Universal Library of Business and Economics **Methodological Guide**

ISSN: 3064-9951 | Volume 3, Issue 1

Open Access | PP: 75-89

DOI: https://doi.org/10.70315/uloap.ulbec.2026.0301010

Innovative Management Model for Multifunctional Infrastructure Hubs (MIH) Under Conditions of High Uncertainty

Tatevosyan A. V.

Director of Private Enterprise Tatevosyan, LLC "Tyres of the World", Zaporizhzhia, Ukraine.

Abstract

This methodological guide is focused on the design and theoretical verification of an innovative management model for Multifunctional Infrastructure Hubs (MIH) in a context of accelerating global turbulence and heightened uncertainty. The text provides an expanded analysis of the key challenges of recent years, including energy-related threats, disruptions to supply chain resilience, and constraints in human resources capacity. Taken together, these factors create an objective demand for transforming traditional operational approaches into adaptive "end-to-end service" ecosystems capable of maintaining process alignment and rapidly reconfiguring functions.

A central emphasis is placed on integrating the high-technology electric transport contour (EV infrastructure) with a digital architecture built on CRM platforms, where requirements for strict data discipline are established and conditions for predictive management are created. The research logic is structured around the toolkit of systems analysis, scenario planning, and risk management, which made it possible to develop the author's standards for comprehensive safety and incident management. The results obtained show that a modular architecture combined with digital standards increases facility resilience and economic performance amid sharp fluctuations in the external environment. The formulated provisions confirm the applicability of the proposed model for sustaining the continuity of critically significant services and for improving the effectiveness of regional security mechanisms. The material has practical value for managers in the development sector, the professional community of urban planning, and investors focused on contemporary technological assets.

Keywords: *Multifunctional Hubs, Innovative Management, Uncertainty, EV Infrastructure, Digital Data Discipline, CRM Systems, Regional Security, Service Resilience, Incident Management, Adaptive Planning.*

CONTENT

Citation: Tatevosyan A. V., "Innovative Management Model for Multifunctional Infrastructure Hubs (MIH) Under Conditions of High Uncertainty", Universal Library of Business and Economics, 2026; 3(1): 75-89. DOI: https://doi.org/10.70315/uloap.ulbec.2026.0301010.

INTRODUCTION

The relevance of this study is determined by the rapid restructuring of the global economic landscape in 2024–2025. According to major analytical organizations, more than 76% of European shippers recorded significant disruptions in supply chain stability throughout 2024, while inflationary dynamics and geopolitical instability continue to retain the status of key risk sources for 2025 [1]. Within this configuration, traditional infrastructure facilities (fuel stations, shopping centers, parking complexes) are losing alignment with new requirements and are subject to functional evolution toward the format of Multifunctional Infrastructure Hubs (MIH). The problem field of the study is linked to the need to construct management mechanisms that ensure resilience, reproducibility of service quality, and the economic viability of facilities amid resource scarcity, workforce constraints, and energy risks.

The scientific complexity of contemporary work manifests in the lack of an integrated model capable of linking physical infrastructure, the electric transport contour, and digital data discipline into a single management framework that remains effective under conditions of high uncertainty.

The objective is to develop and theoretically substantiate an innovative MIH management model based on the principles of adaptability, modular organization, and digital transparency.

The scientific novelty lies in substantiating the synergistic effect between the development of EV infrastructure as an "anchor" traffic generator and the introduction of authorial regional safety standards, which shifts the hub from the category of passive assets to the status of an active element of regional resilience.

The author's hypothesis is that achieving operational effectiveness and the required level of MIH safety under instability is possible only through the introduction of strict norms of digital data discipline and the use of real-time scenario modeling of operational regimes. As a result, embedding MIH into the foundation of the modern city acquires the character of a necessary condition for overcoming current macroeconomic constraints and for building long-term resilience.

CHAPTER 1. THE MIH CONCEPT AND AN INNOVATIVE MANAGEMENT MODEL UNDER HIGH UNCERTAINTY

In the chapter, the concept of Multifunctional Infrastructure Hubs (MIH) is elaborated: the definition and typology, delimitation of scope (including the "zone of influence" of resource flows), the core stakeholder map, and the legal/contractual framework for implementation, with emphasis on the digital layer and on requirements for data governance and cyber resilience. The chapter then considers an innovative MIH governance model under high uncertainty, built on principles of modularity, adaptivity, redundancy, and rapid process reconfiguration, including legally material issues of module status, allocation of responsibility, and the formalization of replacement/testing procedures. A separate section is devoted to end-to-end service architecture: seamless user, resource, and operational flows; the role of the digital twin and 5G slicing in guaranteeing QoS; and the establishment of unified accountability and provability of actions in remote service delivery and payment scenarios. The chapter concludes with scenario-based operationalization of operating modes (normal / peaks / resource deficit / incident) and the design of a KPI/SLA system covering quality, resilience, safety, economics, and social impact, where metrics function simultaneously as a management instrument and as a legal criterion of proper performance.

Definition and Typology of Multifunctional Infrastructure Hubs: Functions, Boundaries, Stakeholders

Multifunctional infrastructure hubs (MIH) represent a complex integration of physical assets and digital services designed to meet a broad range of needs of contemporary urban and regional communities. Unlike narrowly specialized facilities, MIH implements the concept of environmentally oriented and socially responsive infrastructure in which transport functions are connected with residential use,

recreational spaces, and water resource management [2]. By 2025, research and project practice have shaped a typology of such facilities that includes urban micro-hubs, regional logistics hubs, and hybrid service spaces that simultaneously support the movement of people and goods, the delivery of everyday and public services, and the operation of urban engineering systems.

The boundaries of MIH are defined not only by a physical perimeter, but also by their zone of influence on territorial resource flows, including transport, energy, and water-management contours. Key stakeholders include local government bodies, private operators, utility and resource-supplying organizations, and end users; each of these groups articulates its own requirements for reliability, resilience, and the quality of services provided [3]. Their interaction is reasonably structured around the principles of inclusive planning and multi-level governance, implying alignment of interests at the stages of design, construction, and subsequent operation.

The legal nature of MIH is shaped by the cross-sector character of regulated relations: urban planning, the construction and reconstruction of capital facilities, the organization of transport services, the use of water bodies, and the provision of utility and social services form a single bundle of public-law and private-law elements. In this connection, it becomes legally significant to align decisions on MIH siting and parameters with territorial planning and zoning documents, as well as with land plot regimes and restrictions on land use; inconsistency among these components leads to elevated risks of challenges to permitting procedures and subsequent property-related claims.

The contractual model for MIH implementation typically relies on a combination of investment obligations and service delivery regulations, which makes concession agreements and public–private partnership mechanisms particularly relevant, as well as mixed structures involving resource-supplying organizations. For such projects, the allocation of construction and operational risks, the establishment of service availability and quality indicators, the terms of technological connection to engineering networks, and the procedure for indexing payments are of fundamental importance, because these elements ensure a balance between public interests (continuity and safety of services) and private interests (predictability of returns and investment protection).

The digital contour of MIH forms a distinct block of legal requirements: processing information about movements and consumer behavior, user identification, and the integration of payment and dispatch solutions presuppose compliance with personal data regimes, information security requirements, and the operational resilience of information systems. Additionally, when intelligent systems for managing flows and engineering infrastructure are introduced, the legal regime of critical information resources and data access regulations becomes increasingly important, since violations in this area can transform from technical incidents into legally significant events affecting safety, operator liability, and user rights (see Table 1).

Table 1. Matrix of functions and stakeholder interests in MIH (compiled by the author based on [4]).

Stakeholder	Core functions in MIH	Key expectations (2025)
Municipalities	Regulation, safety	Reduced carbon footprint, accessibility
Investors / Developers	Financing, CAPEX	ROI, asset value growth (up to +8%)
Service operators	Operations, OPEX	Minimizing disruptions, customer retention
Residents / Customers	Service consumption	Speed, comfort, data security

The intermediate conclusion is that interpreting MIH as an ecosystem-based construct creates managerial prerequisites for aligning the interests of diverse stakeholders through the deployment of an integrated service offering, thereby forming a foundation for sustainable territorial development.

Principles of Innovative Management: Modularity, Adaptability, Redundancy, Rapid Reassembly of Processes

Innovative management of multifunctional infrastructure hubs under uncertainty is best captured through four core principles that ensure the controllability of a complex system under external volatility. Modularity means the ability to operate autonomously and replace individual components (in particular, charging infrastructure blocks or retail-and-service modules) without shutting down the facility as a whole [5]. Adaptability is achieved through the introduction of artificial intelligence algorithms applied to optimize operating modes at the level of a single hub and across a network; according to industry assessments, a meaningful share of organizations deploy such solutions precisely at the site level or within a network contour.

Redundancy, in its modern interpretation, covers not only duplication of equipment, but also the creation of spare throughput capacity across logistics, energy, and digital contours, including alternative supply routes, computing capacity, and communication channels. Rapid reconfiguration of processes implies the ability to quickly shift a hub from a predominantly commercial operating mode into a mode that prioritizes the provision of vital territorial needs (for example, during large-scale power outages). This, in turn, requires pre-approved action procedures, a clear distribution of authority, and the maintenance of constant operational readiness.

In legal terms, modularity is linked to the need for regulatory certainty regarding the status of replaceable elements—whether they are treated as part of a capital construction facility or as technological equipment placed and operated within a single property complex. Legally significant issues include compatibility and safety requirements for modules, the procedure for their acceptance and commissioning, as well as the formal delineation of responsibility between the asset owner, the operator, and contractor organizations performing maintenance. The absence of proper documentation of replacement and testing procedures increases the risk that operational decisions will be deemed non-compliant with mandatory requirements and, as a consequence, triggers tort and contractual liability in cases of harm.

Redundancy of logistics and digital capacity should be understood not as an optional managerial measure, but as an element of ensuring the reliability and safety of service provision, since failure in one segment can cause cascading disruptions in interconnected systems. From an enforcement perspective, this supports the inclusion—within operational regulations and contracts with counterparties—of continuity indicators, resilience requirements, switching procedures to backup schemes, as well as conditions for information interaction during incidents. Issues of data legal regime and access rights also gain additional weight: reserving computing resources and communication channels presupposes a pre-established procedure for exchanging information among participants, including when restrictive regimes and service priorities are introduced.

Rapid process reconfiguration—associated with transferring an asset into a mode of supporting vital functions—requires aligning management protocols with the current regimes for emergency prevention and response, as well as with requirements for protecting critical information systems, if the hub's digital contour controls transport, energy, or utility processes. In such a contour, the legal construct of facility resilience is expressed in the ability to preserve baseline functions amid partial disruption of external supply through modularity, backup schemes, and a pre-regulated transition to special operating modes, thereby forming an appropriate level of infrastructure "survivability" as a legally significant outcome of management.

"End-to-End Service" Architecture: The Logic of User/Resource/Operations Flows

An "end-to-end service" architecture implies the formation of a continuous user journey—from the moment a need arises to the completion of the operation and receipt of the result. In multifunctional infrastructure hubs, this is ensured through digital coordination that integrates cloud infrastructure management, edge computing, and physical operations into a single operational chain [7]. The logic of flows is built to reduce waiting time and eliminate errors caused by manual input and fragmented accounting procedures.

Resource flows (electricity, water, spare parts) in multifunctional infrastructure hubs are organized according to a "just-in-time" principle, which becomes critically important under supply chain disruptions: according to McKinsey's assessments, disruptions lasting one to two months recur on average every 3.7 years [21]. The use of a hub "digital twin" makes it possible to identify probable bottlenecks and shortages before they manifest in practice by modeling load scenarios, equipment condition, and the throughput of adjacent systems.

From a legal and managerial perspective, an end-to-end service requires establishing a single point of responsibility for the result when several suppliers and operators participate within one facility. Proper formalization of the distribution of duties between the owner of the property complex, the operator of the digital platform, and executors of individual works becomes essential, as does ensuring transparency of service terms and settlements. Where remote application and payment methods are used, legally significant questions include confirmation of intent, identification of participants, evidentiary validity of actions performed, and compliance with consumer protection and personal data requirements.

Within an infrastructure hub, the "just-in-time" principle is not merely a logistics technique, because it is directly connected with risks to the continuity of socially significant services. In contractual structures, this drives the need to stipulate reliability indicators and recovery timelines, interaction procedures under resource shortages, as well as special provisions on substitute supplies and service priorities under constraints. When circumstances are assessed as force majeure, the content of agreed regulations becomes decisive: the absence of pre-defined scenarios for switching to backup solutions can transform an external event into a managerial risk that entails liability for improper performance of obligations.

The use of a "digital twin" increases the significance of data as a management resource and a potentially evidentiary resource, since decisions on reallocating flows, restricting access, prioritizing service, and planning maintenance are made on the basis of digital models. In this context, the legal resilience of the model is ensured by established rules for data creation and storage, its integrity, the delineation of access rights, and the auditability of actions by authorized persons. Information security requirements add further burden: compromising the integrity of the digital model or substituting baseline parameters may cause not only economic losses, but also legally significant consequences relating to operational safety and operator liability.

The application of an "end-to-end" operational logic implemented via 5G slicing makes it possible to secure guaranteed quality-of-service (QoS) parameters for critical operations by isolating them from mass traffic, thereby increasing the predictability of key services [10, 27].

Scenario Operating Modes of MIH: "Normal" / "Peaks" / "Resource Deficit" / "Incident Mode"

Managing multifunctional infrastructure hubs requires a clear gradation of operating modes to ensure comparability of management decisions and predictability of system response to changes in load. The "normal" mode focuses on achieving planned efficiency indicators and stable compliance with service quality parameters. The "peak load" mode is activated when demand rises sharply (holiday periods, climate anomalies, mass events) and involves reallocating workforce capacity, reconfiguring service schedules, and increasing available power supply and the throughput of technological contours.

The "resource deficit" mode is characterized by constraints in external supplies and a transition to autonomous support scenarios, including the use of battery energy storage systems and backup supply schemes, while simultaneously introducing service priorities for socially significant consumers and emergency services. The "incident mode" is introduced when direct security threats arise—from fire to cyberattacks and violations of information system integrity. The average cost of a data breach in 2024 was estimated at USD 4.88 million, which objectively reinforces the priority of protecting the hub's information contour within this mode [1, 6, 9].

From a legal standpoint, formalizing these modes should rely on a linkage between the operator's internal regulations and the public-law requirements applicable to facilities involved in sustaining territorial essential services. Legal significance is attached to distinguishing the grounds for introducing modes, defining the scope of authority of officials, documenting management commands, and establishing criteria for returning to normal operation, since these elements enable an assessment of good faith and reasonableness in potential disputes involving harm, downtime, and improper performance.

Within the contractual contour, the mode-based model should be reflected in operating agreements, service levels, and technological regulations, including procedures for changing service priorities, permissible deviations from quality metrics, conditions for involving additional contractor forces, and the interaction order with resource-supplying organizations. Separate fixation is required for notification mechanisms and data exchange among participants, as well as the procedure for applying penalties and exemptions from liability in emergencies and other objective circumstances, given that the absence of pre-agreed scenarios substantially increases the risk that what is happening will be qualified as a management miscalculation rather than an external event.

In information security, the "incident" mode should be accompanied by predetermined procedures for localization, recovery, and investigation, including action logging, access segmentation, backup copying, and verification of the integrity of critical data. Additional importance attaches to compliance with personal data protection requirements and information system resilience, because compromising the integrity of the digital contour entails not only economic consequences, but also legally significant risks associated with operator liability, potential orders from supervisory authorities, and the evidentiary status of actions taken in a crisis situation [18, 20].

Thus, the scenario-based formalization of operating modes enables personnel and automated management systems to act according to pre-approved algorithms, reducing the probability of errors caused by the human factor and increasing the legal certainty of management decisions under crisis conditions.

KPI and SLA System: Quality, Resilience, Safety, Economics, Social Impact

The indicator system for multifunctional infrastructure hubs should reflect a balance of stakeholder interests and ensure comparability of management decisions at the stages of operation and facility development. A service level agreement (SLA) fixes the parameters of availability and quality of services, including maximum permissible waiting times for charging infrastructure use, requirements for the continuity of digital services, as well as response procedures for deviations and recovery timeframes. Service quality can be measured through a satisfaction index; at the same time, applied assessments suggest that implementing optimization models based on controlled EV charging and capacity aggregation using a "virtual power plant" model can increase the relevant index by 20.7% [8].

To ensure the manageability of MIH, the indicator system is typically formed across several interconnected contours: operational (throughput, service time, equipment availability factor), resource (specific losses, energy intensity of operations, water-use efficiency, share of resource reuse), financial and economic (total cost of ownership, revenue predictability, cost structure), and social and environmental (accessibility for people with limited mobility, safety, reduced emissions and noise). Such multi-contour design prevents the substitution of socially significant objectives with narrowly financial metrics and supports comparison of outcomes for both public and private partners.

The legal significance of indicators is explained by the fact that they serve as criteria of proper performance and grounds for liability measures, including payment recalculation, penalties, and compensation mechanisms. For this reason, indicators and calculation methods must be verifiable, unambiguous, and reproducible: data sources are fixed, rules for excluding anomalies are defined, downtime due to reasons beyond the operator's control is accounted for, and the procedure for changing target values is regulated. Proper methodological detail reduces the risk of disputed qualification of control results and prevents arbitrary interpretations of service quality.

The reliability of the indicator system is ensured through accounting and control arrangements that include event logging, metrologically correct measurements, independent data verification, and procedural audits. With a high share of digital processes, the linkage between operational metrics and information security requirements becomes especially important: data integrity, access-right segregation, and the ability to subsequently confirm facts are necessary not only for management analytics, but also as an evidentiary basis for incidents and claims work. As a result, MIH indicators perform a dual function—managerial and legal—forming a measurable standard of service quality and resilience.

Within Table 2, the key performance indicators (KPI) for MIH management are described.

Table 2. Key performance indicators (KPI) for MIH management (compiled by the author based on [9, 26]).

Category	KPI	Target value 2025
Resilience	Mean Time to Recovery after failure (MTTR)	< 15 minutes
Economics	Gross margin of operational services	35–45%
Safety	Lost Time Injury Frequency Rate (LTIFR)	0.0
Digital	CRM data accuracy	> 99%

A differentiated KPI system makes it possible not only to assess current effectiveness, but also to forecast social impact through the lens of the reliability and accessibility of the urban environment.

CHAPTER 2. MIH SERVICE ARCHITECTURE AND EV INFRASTRUCTURE AS A MANDATORY ELEMENT OF THE MODERN CITY

In the second chapter, the service architecture of MIH is presented as a modular platform in which the "core" (power supply and connectivity) is complemented by scalable blocks (coworking, data centers, and others) and partner offerings, while module-level flexible contracting increases controllability, reduces downtime, and makes quality/liability risks more transparent. The chapter further substantiates EV infrastructure as a mandatory element of the contemporary city: MIH operates as a "charging–parking–service" node and as a traffic anchor, increasing dwell time and generating a multiplicative effect for adjacent services, provided that rules for access, payment, and duty allocation are clearly defined among the site owner, the network operator, and the energy supplier. A dedicated block addresses EV module design (AC/DC, siting, navigation, accessibility, safety, operating regulations, and digital interoperability), including legally significant issues of grid connection, reliability categories, load dispatching, data protection, and evidentiary traceability of service events. The chapter concludes with the economics of the EV module and its integration into the MIH ecosystem: CAPEX/OPEX and tariffs, demand management and subsidies, monetization of dwell time via value-added services and "charging + service" bundles, and a KPI system (throughput, availability/quality, grid parameters, and conversion to adjacent services) linking charging-zone performance to overall MIH indicators.

MIH Function Portfolio: Core Services, Extended Modules, Partner-Based Offerings

The hub's functional content is built around modular scalability, which enables a phased expansion of capacity and services without revisiting the facility's baseline architecture. Among the first-priority services is the guaranteed provision of power supply and communication channels, which together form the technological "frame" for subsequent growth. Additional modules—including co-working areas and data centers—serve as instruments for revenue diversification and for reducing dependence on a single line of activity. The overall effect is that a flexible service structure allows the hub to quickly align its offering with local demand dynamics, lowering the risk of underutilized space and the losses associated with it [4].

From a legal standpoint, modularity increases the controllability of the asset by enabling differentiated regimes for using premises and engineering infrastructure. This makes it possible to conclude separate agreements for each functional block (lease, paid service provision, technological connection), set distinct quality and liability parameters, and implement phased commissioning while complying with urban planning requirements and technical regulation. Separating operational contours also simplifies oversight of the intended use of property and compliance with mandatory safety requirements, including fire safety and anti-terrorism protection.

For modules related to information processing, the legal regime of data and information security becomes especially significant. Operating data centers presupposes a documented allocation of roles and responsibilities among the infrastructure owner, the data processing operator, and telecommunications service providers, as well as the implementation of organizational and technical measures for protecting information. The contractual framework should define procedures for accessing server premises, maintaining access logs, regulating incidents and notifications, and establishing liability for breaches of confidentiality and service availability. This reduces the risk of disputes and simplifies evidentiary confirmation of proper performance.

The hub's economic and legal sustainability is ensured by a combination of long-term and short-term obligations:

core engineering services typically require longer contracts and stable tariffs, whereas additional modules allow more flexible usage models (hourly rental, subscription-based service, mixed payment schemes). This structure makes it possible to redistribute financial flows across directions, compensating for seasonal fluctuations in visitor traffic and for technological demand peaks. As a result, prerequisites emerge for minimizing downtime, improving revenue predictability, and managing risks more transparently—including the risks of non-performance and deterioration in service quality [4, 10].

EV Infrastructure as a Mandatory Element of the Modern City: MIH as a Charging/Parking/Service Node and a "Traffic Anchor"

In recent years, electric mobility has become one of the key drivers reshaping urban infrastructure: by the end of 2024, global electric vehicle sales reached 17 million units [11]. In this context, the multifunctional infrastructure hub (MIH) becomes an "anchor" consumer and an anchor destination, generating a stable visitor flow because EV owners spend substantially more time on-site—ranging from 30 minutes to 4 hours [4].

A longer on-site dwell time naturally increases the value of complementary services and strengthens the multiplier effect for the urban environment: commercial areas, public spaces, and everyday service offerings see higher utilization, supporting a more balanced distribution of transport activity within the district. At the same time, demand becomes more firmly tied to predictable infrastructure quality—above all, the availability of charging capacity, reliable connectivity, and safety while on the premises—requirements that should be reflected in contractual frameworks and operational regulations.

From a legal perspective, operating charging infrastructure as part of MIH requires a clear delineation of obligations among the site owner, the charging network operator, and energy-supplying organizations. Of particular importance are access rules for charging bays, reservation procedures (where applicable), payment and refund terms, and the allocation of responsibility for equipment downtime and deviations from service parameters. The priority of transparent service conditions is driven by the mass nature of consumption and by the need to prevent conflicts related to queue order, limited parking capacity, and the quality of the service provided.

An additional regulatory contour involves ensuring safety and the lawful handling of data generated in the course of EV service delivery. The use of digital accounting and payment tools, integration with navigation and dispatch services, and the deployment of access control systems objectively increase both the volume of processed information and the significance of protective measures. Proper documentation of processes, the regulation of staff access, and a defined incident-response procedure reduce legal risks and strengthen infrastructure continuity—directly aligning with MIH's role as a supporting element of modern urban mobility [4].

Figure 1 will be used to provide a clearer illustration of the dynamics of global expansion in fast-charging networks.

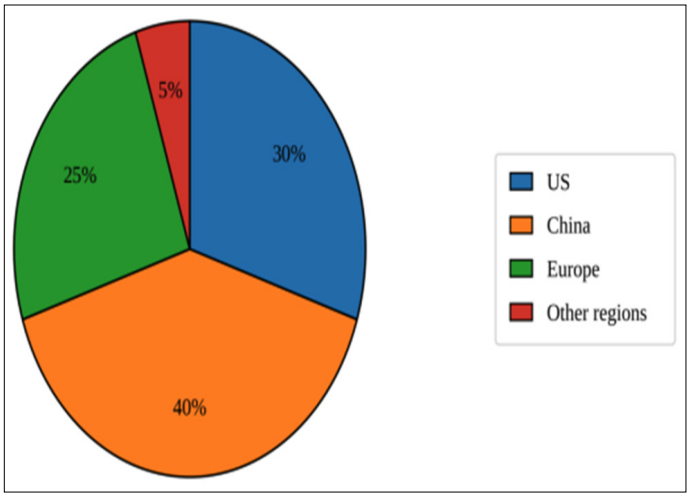

Fig.1. Dynamics of the global expansion of fast-charging networks (compiled by the author based on [4, 9, 12]).

Integrating EV charging transforms the hub from a transit point into a purpose-driven destination, creating opportunities for cross-selling complementary services.

Designing the EV Module: Charger Types (AC/DC), Siting, Navigation, Accessibility, Rules of Use

Designing an EV charging zone requires precision in both engineering and operational parameters. In 2025, the emphasis shifted toward high-power charging nodes (250 kW and above), which significantly reduces waiting time and increases the turnover of parking bays [11]. Key design decisions include siting the module close to supply centers and substations to reduce capital expenditures associated with grid connection and network construction, as well as ensuring interoperability with mapping and navigation services through standardized roaming and data exchange approaches used by the industry (including OCPI-type integration practices). Proper zoning and the deployment of fast-charging connectors ensure high throughput capacity, which becomes critical during peak-load periods.

From the standpoint of legal and regulatory support, correctly structuring the grid connection process and subsequent operation of the facility is essential: determining the required maximum capacity, power supply reliability categories, and limitation and redundancy regimes. With high installed capacity, the role of load dispatching and the formalization of service priority rules increases; these requirements should be secured in operational documentation and in contractual terms with charging infrastructure operators and energy suppliers, including arrangements for commercial metering and liability for deviations in power quality parameters [5].

Equally important is compliance with mandatory safety requirements and anti-terrorism protection for facilities characterized by intensive visitor flows and concentrated energy. Planning solutions should account for fire separation distances, evacuation routes, requirements for electrical equipment placement, and restrictions on access to technical zones, while also ensuring accessibility for low-mobility groups with respect to parking spaces and approaches to charging posts. The presence of standardized regulations for inspections, maintenance, and incident response reduces the risk of downtime and legal disputes related to damage to property, life, or health, and strengthens the overall safety contour of the hub [17, 18].

Digital integration with mapping services and payment solutions drives the need for an appropriate data governance regime and transparent service rules. Practically significant issues include establishing procedures for user identification, tariff calculation, recording the fact of service delivery, and handling claims, as well as regulating access to event logs and information on charging sessions. While protocol-based interoperability (such as OCPI) acts as a mechanism of technological compatibility, legal robustness is achieved precisely through a detailed allocation of rights and obligations among participants, including responsibility for correctly displaying charger availability status and for the accuracy of settlements.

EV Economics: CAPEX/OPEX, Tariffs, Monetizing Dwell Time, Value-Added Services as a Payback Driver

The use of an "end-to-end" operational logic implemented through network slicing in 5G environments can provide guaranteed quality-of-service (QoS) parameters for critical operations by isolating them from mass traffic, thereby increasing the predictability of key services [10, 27] (see Table 3). In the EV module, this predictability is not an abstract technological advantage: it directly affects the stability of payment operations, remote dispatch control, monitoring telemetry, and the integrity of customer-facing digital channels, which together shape both revenue protection and service continuity.

Table 3. Structure of operating expenses (OPEX) of the EV module.

Cost item	Share of OPEX	Risk factor
Electricity (demand charges)	40–70%	Peak loads
Network service (SaaS)	5–10%	Software reliability
Technical maintenance	10–15%	Equipment wear

A primary lever of profitability is demand-side management (Demand Response) combined with the use of subsidy mechanisms that, in a number of jurisdictions, can cover a substantial portion of capital expenditures for charging deployment, thereby improving project economics and reducing payback periods [4, 5]. In practice, the monetization of dwell time becomes a second, equally important channel: the longer the charging session, the higher the potential conversion into additional services—retail purchases, food and beverage, paid parking, or workspace access—turning the EV module into a catalyst for incremental revenue streams rather than a standalone cost center [4]. This logic aligns with the broader assessment that the business viability of fast-charging projects depends not only on electricity margins, but also on the chosen business model, utilization rate, and the structure of complementary revenues [4].

Integrating EV Scenarios into the Overall MIH Ecosystem: "Charging + Service" Bundles, Customer Routing, EV Module KPIs

Synergy between charging infrastructure and retail-and-service formats is achieved through service bundling models such as "charging + coffee," "charging + co-working," and similar pairings that form a unified consumption pattern within a single site. This approach increases demand stability and supports loyalty formation, while also creating conditions for more accurate forecasting of grid load through the introduction of pre-planning mechanisms and flow distribution via booking systems. As a result, the EV module is no longer perceived as an isolated technical installation, but as an embedded element of a broader user journey that links energy consumption to time-efficient, comfortable, and economically meaningful on-site behavior.

Service bundles should be formalized through legally robust models that eliminate uncertainty regarding the status of the service and its components. In practice, applicable structures include a single contract with multiple subject matters, or a set of interconnected contracts in which the charging session and the accompanying service (food service, rental of a workplace, access to communication services) have separate terms and refund rules. To reduce the risks of consumer disputes, transparent pricing, procedures for confirming the delivery of each service component, cancellation rules for bookings, and a clear allocation of responsibility between the charging operator and retail/service providers are all significant elements of the contractual design.

Booking tools and digital identification operate not only as a convenience feature, but also as a capacity management mechanism: advance allocation of time windows helps smooth peaks and reduces the probability of infrastructure overload, strengthening the technological resilience of the facility. At the same time, the digital model requires a regulated approach to information processing, including data

on reservations, payments, and charging session parameters, as well as established rules for data access and retention to ensure confidentiality and prevent unauthorized interference. Where personal data and user activity traces are processed within the customer routing scenario, compliance with the applicable data protection regime and information security expectations becomes a necessary condition for sustainable operations and for reducing legal exposure [6, 7].

The shift toward perceiving charging as an element of everyday service and comfortable on-site presence creates a competitive advantage based not on the price per kilowatt-hour, but on the quality of the surrounding infrastructure and service environment. As a result, the charging zone is integrated into the user scenario as part of aggregated consumption, providing the hub with more predictable occupancy and improving space utilization by coupling the energy service with retail, leisure, and business functions. In management terms, this requires a KPI contour for the EV module that combines throughput indicators (sessions per bay per day, average dwell time, utilization rate), service quality metrics (availability, average wait time, failed session rate), grid-related parameters (peak demand, load smoothing effect), and customer metrics (conversion into bundled services, repeat visits), thereby linking EV operations with the overall MIH performance framework.

CHAPTER 3. DIGITAL MANAGEMENT ARCHITECTURE FOR MIH: CRM, ANALYTICS, AND DIGITAL DATA DISCIPLINE

In the third chapter, a digital governance architecture for MIH is formed as a system in which processes are translated into formalized "digital traces" and become measurable: online scheduling/booking, queue and status management, SLA and incident control with provability of actions through logs, timestamps, and classifiers. The role of CRM is then explained as the core of interaction management: consolidation of client and asset profiles, consumption history, segmentation and trigger communications, as well as the legal fixation of access regimes, data ownership, and processing/consent rules. Separately, data discipline is treated as a mandatory standard (input data quality with <1% errors) for correct analytics and AI optimization, effectively shifting CRM from an accounting tool to a decision-making infrastructure. The chapter closes with a description of integrations (payments, accounting, messengers, equipment monitoring, EV operators/maps) and the analytics layer (KPI dashboards, funnels, seasonality, predictive scenarios) enabling proactive mode switching and reducing managerial and legal uncertainty via predefined thresholds, procedures, and responsibility assignments.

Digital Process Map: Online Scheduling/Booking, Queues, Operation Statuses, SLA Compliance Control

The digital transformation of the management contour begins with formalizing processes and translating them into a regulated format that enables verifiability and comparability of outcomes. By 2025, automation of management procedures makes it possible to reduce incident response times, while remote monitoring ensures real-time control over compliance with service level agreements (SLA). The result is operational transparency that removes "gray zones" in management and allows performance to be assessed objectively for each shift based on a unified, traceable set of indicators [12].

The legal significance of such formalization is expressed in stronger evidentiary support for proper performance of duties and in reduced conflict intensity in relations with counterparties and users. The existence of approved regulations, response route maps, event logs, and unified incident classifiers ensures the reproducibility of management decisions and the correct distribution of responsibility among infrastructure owners, contractors, and service operators. In the event of a dispute, the digital traces of management actions (timestamps, access records, and fault resolution protocols) form a basis for establishing factual circumstances and for assessing whether the parties acted in good faith and with due care.

Technological observation of service quality indicators gains independent value for internal control and risk management. SLA indicators—once embedded in contractual terms—require methodologically correct measurement: identification of data sources, rules for calculating availability and recovery time, and procedures for verification and resolving discrepancies. With properly organized control, the substitution of results with formal reports is excluded, because quality assessment relies on a continuous array of objective data that can be compared across shifts, periods, and infrastructure segments.

At the same time, digitalized management presupposes compliance with information security requirements and proper data-handling regimes, because monitoring and dispatch control are inevitably linked to processing information about events, access, and payments. Normative fixation of access levels, separation of authority, mandatory logging of staff actions, and a regulated response to cyber incidents create conditions for preventing unauthorized interference and minimizing damage. As a result, process transparency is achieved not declaratively, but through a legally grounded linkage of internal regulations, contractual service quality metrics, and protected digital control procedures [12].

CRM as the Core of Interaction Management: Customer/Asset Profile, History, Segmentation, Trigger Communications

A customer relationship management system acts as a central element of a multifunctional infrastructure hub because it accumulates and synchronizes information on electricity consumption, footfall, and purchase structure. Consolidation of these datasets creates a foundation for

moving toward predictive maintenance of equipment and for building targeted communications with users based on real service-consumption scenarios. The result is that the accumulated interaction history acquires the characteristics of an independent intangible asset: it stabilizes demand and enables customer retention mechanisms through improved quality and predictability of service delivery [13].

The legal value of such an asset is determined by the fact that the data generated during operation requires a clear definition of access regimes and a distribution of responsibility among the hub owner, service operators, and contractors who support information systems. Where these issues are underdeveloped, risks arise: loss of control over datasets, difficulties in proving proper performance, and complications in claims management. Accordingly, it becomes materially important to fix in contractual documentation the rules of ownership and use of data arrays, permissible purposes of processing, retention periods, and transfer procedures in the event of a change of operator or software supplier.

Operational advantages of predictive maintenance can be achieved only when data comparability is established through normative and organizational measures: unified equipment directories, fault classifiers, rules for registering performed works, and criteria for taking equipment out of service for repair. With such mechanisms in place, the digital management contour supports a transition from reacting to failures to managing reliability based on statistical patterns, reducing the risk of unplanned downtime and ensuring stable achievement of service quality targets. At the same time, transparency of shift performance and contractor oversight increases, since evaluation is based on recorded events rather than narrative reports.

Targeted communications with users in infrastructure facilities require heightened attention to the lawfulness of data processing and the correctness of consent procedures, especially when using data about visits, payments, and preferences. In the absence of legal certainty, the probability of conflicts grows—related to intrusive messaging, disputable tariffing, as well as challenges to the legal basis for processing and transferring data to third parties. Therefore, a legally resilient model is one in which the rules of informing users, the composition of processed data, the volume and channels of communications, and the opt-out mechanisms are predefined, clearly fixed, and accessible to the user. This reduces regulatory and reputational risks while preserving service effectiveness [13].

Digital Data Discipline (CRM) as a Mandatory Management Standard

Digital data discipline is understood as a system of strict standards and procedures that regulate how data is entered, validated, and maintained. For the correct operation of AI-driven optimization algorithms, the quality of input information is decisive: even minor distortions can accumulate into systematic bias and reduce the reliability of results. In this context, data errors are treated as a critical factor, and the target threshold for their share is set at below 1% [14] (see Figure 2).

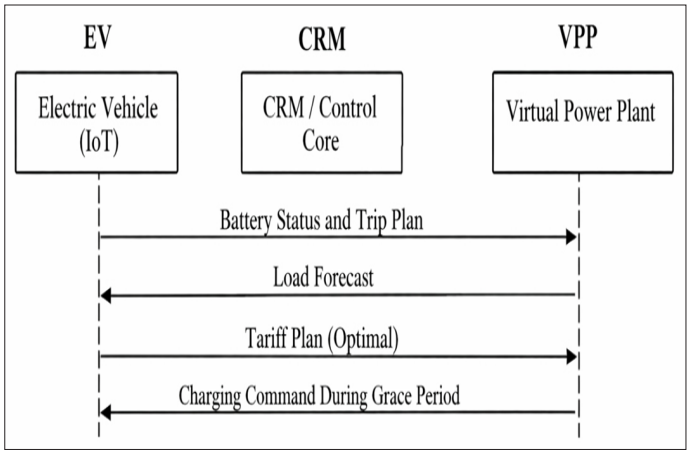

Fig.2. Logic of two-level optimization of the interaction between EV and the hub energy system (compiled by the author based on [4]).

Strict data discipline transforms CRM from a predominantly accounting-oriented solution into an infrastructure that supports automated management decision-making on the basis of reliable and consistent data.

Integrations: Payments, Inventory/Accounting, Telephony/Messengers, Equipment Monitoring, EV Operators/Charging Maps

Deep cross-system integration via application programming interfaces enables an infrastructure hub to operate as a single technological complex in which engineering, service, and settlement contours act in a coordinated manner. The deployment of predictive maintenance based on automated operational analytics and machine-learning methods reduces equipment downtime and supports stability of critical services by shifting the focus from reactive repair to condition-based intervention [15]. Interim conclusion: connecting to external aggregators (such as PlugShare and similar platforms) supports a steady inflow of new users by ensuring the hub's presence in global navigation and reference ecosystems [9].

The legal resilience of such integration is determined not so much by the mere fact of technological connectivity as by the formalization of data exchange conditions and the allocation of responsibility among participants. Contractual provisions on ownership of data arrays, permissible processing purposes, access-granting procedures, requirements for transaction logging, and incident notification obligations—as well as the legal consequences of compromising the integrity or availability of information resources—are of material importance. Without these elements, the risk of "diffused" accountability increases across the infrastructure operator, software vendors, and external platforms, complicating

claims resolution and the establishment of causal links when failures occur.

Predictive equipment maintenance requires a normatively fixed methodology for generating and using diagnostic data: unified asset registries, fault classifiers, rules for verifying signals, and criteria for taking units out of service for repair. In a legally robust model, technical intervention decisions rely on documented condition indicators, and subsequent works are recorded as execution of approved maintenance-and-repair regulations with specification of time, scope, and responsible persons. Such an architecture strengthens the evidentiary basis of proper operation, reduces the probability of recurring downtime, and supports compliance with service quality parameters agreed with counterparties [15].

Integration with external aggregators and navigation systems requires adherence to principles of accuracy and internal consistency of published information, because errors in availability status, tariffs, and operating modes generate reputational and claims-related risks. Accordingly, agreements with aggregators should define procedures for updating information, liability for data distortion, deadlines for correcting errors, and mechanisms for handling user complaints. Additionally, issues of non-discriminatory access and fair competition become relevant: presence in navigation services should be accompanied by transparent display criteria and correct tariffing that avoids misleading users and supports stable user flow formation without sacrificing service quality.

Analytics and Management Decisions: KPI Dashboards, Funnels, Seasonality, Predictive Scenarios

The analytical management contour enables proactive switching of operating modes ("normal"/"peaks") based on combined data on weather conditions, transport load, and holiday calendars. Under this approach, the infrastructure operating regime is not determined after the fact, but as the result of a formalized assessment of predictive factors, allowing coordinated redistribution of capacity, personnel, and service resources before maximum load occurs [16].

For the legal and organizational support of this model, it is essential to fix in local acts the list of indicators, threshold values, and the decision-making procedure for changing regimes. Internal regulations should define the authority of dispatch and operations teams, the procedure for notifying contractors, the criteria for prioritizing service provision, and the requirements for documenting management actions. The existence of such procedures increases the evidentiary strength of proper management and reduces the likelihood of conflicts related to service order, temporary restrictions on access to certain services, or short-term changes in rules for infrastructure use [16].

A technically grounded change of regimes presupposes accounting for constraints in power supply and site throughput, including load-limitation modes and the need to reserve critically important functions. During "peaks," it is advisable to provide algorithms for dynamic power distribution among charging posts, strengthening shifts, and altering on-site traffic logistics, because it is precisely the set of measures—rather than a single technical solution—that ensures preservation of target service quality indicators. At the same time, the significance of safety measures increases, including access control to technical zones, prevention of equipment overheating, and readiness for abnormal situations under higher visitor density [16].

Integrating weather, traffic, and holiday-period data into management decisions requires compliance with information quality requirements and continuity of data inflow. In this part, it is critical to define data sources, verification procedures, permissible update delays, and action algorithms when external channels are unavailable. With proper configuration of the analytics block, load predictability increases and the risk of disruptions decreases, simultaneously improving infrastructure utilization efficiency and reducing managerial uncertainty under peak demand fluctuations [16]. Predictive analytics makes it possible to allocate resources in advance for expected demand, preventing queues and grid overload.

CHAPTER 4. COMPREHENSIVE SAFETY AND RESILIENCE OF MIH: REGIONAL STANDARDS, INCIDENT MANAGEMENT, COMPLIANCE

In the fourth chapter, a comprehensive security and resilience model for MIH is presented, grounded in a risk map under uncertainty (technological, energy, operational, human-factor, and information threats) and in the linkage of engineering measures with digital monitoring and provable control. The chapter then formulates regional MIH safety standards developed by the author, with emphasis on critical zones (including EV loops) and on a continuous-improvement CAPA cycle as a mechanism for root-cause identification, corrective actions, and prevention of repeated incidents. A separate component addresses standard implementation through training, checklists, audits, and a compliance culture: 100% coverage of staff and contractors, role-based accountability, documented procedures, and the reduction of "gray zones" through reproducible regulations. A substantial block is devoted to payment and information security (access control, logging, antifraud, and protection against social engineering), including tokenization and immutable operation journals as tools for improving integrity, investigability, and user/partner trust. The chapter concludes with a KPI system for security and resilience (incident frequency/severity, response time, audit results, and compliance level), where metrics serve both as managerial indicators and as legal criteria of due performance, directly shaping economic sustainability by preventing downtime, penalties, and insurance losses.

MIH Risk Map Under Uncertainty: Technological, Energy, Operational, Human Factor, Information Risks

The safety of a multifunctional infrastructure hub presupposes simultaneous counteraction to information threats and the management of physical risks, including fires and failures in network facilities. Against the backdrop of rising global turbulence and the increasing strain on supply chains and infrastructure systems, this objectively raises requirements for the resilience of the digital management contour and for the reliability of engineering infrastructure [1, 21]. Interim conclusion: comprehensive risk monitoring makes it possible to detect threats at an early stage and minimize damage.

The legal construct of protection should be built on a formalized distribution of duties among the facility owner, the operator of information systems, and contractor organizations performing technical maintenance. Of material significance is the fixation—in contracts and local acts—of procedures for delineating access to critical components, requirements for logging staff actions, deadlines for remediation of identified vulnerabilities, as well as incident notification procedures and interaction with authorized services. Such distribution eliminates uncertainty of responsibility during incidents and strengthens the evidentiary basis for proper performance of safety obligations.

Physical risks require not only engineering measures, but also a normatively supported system of prevention and response: establishing inspection regulations, test periodicity and maintenance schedules, procedures for taking equipment out of operation when parameters deviate, as well as evacuation algorithms and consequence localization. For facilities with a high concentration of energy equipment, documenting dispatch decisions and recording the actions of operational personnel is critical, because these records form the foundation for subsequent legal assessment of the causes of the incident and the correctness of measures taken.

Integrating digital risk-detection tools with engineering systems is advisable provided that indicators and trigger thresholds are configured methodologically correctly and that continuity of data flows is ensured. It becomes legally significant to establish requirements for measurement reliability, procedures for storing event logs, and access to them, since monitoring results are used both for internal quality control of operation and for resolving claims related to downtime, property damage, or deviations from service parameters. As a result, the risk management system becomes not declarative but verifiable, contributing to the reduction of both factual and legal losses [17, 18].

Regional Safety Standards (Developed by the Author) for MIH

The author's standards cover requirements for chemical safety, electrical safety, fire safety, and occupational safety. A priority emphasis is placed on regulating EV zones with a focus on strict electrical safety requirements and on formalizing incident management through CAPA plans that ensure cause identification, corrective actions, and prevention of recurrence [17, 18, 24, 25] (see Figure 3).

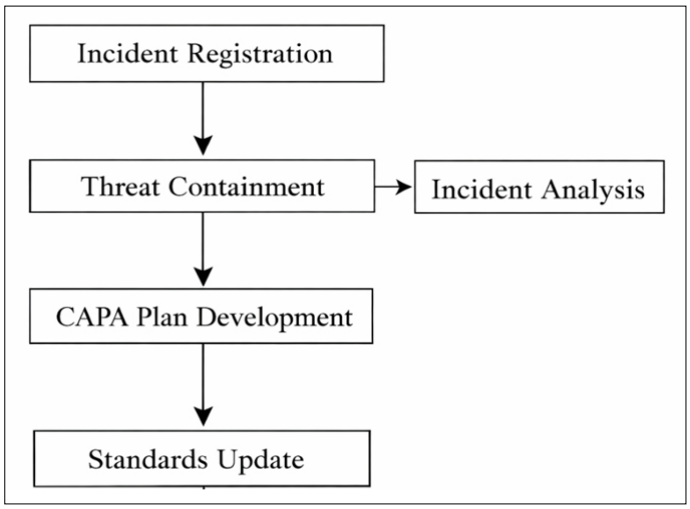

Fig.3. Continuous safety improvement cycle (CAPA) (compiled by the author based on [17, 18, 24, 25]).

The implementation of the author's standards creates a unified protective contour that does not depend on the qualifications of individual on-site employees.

Implementing the Standards: Training, Checklists, Audits, Compliance Culture, Role-Based Accountability

Implementation of standards in operational practice is enabled through digital checklists and remote learning platforms that unify requirements and record the outcomes of their application. Regular personnel certification should cover 100% of workers, including employees of contractor organizations authorized to service engineering and information infrastructure [18, 20].

Digital checklists perform not only an organizational function but also a legally significant one, because they ensure the documentability of mandatory procedures, the traceability of actions taken by specific officials, and the reproducibility of control results. When checklists are configured correctly, uniform execution of operations is achieved, the risk of arbitrary interpretation of regulations is minimized, and the probability of substituting actual performance with formal reporting is reduced. In disputable situations, such records form an evidentiary basis for confirming compliance with technological requirements, including verification of inspection periodicity, completion of preventive measures, and the timeliness of eliminating identified nonconformities.

Remote learning platforms and personnel certification are advisable provided that the content of programs, the frequency of knowledge checks, and the criteria for admission

to high-risk work are fixed normatively. Mandatory training should be accompanied by recorded outcomes, the retention of testing protocols, and a re-training procedure in cases of unsatisfactory results, which improves manageability of workforce-related risks. A comprehensive model covers not only initial training but also regular updating of knowledge in response to changes in regulatory requirements and internal procedures, because it is the currency of competencies that determines personnel capability to act properly in abnormal situations [18, 22].

A culture of compliance is formed through systemic incentives and transparent feedback mechanisms, where the identification of violations is treated as a basis for corrective measures rather than as an instrument of repression. In such a model, incident prevention becomes the priority: timely identification of deviation causes, elimination of organizational gaps, improvement of briefings, and optimization of access-to-work procedures. Practical effectiveness is achieved when personal accountability is combined with supporting mechanisms—clear regulations, accessible training materials, regular inspections, and management evaluation not only of the outcome but also of adherence to the prescribed sequence of actions—which consistently reduces the likelihood of errors and increases the predictability of operational safety [18, 23].

Payment and Information Security: Access Control, Logging, Anti-Fraud, Protection Against Social Engineering

Data protection in a multifunctional infrastructure hub can be strengthened through tokenization and immutable operation logging based on distributed ledger technologies, which increases control over critical actions within information systems [19]. These mechanisms make unauthorized interference with hub management parameters more difficult, because access to sensitive operations is tied to verifiable authority, and information about actions taken is recorded in a form resistant to covert modification [19]. Interim conclusion: reliable protection of information processes builds trust among users and partners, which becomes a key condition for the sustainability of service-economy assets [6, 19].

Within this logic, tokenization is treated as a way to minimize the volume of identifiers and payment credentials processed in applied contours: operational systems use de-identified representations, while source values are stored in protected segments. This approach reduces potential damage if individual components are compromised, simplifies access segmentation, and enables a differentiated processing regime depending on criticality level. An additional effect is the strengthening of internal control, because access to source data becomes exceptional and is subject to separate recording.

Distributed-ledger-based logging should be qualified as an instrument for ensuring the integrity and verifiability of management actions—above all with respect to configuration changes, access rights, and parameters affecting safety and continuity. The practical value of such a solution is expressed in reduced risk of hidden alteration of event logs and in simplified subsequent incident investigation: traceability of the action chain is ensured, a technically confirmed chronology is formed, and the evidentiary suitability of records increases for internal reviews and claims resolution [19, 25]. At the same time, the robustness of the mechanism is determined not only by the recording technology, but also by organizational procedures—segregation of authority, multi-factor confirmation for critical operations, and regular audits.

The economic significance of a protected digital contour is linked to the fact that hub services depend on uninterrupted payment, dispatching, and access processes, while trust becomes a factor that directly affects the user's choice of a particular site and the willingness of partners to integrate. Verifiable mechanisms for change control and proper data handling reduce operational and reputational risks, improve the predictability of service quality, and strengthen contractual discipline in relations with service operators and technology solution providers [19, 20].

Safety and Resilience KPIs: Incident Frequency/ Severity, Response Time, Audit Results, Standard Compliance Level

The effectiveness of the management and safety system is confirmed by the resilience of continuous operational processes, expressed in the absence of critical downtime, as well as by maintaining a zero level of occupational injury. These indicators reflect not a one-time success, but the stability of an organizational and technical model in which the fault tolerance of engineering infrastructure and disciplined execution of regulations ensure predictable service delivery and minimize adverse consequences.

From a legal standpoint, these outcomes function as integral indicators of proper fulfillment of obligations to provide safe working conditions and safe operation of the facility. The absence of injuries—subject to correct accounting and documentation of incidents—indicates the effectiveness of briefings, certification, admission to work, and control over compliance with mandatory occupational safety requirements. The absence of critical downtime, in turn, reflects the sufficiency of measures related to maintenance, redundancy, incident management, and compliance with service quality parameters fixed in contractual obligations [17, 18, 25].

Methodologically correct fixation of these indicators requires a unified approach to classifying incidents and downtime, setting "criticality" thresholds, distinguishing causes by responsibility zones, and confirming data through primary digital logs. With such an evidentiary base, the indicators can be used not only for internal evaluation of shifts and

contractors, but also as an element of management reporting and as justification of the economic effectiveness of investments in safety, maintenance, and digital monitoring (see Table 4).

Table 4. KPIs of the MIH safety and resilience system.

Indicator	Target value	Verification method
Standard compliance level	100%	Monthly audit
Fault localization time (electric power)	< 30 seconds	Automated IoT logs

Achieving target safety KPIs directly correlates with the facility's economic resilience through the avoidance of penalties and insurance payouts.

CONCLUSION

This methodological guide has developed and substantively verified an innovative management model for multifunctional infrastructure facilities (MIH) intended for application in an environment of high uncertainty. Over the course of the study, the full spectrum of declared objectives has been achieved: the significance of MIH as supporting nodes of regional resilience has been articulated; an analytical examination of the "end-to-end service" architecture has been conducted; and the defining role of EV infrastructure as a factor stimulating economic development has been substantiated. The results indicate that coupling physical modules with rigorously standardized digital data discipline reduces operational risks and delivers an increase in user satisfaction of more than 20%.

The author-developed regional safety standards form a coherent protective contour for the facility, including requirements for chemical safety, electrical safety, and fire safety, which becomes particularly relevant in the context of the 2024 updates to hazard communication and related regulatory expectations. The final conclusion is that sustainable MIH performance under uncertainty is determined by the system's capacity for rapid scenario-based adaptation and by the accuracy level of predictive analytics implemented on the CRM foundation. The proposed model is scalable and allows adaptation to different regional development contours oriented toward achieving technological leadership. The provisions presented have strategic relevance for top management of infrastructure companies, regional governance bodies, and risk-management professionals in the energy and transport sectors.

REFERENCES

1. Xeneta. (2025, March 28). The biggest global supply chain risks of 2025. Retrieved from: https://www.xeneta.com/blog/the-biggest-global-supply-chain-risks-of-2025 (date accessed: October 1, 2025).
2. Burgess, S. (2015). Multifunctional green infrastructure: A typology. In D. Sinnett, N. Smith, & S. Burgess (Eds.), Handbook on green infrastructure: Planning, design and implementation (pp. 227–241). Edward Elgar Publishing. https://doi.org/10.4337/9781783474004.00020
3. Li, L., & Carter, J. (2025). Exploring the relationship between urban green infrastructure connectivity, size and multifunctionality: A systematic review. Landscape Ecology, 40(3), 61. https://doi.org/10.1007/s10980-025-02069-1
4. Bernal, D., et al. (2024). Assessment of economic viability of direct current fast charging stations: Business models and profitability considerations. Sustainability, 16(15), 6701. https://doi.org/10.3390/su16156701
5. U.S. Department of Energy, Alternative Fuels Data Center. (n.d.). Procurement and installation for electric vehicle charging infrastructure development. Retrieved from: https://afdc.energy.gov/fuels/electricity-infrastructure-development (date accessed: October 9, 2025).
6. United Nations Conference on Trade and Development (UNCTAD). (2025, December 3). Global trade update (December 2025). Retrieved from: https://unctad.org/system/files/official-document/ditcinf2025d10_en.pdf (date accessed: December 5, 2025).
7. European Telecommunications Standards Institute (ETSI). (2019, February). Developing software for multi-access edge computing (ETSI White Paper No. 20, 2nd ed.). Retrieved from: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp20ed2_MEC_SoftwareDevelopment.pdf (date accessed: October 11, 2025).
8. Tang, J., & Li, X. (2025). Two-stage dual-level dispatch optimization model for multiple energy resources. Energies, 18(4), 896. https://doi.org/10.3390/en18040896
9. U.S. Department of Energy, Alternative Fuels Data Center. (n.d.). Electric vehicle charging stations: Charging infrastructure procurement and installation. Retrieved from: https://afdc.energy.gov/fuels/electricity-stations (date accessed: October 15, 2025).
10. Mahmood, N. H., et al. (2022). Design, development, and evaluation of 5G-enabled vehicular services: The 5G-HEART perspective. Sensors, 22(2), 426. https://doi.org/10.3390/s22020426
11. Recurrent. (2025, May 1). EV market trends report: Growth in public charging infrastructure continues (White paper). Retrieved from: https://www.recurrentauto.com/research/ev-market-trends-report (date accessed: October 19, 2025).

12. Nearby Computing. (n.d.). NearbyOne. Retrieved from: https://www.nearbycomputing.com/nearbyone/ (date accessed: October 21, 2025).

13. Singapore FinTech Association. (n.d.). Member-2-member directory. Retrieved from: https://singaporefintech.org/member-2-member-directory/ (date accessed: October 23, 2025).

14. Rotsos, C., et al. (2017). Network service orchestration standardization: A technology survey. Computer Networks, 115, 123–142. https://doi.org/10.1016/j.comnet.2016.11.021

15. Gartner. (n.d.). Definition of AIOps (artificial intelligence for IT operations). Retrieved from: https://www.gartner.com/en/information-technology/glossary/aiops-artificial-intelligence-operations (date accessed: October 27, 2025).

16. U.S.-ASEAN Business Council. (2024). US-ABC recommendation paper: The electric vehicle ecosystem in ASEAN. Retrieved from: https://www.usasean.org/sites/default/files/2024-03/US-ABC%20Recommendation%20Paper%20-%20Electric%20Vehicle%20Ecosystem%20in%20ASEAN.pdf (date accessed: October 29, 2025).

17. U.S. Bureau of Reclamation. (2024). Reclamation safety and health standards—2024 edition: Electrical safety requirements (Section 1.10). Retrieved from: https://www.usbr.gov/safety/rshs/documents/1.10%20Electrical%20Safety%20Requirements.pdf (date accessed: October 31, 2025).

18. Occupational Safety and Health Administration. (2015). Training requirements in OSHA standards (OSHA 2254). Retrieved from: https://www.osha.gov/sites/default/files/publications/osha2254.pdf (date accessed: November 2, 2025).

19. Srinivas, O., Pradhan, N. R., & Nanda, S. D. (2025). Sustainable energy-driven P2P blockchain system for tracking EV performance and maintenance. In Sustainable Energy Technologies and Computational Intelligence (SETCOM). https://doi.org/10.1109/SETCOM64758.2025.10932447

20. Korkou, M., Tarigan, A. K., & Hanslin, H. M. (2023). The multifunctionality concept in urban green infrastructure planning: A systematic literature review. Urban Forestry & Urban Greening, 85, 127975.

21. McKinsey & Company. (2025, December 2). Supply chain risk pulse 2025: Tariffs reshuffle global trade priorities. Retrieved from: https://www.mckinsey.com/capabilities/operations/our-insights/supply-chain-risk-survey (date accessed: December 10, 2025).

22. Korkou, M., Tarigan, A. K. M., & Hanslin, H. M. (2023). The multifunctionality concept in urban green infrastructure planning: A systematic literature review. Urban Forestry & Urban Greening, 85, 127975. https://doi.org/10.1016/j.ufug.2023.127975

23. United Nations Conference on Trade and Development (UNCTAD). (2025, October 22). Global supply chains under strain – ministers call for just and resilient transitions. Retrieved from: https://unctad.org/news/global-supply-chains-under-strain-ministers-call-just-and-resilient-transitions (date accessed: November 10, 2025).

24. Federal Register. (2024, May 20). Hazard communication standard (Final rule). Retrieved from: https://www.federalregister.gov/documents/2024/05/20/2024-08568/hazard-communication-standard (date accessed: November 12, 2025).

25. Occupational Safety and Health Administration. (n.d.). OSHA's final rule to amend the hazard communication standard. Retrieved from: https://www.osha.gov/hazcom/rulemaking (date accessed: November 14, 2025).

26. U.S. Department of Energy, Alternative Fuels Data Center. (2024). Electric vehicle charging infrastructure trends: Second quarter 2024. Retrieved from: https://afdc.energy.gov/files/u/publication/electric_vehicle_charging_infrastructure_trends_second_quarter_2024.pdf (date accessed: November 16, 2025).

27. Corujo, D., Cunha, V. A., Perdigão, A., Silva, R., Santos, D., Aguiar, R., Paixão, P., Elísio, P., Antunes, R., Marques, C. M., Gomes, A., & Quevedo, J. (2023). An empirical assessment of the contribution of 5G in vertical industries: A case for the transportation sector. IEEE Access, 11, 15348–15363. https://doi.org/10.1109/ACCESS.2023.3243732