The American Journal of Engineering and Technology
ISSN 2689-0984 | Open Access

TYPE Original Research
PAGE NO. 99-106
DOI 10.37547/tajet/Volume07Issue10-13

Check for updates

Role Of a Unified IT Network as The Foundation for The Digital Transformation of Multi-Profile Facilities

Chata Marat Muratuly
New York, USA

OPEN ACCESS

SUBMITED 28 August 2025
ACCEPTED 26 September 2025
PUBLISHED 25 October 2025
VOLUME Vol.07 Issue 10 2025

CITATION

Chata Marat Muratuly. (2025). Role Of a Unified IT Network as The Foundation for The Digital Transformation of Multi-Profile Facilities. The American Journal of Engineering and Technology, 7(10), 99–106. https://doi.org/10.37547/tajet/Volume07Issue10-13

Abstract: At present, digital transformation acts as a determining element in maintaining competitiveness and increasing the operational efficiency of facilities of various purposes—from production complexes to socio-administrative structures. The study is aimed at a comprehensive examination of the role of a unified IT network as a basic systemic framework that ensures the implementation of this transformation. The purpose of the work is to identify the fundamental design principles and to demonstrate the strategic significance of a convergent network infrastructure for the coherent integration of heterogeneous engineering, operational, and business systems. The methodological basis of the research relies on a systems analysis of contemporary scientific literature over the period, the examination of relevant regulatory and standard requirements, and the practical deconstruction of a case involving the deployment of a comprehensive IT infrastructure at a strategically important facility—the National Company Kazakhstan Garysh Sapary. As a result of the analysis, a conceptual model of a unified network has been formed, as well as a rationale for its key advantages, including the improvement of operational efficiency, the rationalization of resource use, and the strengthening of cybersecurity levels. The scientific novelty consists in interpreting the unified IT network not only as a technical element but as a strategic asset that creates synergistic effects when digital technologies are introduced. The obtained conclusions and formulated practical recommendations are of value to organization leaders, IT directors, system architects, and engineering specialists who design and modernize the

infrastructures of multi-profile facilities within the context of the developing digital economy.

Keywords: Digital transformation, unified IT network, multi-profile facilities, systems integration, Internet of Things (IoT), building automation, IT/OT convergence, cybersecurity, smart building, Kazakhstan.

Introduction

The current stage of global economic evolution is marked by the all-encompassing introduction of digital technologies into every sphere of operation of systems and institutions. In this context, digital transformation is understood not as the mere adoption of IT tools or the automation of individual operations, but as the systemic re-thinking and re-engineering of business models, technological processes, and managerial practices based on data analytics and digital interactions. For complex multi-profile entities—such as airports, industrial clusters, medical institutions, and administrative centers—this transformation is of critical importance, as their resilience and efficiency depend on the integrated functioning of heterogeneous subsystems: from engineering networks and energy management to access control and industrial automation. The relevance of this study is determined by the fact that the historically formed, fragmented IT infrastructure constitutes a systemic barrier to implementing a holistic digital strategy. According to analytical data, more than half of digital transformation initiatives fail to achieve the expected results precisely because of the mismatch and fragmentation of the underlying infrastructure [1]. In the context of Kazakhstan, where the state program Digital Kazakhstan is being implemented, the volume of the Kazakhstani media market reached a historical maximum of 135 billion tenge in 2024 [2], and the formation of a modern, coherent IT foundation for key economic assets acquires not only economic but also strategic significance. The forecast growth of the internet advertising market volume by 29 % year-on-year by 2025 further reflects the high level of digital activity and the increasing dependence on resilient digital platforms in the national economy [2]. At the same time, despite a significant body of research focused on specific technological dimensions of digitalization—such as cloud architectures, artificial intelligence, or the Internet of Things—there remains an insufficient theoretical and empirical understanding of a unified network infrastructure as a fundamental, preliminary factor and mandatory condition for successful transformation.

The aim of this work is to identify the fundamental design principles and to demonstrate the strategic significance of a convergent network infrastructure for the coherent integration of heterogeneous engineering, operational, and business systems.

The scientific novelty lies in interpreting such a network as a strategic asset capable of creating synergistic effects and forming platform conditions for the deployment and scaling of next-generation technologies.

The author's hypothesis is formulated as follows: the transition from a heterogeneous, fragmented network architecture to a single, homogeneous infrastructure not only reduces operating costs but also significantly increases the adaptability, level of protection, and controllability of the asset, which together constitute the essential content of digital transformation.

Methods

In the contemporary literature on the digital transformation of multiprofile facilities several thematic blocks can be distinguished, each contributing to the understanding of the role of a unified IT network.

1. Theoretical and strategic foundations of digital transformation. In the work by Reier Forradellas R. F., Garay Gallastegui L. M. [3] digital transformation and artificial intelligence are considered through the prism of their comprehensive impact on business, including legal, economic and prospective aspects, which lays the theoretical foundation for understanding the required infrastructure and the role of unified IT networks as a platform for service integration and decision making in multiprofile facilities. Williams L. D. [7] develops the conceptual frameworks of the digital economy and Industry 4.0, emphasising that intelligent and information systems form an ecosystem in which technical platforms (including networks) become not merely data carriers but active participants in the value stream — that is, an infrastructure through which competitive advantage and enterprise flexibility are realised under conditions of digital transformation. It is also worth mentioning the analytical practice of strategic orientation toward technological trends presented in the Gartner report, which functionally links the choice and development of IT architectures (including unified networks) with the determination of priority areas of digital investment and the transformational roadmaps of organisations, setting

external benchmarks and instrumental categories for architectural decision making [1].

2. Architectures and technological mechanisms of smart and sustainable systems. Studies devoted to the implementation of IoT and related devices in the context of smart buildings and sustainable development emphasise that the digital transformation of multiprofile facilities requires an inseparable combination of network infrastructure and application systems. Poyyamozhi M. et al. [12] , in a systematic review of the potential of IoT for energy management in smart buildings, identify key applications, barriers and prospects, where the network serves as a critical layer for the collection, transmission and pre-processing of data needed for adaptive resource management; at the same time the authors note the necessity of coherent architectural integration and interface standardisation to ensure scalability and interoperability. Găitan V. G., Zagan I. [4] demonstrate a practical implementation of an extended Modbus server for BIoT-enabled smart switch devices, illustrating how network and application protocols can be adapted within embedded systems to ensure manageability and connectivity in biosensor and intelligent devices — the focus is on extending traditional communication stacks in view of the requirements of modern distributed devices. Büyüközkan G., Uztürk D. [5] propose an integrated design framework for smart agriculture that links digitalisation with sustainability, which in fact requires a unified, flexible and semantically meaningful network platform capable of aggregating diverse sensor, analytic and operational layers into a single decision-making system. All these works share the understanding that smart applications do not exist in a vacuum: they rely on a convergent, managed network with the capability to service heterogeneous devices, quality of service and semantic compatibility.

3. IT/OT convergence and ensuring resilience and security. The problem of merging traditional operational technologies (OT) with information technologies (IT) is regarded as a key challenge and at the same time as a source of synergy for multiprofile facilities. Foschini L. et al. [11] propose an architecture based on software-defined networking (SDN) for converged IT/OT networks and conduct a qualitative analysis of resilience to DDoS attacks, emphasising that centralised flow control within SDN provides mechanisms for flexible segmentation, anomaly detection and adaptive response, while simultaneously requiring new approaches to reconciling security policies between horizontal and vertical management levels. Nankya M., Chataut R., Akl R. [6] investigate in detail the components of industrial control systems (ICS), the corresponding cyber-threats and machine-learning-based protection, which complements the previous block — here security is not superficial but embedded in converged networks, where traffic analytics and behavioural data processing become part of the overall network platform for early incident detection and autonomous defensive reactions. Together these sources offer two complementary approaches: an architectural one (through SDN and segmentation) and an intelligent one (through ML-based detection), while raising the question of the necessary alignment of these levels within a single unified network so as not to generate fragmentation of control and policies.

4. Institutional, regional and market contexts of digital transformations (with an emphasis on Kazakhstan). Issues of implementing digital initiatives in specific regional and corporate contexts are raised in sources related to Kazakhstan. The publication on the Digital Kazakhstan programme on Tadviser presents an overview of the national digitalisation strategy, including infrastructure initiatives, objectives for service integration and the creation of a digital platform for public and commercial actors, which forms the institutional background within which the unified IT network becomes the basic infrastructure for cross-sectoral interaction and service coordination [10]. Sources describing the corporate history and portfolio of actors such as Kulager Construction Corporation LLP and the SBIC-KA project (via the Gharysh website) provide empirical reference points for understanding the implementation of multiprofile facilities in the local context, where existing project management and technology adoption practices are combined with requirements for connectivity and coordination among various professional domains [8, 9]. The article on investments in the Kazakh digital media market in 2025 reveals the economic context of the growth of digital platforms and demand for convergent information channels, indirectly signalling an increased load on network infrastructures and the need for unified approaches to ensuring bandwidth, quality and data manageability at scales that go beyond single niche applications [2]. Taken together, these sources illustrate how strategic state directives, corporate implementations and market pressures form a

multilayered ecosystem in which the unity of the network foundation is a necessary condition for the coherence, scalability and resilience of digital transformations.

On the one hand theoretical sources underscore the need for architectural flexibility and constant monitoring of trends, whereas applied implementations [4, 11] often focus on specific technical patterns without an explicit mechanism for evolution in response to strategic shifts. This creates tension between a stable, manageable network platform and the need for adaptability to new digital requirements. In addition, approaches to security in converged networks demonstrate different understandings of the levels of embedment: some rely on architectural segmentation through SDN, others on intelligent detection mechanisms, yet the synergy of these models and their coordination within a single unified network are poorly developed, which can lead to gaps in response and responsibilities.

The existing literature covers a wide range of topics — from strategic orientation of digital transformation and economic models to specific technical implementations in IoT/BIoT, converged networks and security, as well as regional institutional contexts. However, between strategic ideals and engineering solutions there is a deficit of mechanisms for coordinated evolution. The contradictory emphases on architectural segmentation and intelligent protection require a unifying concept of security management within a single network. The key gaps lie in the area of multidomain network management, adaptive alignment of strategy and tactics, the human factor of implementation and operational interoperability, especially in transformational environments such as Kazakhstan, where the combination of government regulation, corporate practices and market changes imposes unique requirements on the unified IT network as the basis for the digital transformation of multiprofile facilities.

Results And Discussion

The results of the conducted research and the accumulated practical experience make it possible to develop a substantiated concept of a unified IT infrastructure and to emphasize its strategic importance within the framework of digital transformation. The traditional model for building network infrastructure at a multifunctional facility is based on segmentation by application subsystems: separate physical or logical networks are allocated for security-and-fire alarm systems (ОПС), access control and management systems (СКУД), video surveillance, automation of engineering systems (BMS/BAS), and corporate user information exchange [3, 4]. As illustrated in Table 1, such a fragmented approach leads to a number of systemic shortcomings: redundant duplication of cable pathways, increased complexity of operational support, protocol interoperability issues, and, critically, it eliminates the possibility of performing coordinated data analysis and implementing end-to-end management.

Table 1. Comparative characteristics of the traditional and unified approaches to an object's IT infrastructure (compiled by the author based on [3, 4, 7, 12]).

Parameter	Traditional (heterogeneous) approach	Unified (convergent) approach
Physical environment	A multitude of parallel cabling networks (copper, fiber) for each system.	A single Structured Cabling System (SCS) based on high-speed standards (e.g. Cat.6A/7, fiber optic).
Active equipment	A disparate fleet of switches and routers from different manufacturers, often incompatible.	A centralized cluster of switching equipment with a unified management and monitoring system.
Logical structure	Physically and logically isolated networks. Data exchange is difficult or impossible.	A single IP network, logically segmented using Virtual Local Area Network (VLAN) technology to separate traffic and ensure security.
Management	Decentralized, requiring specialists for each individual system.	Centralized management and monitoring of the entire network infrastructure from a single center.
Scalability	Low. Adding a new system	High. New systems and devices are

	requires laying a new network.	easily integrated into the existing IP network.
Data	Data are locked in the silos of their respective systems. Comprehensive analysis is impossible.	Data from all subsystems can be collected on a single platform (BIoT, SCADA, digital twin) for analysis and decision-making.
Security	Vulnerabilities in one system may go unnoticed. Difficulty in implementing a unified security policy.	A unified security policy, centralized access control, and anomaly monitoring across the entire network (IT and OT).

In contrast to the fragmented model, the unified network is built on the principles of convergence. The foundation of such an architecture is a single physical subsystem — a structured cabling system (SCS) that covers all functional zones of the facility and is designed with substantial bandwidth redundancy for data transmission. Upon this physical base, a single IP infrastructure is formed by means of modern active network equipment (switches, routers). The segregation and security of data flows of various subsystems (for example, separating the video stream from the building management system data) is implemented not through physical segmentation but logically, using Virtual Local Area Network (VLAN) mechanisms. This architecture is schematically illustrated in Figure 1.

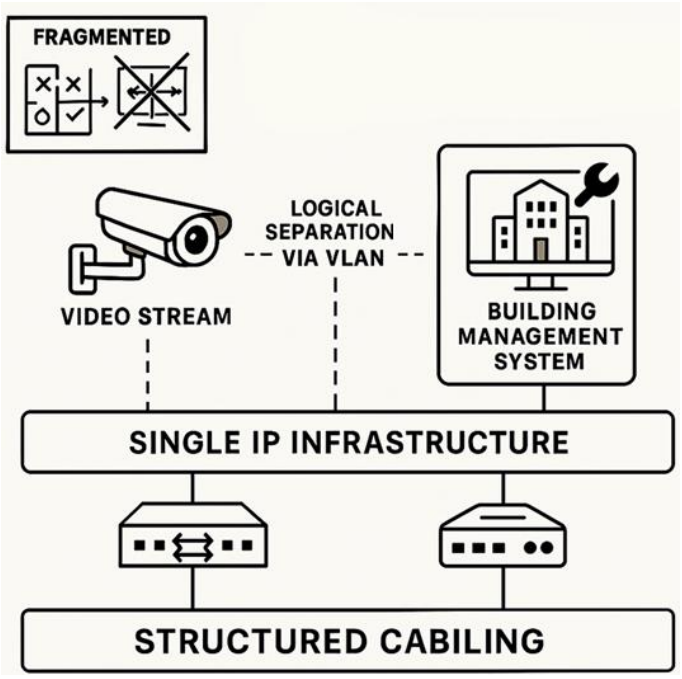

Fig. 1. Conceptual model of a unified IT network of a multi-profile facility (compiled by the author based on [4, 5, 7]).

Practical evidence of the effectiveness of the approach described was provided by the experience accumulated in the creation of a comprehensive engineering and IT infrastructure for a number of multipurpose facilities in Kazakhstan by the Construction Corporation Kulager. Within these projects—including airports, medical institutions and production sites—the integration of fire-safety subsystems, information-communication networks and engineering automation was not merely desirable but constituted a fundamental requirement for the architecture and operation of the facilities.

Particular significance in this context is attached to the implementation at the facility of the National Company Kazakhstan Garysh Sapary. The complex belongs to strategic-level facilities and imposes exceptionally high requirements for functional sustainability, fault tolerance and information security. To meet these requirements, a deeply integrated system was built using equipment from leading international manufacturers: Bosch for security and public-address systems, Siemens for automation of engineering processes and Cisco as the basis of the network

infrastructure [6, 7].

On the basis of Cisco technologies, a unified information and network framework was created that serves as a single communication space linking all key subsystems of the complex. Within this environment Bosch security solutions—video surveillance, fire detectors and access-control systems—transmit events and data over the common IP infrastructure. This makes it possible, in the event of fire detection, to automatically initiate multichannel response scenarios: display the image from the nearest camera on security service workstations, unlock evacuation exits and activate smoke-extraction mechanisms. In parallel, Siemens controllers for engineering systems responsible for climate control, lighting and energy resources are likewise integrated into the same network, which allows centralized management of consumption on the basis of synthesized data on staff presence (via ACS), temporal parameters and external meteorological conditions. At the same time, corporate IT resources—workstations, servers and data-storage systems—are located in the same physical infrastructure but are logically segmented by VLANs, which simultaneously ensures the availability of shared services and compliance with strict cybersecurity requirements.

Such end-to-end consolidation of functional domains generates a synergistic effect unattainable under the traditional separate construction of subsystems. In particular, the coordinated operation of components not only increases operational and functional reliability but also optimizes the use of resources, minimising redundant expenditures [8, 9].

The unified network becomes a key foundation for subsequent stages of digital transformation, primarily for the formation of a digital twin of the facility. A digital twin is a dynamic virtual replica of a real object that in real time accumulates and synthesises data from all sensors and control systems. This integration makes it possible not only to monitor current operational parameters but also to carry out analytical modelling of alternative what-if scenarios, increase process efficiency through optimisation and implement predictive maintenance of equipment on the basis of degradation forecasts. Without a single convergent network that provides collection, transport and harmonisation of data streams from heterogeneous sources, the full capabilities of a digital twin are fundamentally unattainable. Figure 2 presents the sequential stages of digital transformation that become feasible owing to the presence of a unified network infrastructure.

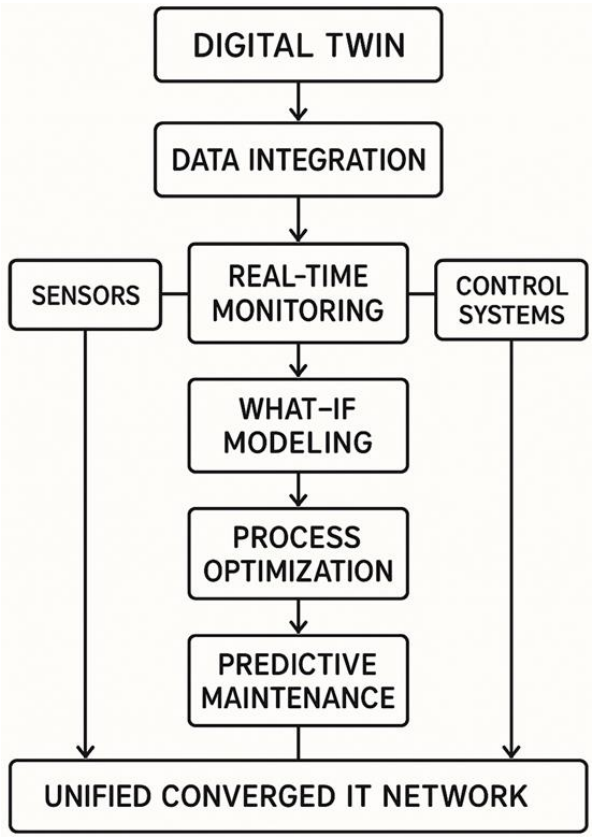

Fig. 2. Stages of digital transformation of a multi-profile facility based on a unified IT network (compiled by the

author based on [3, 5, 7]).

Implementation of the described architecture in Kazakhstan is in close correlation with both global and national strategic development trends. The Digital Kazakhstan initiative is oriented toward the large-scale digitalisation of critically important economic sectors, including the industrial complex and infrastructure systems [10], which creates an institutional demand for integrated and intelligent network solutions. Simultaneously, the ongoing expansion of cloud services and the growing interest in open-source-based solutions generate a demand for adaptive, easily scalable local networks capable of seamless interaction with external platforms and services [11].

The analysis conducted makes it evident that a unified IT network goes beyond a traditional engineering solution and acquires the status of a strategic asset forming the foundation for deep and systemic digital transformation. Such a network provides the basis for the transition from fragmented, reactive management of individual subsystems to a holistic, anticipatory and coordinated model of operating an asset perceived as a single dynamic system. Practical experience accumulated during the implementation of similar integration solutions at advanced facilities in Kazakhstan demonstrates that it is precisely this systemic, proactive architecture that yields the greatest efficiency of investments in digital technologies, ensuring synergistic returns and the resilience of the complex as a whole.

Conclusion

The conducted study confirms the proposed hypothesis: a unified IT infrastructure constitutes a key and irreplaceable framework for digital transformation at multidisciplinary facilities. A review of academic works showed that, despite the intensive study of individual digital technologies, the strategic significance of the basic network platform is often underestimated or examined fragmentarily. The consolidation of security systems, automation, and corporate IT services on the basis of a single, logically segmented IP network ensured the achievement of synergistic effects: operational efficiency increased, resource consumption was optimized, and the mechanisms for protecting the facility as a whole were strengthened.

The aim of the study has been achieved: the basic principles for building a unified network (including a single structured cabling system, logical segmentation, and centralized management) have been formulated and substantiated, and its strategic role has been confirmed. The proposed conceptual models, together with visual materials covering a comparative assessment of approaches and key stages of transformation, contribute to an orderly and in-depth understanding of the subject area. The conclusions obtained possess both theoretical and applied value: they complement the scientific conceptualization of the infrastructural foundations of the digital economy and may be in demand by managers and technical specialists when planning and implementing modernization programs and constructing complex facilities aimed at the sustainable attainment of the goals of digital transformation.

References

1. CIO's Guide to Using the Gartner Top 10 Strategic Technology Trends Report. [Electronic resource]. - Access mode: https://www.gartner.com/en/information-technology/insights/top-technology-trends (date accessed: 19.06.2025).
2. 69.5 billion tenge in digital: what is happening with the media market of Kazakhstan in 2025. [Electronic resource]. - Access mode: https://profit.kz/articles/14959/69-5-mlrd-tenge-v-digital-chto-proishodit-s-mediarinkom-Kazahstana-v-2025-godu/ (date accessed: 25.07.2025).
3. Reier Forradellas R. F., Garay Gallastegui L. M. Digital transformation and artificial intelligence applied to business: Legal regulations, economic impact and perspective //Laws. – 2021. – Vol. 10 (3). – pp. 1-22. https://doi.org/10.3390/laws10030070.
4. Găitan V. G., Zagan I. Modbus extension server implementation for BIoT-enabled smart switch embedded system device //Sensors. – 2024. – Vol. 24 (2). – pp. 1-22. https://doi.org/10.3390/s24020475.
5. Büyüközkan G., Uztürk D. Integrated design framework for smart agriculture: Bridging the gap between digitalization and sustainability //Journal of Cleaner Production. – 2024. – Vol. 449. https://doi.org/10.1016/j.jclepro.2024.141572.
6. Nankya M., Chataut R., Akl R. Securing industrial control systems: Components, cyber threats, and machine learning-driven defense strategies

//Sensors. – 2023. – Vol. 23 (21). – pp. 1-41. https://doi.org/10.3390/s23218840.

7. Williams L. D. Concepts of Digital Economy and Industry 4.0 in Intelligent and information systems //International Journal of Intelligent Networks. – 2021. – Vol. 2. – pp. 122-129.
8. Portfolio - TOO "Construction Corporation "Kulager". [Electronic resource]. - Access mode: https://www.fgwilson.kz/gallery/view/too-stroitelynaya-korporaciya-kulager (date accessed: 17.06.2025).
9. Kompaniya kuru tarihi. [Electronic resource]. - Access mode:https://www.gharysh.kz/ru/about/project/sbik-ka/ (date accessed: 20.06.2025).
10. Digital Kazakhstan. [Electronic resource]. - Access mode:https://www.tadviser.ru/index.php/Статья:Цифровой_Казахстан (date accessed: 27.06.2025).
11. Foschini L. et al. An SDN-enabled architecture for IT/OT converged networks: A proposal and qualitative analysis under DDoS attacks //Future Internet. – 2021. – Vol. 13 (10). – pp. 1-19. https://doi.org/10.3390/fi13100258.
12. Poyyamozhi M. et al. IoT—A promising solution to energy management in smart buildings: A systematic review, applications, barriers, and future scope //Buildings. – 2024. – Vol. 14 (11). – pp. 1-31. https://doi.org/10.3390/buildings14113446.