrial IoT performance and reliability evaluation. *IEEE Sensors Journal*, 25(3), 5337-5348. doi: 10.1109/JSEN.2024.3512859.

[20] Mahmud, R., Toosi, A.N., Rodriguez, M.A., Madanapalli, S.C., Sivaraman, V., Sciacca, L., Sioutis, C., & Buyya, R. (2021). Software-defined multi-domain tactical networks: Foundations and future directions. In A. Mukherjee, D. De, S.K. Ghosh & R. Buyya (Eds.), *Mobile edge computing* (pp. 183-227). Cham: Springer. doi: 10.1007/978-3-030-69893-5_9.

[21] Masesov, M., Krotov, V., & Openko, P. (2021). Active queue management in tactical radio networks using fuzzy logic. *Modern Information Technologies in the Field of Security and Defense*, 40(1), 37-46. doi: 10.33099/2311-7249/2021-40-1-37-46.

[22] McCrory, D. (2023). *Electronic warfare in Ukraine: Preliminary lessons for NATO air power capability development*. Retrieved from https://www.japcc.org/articles/electronic-warfare-in-ukraine/.

[23] Motorola Solutions. (2026). *MOTOTRBO™ DM4000e series: Mobile two-way radios*. Retrieved from https://www.motorolasolutions.com/content/dam/msi/docs/EA_Collaterals/ENGLISH/MOTOTRBO/Mobiles/dm4000e_datasheet_eng.pdf.

[24] Mureșan, A., & Bechet, P. (2024). Waveform analysis in integrated tactical radio systems. *Land Forces Academy Review*, 29(4), 584-595. doi: 10.2478/raft-2024-0060.

[25] National Institute of Standards and Technology. (2001). *Advanced Encryption Standard (AES) (FIPS PUB 197)*. Retrieved from https://csrc.nist.gov/files/pubs/fips/197/final/docs/fips-197.pdf.

[26] National Institute of Standards and Technology. (2019). *Security requirements for cryptographic modules (FIPS PUB 140-3)*. Retrieved from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf.

[27] Patel, Z., Khanpara, P., Valiveti, S., & Raval, G. (2023). The evolution of ad hoc networks for tactical military communications: Trends, technologies, and case studies. In S. Shakya, V. Balas & W. Haoxiang (Eds.), *Proceedings of the 3rd international conference on sustainable expert systems* (pp. 331-346). Singapore: Springer. doi: 10.1007/978-981-19-7874-6_24.

[28] Salnyk, S.V., & Sydorkin, P.H. (2024). Analysis of the use of programmable radio communication means in mobile radio networks. *Systems of Arms and Military Equipment*, 77(1), 110-116. doi: 10.30748/soivt.2024.77.16.

[29] Sholudko, V.H., Yesaulov, M.Yu., Vakulenko, O.V., Hurskyi, T.H., & Fomin, M.M. (2023). *Organization of military communications: Study guide*. Kyiv: Skif Publishing House.

[30] Shtonda, R., Zinchenko, M., & Chayka, Y. (2023). Application of small-sized digital tropospheric communication stations during combat operations. *Modern Information Technologies in the Field of Security and Defense*, 47(2), 25-30. doi: 10.33099/2311-7249/2023-47-2-25-30.

[31] Silvus Technologies. (2025). *StreamCaster® 4400 Enhanced: SC4400E (4x4 MIMO radio)*. Retrieved from https://silvustechnologies.com/wp-content/uploads/2025/12/StreamCaster-4400-SC4400E-Enhanced-Datasheet.pdf.

[32] Starlink. (2026). *Starlink specifications*. Retrieved from https://starlink.com/legal/documents/DOC-1723-29826-76.

[33] Suess, J. (2022). *Jamming and cyber attacks: How space is being targeted in Ukraine*. Retrieved from https://www.rusi.org/explore-our-research/publications/commentary/jamming-and-cyber-attacks-how-space-being-targeted-ukraine.

[34] Suomalainen, J., Ahmad, I., Shajan, A., & Savunen, T. (2024). Cybersecurity for tactical 6G networks: Threats, architecture, and intelligence. *Future Generation Computer Systems*, 162, article number 107500. doi: 10.1016/j.future.2024.107500.

[35] Suomalainen, J., Julku, J., Heikkinen, A., Rantala, S.J., & Yastrebova, A. (2022). Security-driven prioritization for tactical mobile networks. *Journal of Information Security and Applications*, 67, article number 103198. doi: 10.1016/j.jisa.2022.103198.

[36] Thornton, C.E., Allen, E., Jones, E., Jakubisin, D., Templin, F., & Liu, L. (2023). On the role of 5G and beyond sidelink communication in multi-hop tactical networks. *arXiv*. doi: 10.48550/arXiv.2309.16628.

[37] Watling, J., & Reynolds, N. (2023). *Meatgrinder: Russian tactics in the second year of its invasion of Ukraine*. Retrieved from https://static.rusi.org/403-SR-Russian-Tactics-web-final.pdf.

[38] Yuan, S., Peng, M., Sun, Y., & Liu, X. (2023). Software defined intelligent satellite-terrestrial integrated networks: Insights and challenges. *Digital Communications and Networks*, 9(6), 1331-1339. doi: 10.1016/j.dcan.2022.06.009.