TECHNICAL UNIVERSITY OF CLUJ-NAPOCA

ACTA TECHNICA NAPOCENSIS

Series: Applied Mathematics, Mechanics, and Engineering
Vol. 69, Issue Special III, July, 2026

DIGITAL TRANSFORMATION OF MILITARY LOGISTICS IN THE INDUSTRY 4.0 ERA: AI FOR TECHNICAL SKILLS DEVELOPMENT AND MAINTENANCE OPTIMIZATION

Ciprian CUSUTURĂ, Toma PLEȘANU, Tiberiu GIURGIU

Abstract: *This work examines how a NATO member state can modernize military logistics and maintenance through Industry 4.0 principles and AI-enabled decision support. It frames logistics as an operational function shaped by multinational interoperability, high-tempo deployment, and contested environments. A layered reference architecture is proposed, linking sensors and local gateways to a central data platform, analytics modules, and decision dashboards, with cybersecurity and resilience built in. The study highlights predictive analytics, anomaly detection, reliability estimation, and optimization for stocks and transport, and it addresses workforce upskilling and AI-assisted training. Practical recommendations emphasize data governance, phased pilots, and alignment with allied standards.*

Keywords*: Industry 4.0; military logistics; predictive maintenance; artificial intelligence; NATO interoperability.*

1. INTRODUCTION

Modern military logistics operates in a complex strategic environment in which NATO member states must sustain both high-intensity collective defense and diverse missions, from air policing to civil support. Despite differing support profiles, all require rapid response, full life-cycle resource management, and multinational coordination. The growing complexity of assets, including IT systems and sensors, makes traditional stock accounting insufficient and demands an integrated view of cost, risk, and operational impact.

Rapid deployment, dispersed forces, and exposure to kinetic, cyber, and hybrid threats position logistics as a core element of operational planning rather than a rear-area activity. However, many organizations still rely on fragmented processes and delayed reporting, leading to outdated situational awareness. Digital transformation addresses this gap by integrating equipment, storage, and transport data into unified systems, enabling near real-time visibility and condition-based maintenance supported by analytics [1].

Beyond technology, digital transformation requires procedural redesign, workforce upskilling, and the structured interpretation of AI-generated indicators. Cybersecurity, auditability, and continuity planning must be embedded from the beginning, given the vulnerabilities of interconnected systems. At the same time, budget constraints reinforce the need to link optimized logistics and maintenance practices to measurable readiness outcomes [2].

Recent research frames AI integration in logistics as a capability-building process in which data-driven knowledge processes and dynamic organizational capabilities are hybridized, enabling faster sense-making, adaptive decision-making, and sustained operational effectiveness in complex and uncertain environments [3].

Although digital transformation in military logistics is widely discussed, several gaps persist, including limited methodological formalization linking AI models to operational

KPIs, insufficient distinction between illustrative frameworks and empirically validated results, and underdeveloped guidance for phased legacy-system integration.

This paper is positioned as a research-oriented design framework combining structured methodological formulation with illustrative case-based evaluation.

Its main contributions are:

- a layered AI-enabled architecture aligned with operational logistics requirements;
- formalized KPI definitions integrated into a comparative evaluation structure;
- a structured anomaly-detection and decision-support logic;
- a phased interoperability model.

2. NATO OPERATIONAL LOGISTICS

In modern military operations, logistics is an essential operational function rather than a supporting service. Allied doctrine, including AJP-4, treats logistics as a core enabler of freedom of action, force concentration, and operational endurance. Without a credible supply chain, even a well-trained and well-equipped force cannot be sustained and gradually loses operational relevance [4].

For a NATO member state, logistics shapes decisions at strategic, operational, and tactical levels. Strategically, it supports force generation and sustainment, operationally, it converts resources into deployable capability and tactically, it delivers supplies and technical support under mobility and risk constraints. In joint operations, logistics must support land, air, naval, and cyber forces with distinct demand profiles while maintaining a coherent view of priorities and resource constraints [5].

Most NATO members structure logistics at strategic, operational, and tactical levels aligned with allied principles and national systems. Strategic bodies set policy and plan long-term resources, operational commands manage supply, storage, contracts, and transport flows, and tactical units deliver supplies and conduct short-term repairs near combat forces. Across all levels, logistics coordinates activities through the full cycle of planning, delivery, recovery, and disposal, supported by node-based movement concepts and digital tools such as LOGFAS [4].

Studies on cross-docking strategies show that redesigning logistics flows around synchronized inbound and outbound operations can significantly reduce handling time, inventory holding, and overall logistics costs, while increasing responsiveness and reliability in complex supply networks [5].

Persistent “data friction” limits readiness. Delays from manual collection, sequential consolidation, and layered validation mean leaders often plan to use an outdated picture. Accuracy suffers when echelons keep mismatched records, while weak traceability in mixed paper and partial digital setups makes it hard to track items across procurement, storage, use, repair, transfer, and disposal, increasing safety risks when defective lots or parts must be identified. These gaps drive reactive maintenance, more unplanned failures, and longer downtime, complicating force generation for NATO missions. Industry 4.0 shows data discipline and analytics can raise availability, but military logistics also needs security, resilience, and multinational standardization.

3. INDUSTRY 4.0 IN THE MILITARY DOMAIN

Industry 4.0 describes a model in which physical assets and digital systems are integrated through sensors, connected equipment, and shared data platforms, a concept that aligns well with data-driven military environments. In military logistics, its principles translate into interoperability based on common data standards, near real-time visibility of stocks, movements, asset condition, and decision support driven by analytics rather than periodic reports. It also promotes controlled decentralization, modular and scalable architectures, and digitally governed ecosystems that integrate military units with suppliers and partners [6].

In practice, Industry 4.0 is enabled by a stack of technologies used together. **IoT**

provides identification and sensing for tracking containers, pallets, ammunition lots, and critical parts, as well as monitoring vehicles, trailers, and storage facilities. **Cyber-physical systems** connect sensors, control elements, and software so that warehouses, maintenance workshops, and even logistics convoys can be coordinated and partly automated, but this raise demands for cybersecurity and rigorous data standardization. The layered separation between sensing, integration, analytics, and decision functions reflects established cyber-physical system architectures associated with Industry 4.0 implementations [7].

Digital twins extend this approach by providing continuously updated models of fleets and logistics networks, enabling simulation of wear, bottlenecks, and disruption scenarios before they affect operations. This supports condition-based and predictive maintenance, risk-based prioritization, and more efficient allocation of transport and spare parts, provided that data streams remain reliable and timely [8].

Cloud computing, including hybrid and edge models, provides the backbone for collecting and processing data from IoT, CPS, and digital twins across military logistics structures. Effective integration requires clear data architecture defining collection, validation, model execution, and information flow across tactical, operational, and strategic levels, as well as across logistics, maintenance, transport, and allied systems. Key challenges include legacy systems, fragmented data, skills gaps, digital sovereignty concerns, and strict confidentiality requirements [9].

NATO, EU, and other international programs already illustrate the direction of travel: digitalization of movement authorization and documentation to speed and secure military mobility, stronger cyber resilience for dual use infrastructure, and pilots that consolidate stock and transport visibility into shared platforms. EDA-related work cited in the text points to digital product passports for life cycle traceability and improved maintenance history access, alongside exploration of unmanned platforms for logistics tasks, while several defense organizations pursue multi-cloud approaches and digital twin pilots for critical infrastructure and major platforms [10],[11],[12].

4. METHODS

This study employs a structured comparative design to evaluate the operational implications of AI-enabled maintenance within two representative contexts: a mixed vehicle fleet and a CNC-based technical workshop. The objective is to assess the internal coherence and performance behavior of the proposed framework rather than to provide empirical validation based on classified operational data.

The analysis is based on defined performance indicators, including availability, mean time to repair (MTTR), unplanned failure rate, total downtime per asset, and reject rate in workshop operations. Availability is calculated as the ratio between effective operating time and scheduled operating time, while MTTR reflects the average duration of repair events. Performance improvement is expressed as percentage change between baseline and post-implementation scenarios.

The case studies rely on structured illustrative datasets designed to reflect plausible maintenance dynamics under documented operational assumptions. These datasets do not represent real NATO deployment records but are constructed to simulate typical performance ranges observed in publicly reported defense sustainment contexts [13],[14]. The purpose is to test model behavior under controlled conditions.

Validation is conducted through comparative KPI analysis and consistency checks of the anomaly-detection and decision-support logic. The study demonstrates methodological coherence and operational plausibility, while full empirical validation using real operational data remains a direction for future research.

Failure frequency was modeled as a homogeneous Poisson process, assuming independent failures and constant annual intensity. The probability of observing k failures in time interval t is:

$$P(N(t) = k) = \frac{(\lambda t)^k e^{-\lambda t}}{k!} \quad (1)$$

where λ represents the average number of failures per asset per year. As the observation interval in this study is one year (t = 1), λ directly equals the expected annual failure rate.

For each simulation run, the annual number of failures for each asset was generated as:

$$N_i \sim \text{Poisson}(\lambda) \quad (2)$$

For each asset, the annual number of failures was generated independently as a Poisson-distributed random variable.

Repair durations were modeled using a log-normal distribution:

$$T_r \sim \text{LogNormal}(\mu, \sigma^2) \quad (3)$$

with parameters selected so that the expected repair time:

$$E[T_r] = \exp\left(\mu + \frac{\sigma^2}{2}\right) \quad (4)$$

matches the observed baseline MTTR. Total downtime per asset was computed as:

$$D = \sum_{j=1}^{N} T_{r,j} \quad (5)$$

and operational availability as:

$$A = \frac{T_{scheduled} - D}{T_{scheduled}} \quad (6)$$

Each scenario was evaluated using 1000 Monte Carlo runs (seed = 42). Reported KPI values represent mean outcomes, with uncertainty expressed through 95% confidence intervals:

$$CI = \bar{X} \pm 1.96 \frac{s}{\sqrt{n}} \quad (7)$$

Three scenarios were analyzed: baseline, moderate AI impact (−15% failure intensity, −20% repair duration), and high AI impact (−30% failure intensity, −30% repair duration), with additional ±10% sensitivity testing of failure intensity.

The probabilistic modeling framework described above provides the quantitative basis for the performance comparisons presented in the following case studies.

5. AI-ENABLED MILITARY LOGISTICS

Predictive maintenance approaches in Industry 4.0 environments typically combine sensor-based monitoring, historical failure data, and supervised or semi-supervised machine learning models to estimate remaining useful life and failure probability under operational variability [8],[15],[16].

Predictive analytics leverages historical and real-time data to estimate future demand, failure probability, and sustainment needs, including spare parts consumption, major repair and forward stock requirements. In a NATO context, it supports national planning and pre-deployment preparation through scenario testing and model-based estimation, replacing heuristic assumptions while preserving human decision authority [8],[15].

Anomaly detection represents a practical AI application in military maintenance by identifying early deviations in parameters such as vibration, temperature, response time, or consumption patterns before complete failure occurs. In industrial and cyber-physical systems, anomaly detection models such as Isolation Forest, one-class SVM, and density-based methods are widely used to identify deviations from learned baseline behavior in high-dimensional sensor data streams [17]. By monitoring selected critical assets and generating graded alerts linked to predefined procedures, maintenance shifts from reactive repairs to planned interventions, improving technician scheduling and reducing unplanned stoppages.

AI also enhances logistics flow optimization across inventory positioning, reorder levels, transport routing, and distribution planning under operational constraints. Scenario simulation, including infrastructure disruption or supplier delays, enables not only cost

optimization but also reduced exposure, congestion, and stockout risk during high-tempo operations.

Pattern analysis of technical and operational data reveals correlations between mission type, environment, load profile, and failure behavior. However, effective use requires disciplined data governance, cybersecurity safeguards, and expert interpretation, as poor data quality or manipulated systems can compromise results. Clear human accountability, audit mechanisms, and controlled deployment remain essential.

Despite formal oversight mechanisms, automation bias may emerge, particularly under operational pressure. Regular simulations, scenario-based exercises, and structured performance evaluation are therefore necessary to ensure personnel retain critical judgment and do not over-rely on recommendations.

The growing integration of sensors, data platforms, and analytics expands the attack surface of military logistics systems, introducing risks such as data manipulation, spoofing, denial-of-service, and lateral propagation. Mitigation measures include network segmentation, encrypted transmission, role-based access control, continuous monitoring, and audit logging, alongside degraded-mode procedures that allow core logistics functions to revert to validated manual processes if required.

Accordingly, the architecture incorporates zero-trust principles, strict identity validation, least-privilege access, telemetry monitoring, and predefined incident response procedures to maintain operational continuity even in partial system compromise scenarios.

Within this structured environment, anomaly detection and fault-risk estimation rely on defined operational features and probabilistic modeling. Key inputs include vibration RMS, temperature gradients, current deviation, operating hours, and maintenance history. The anomaly-detection component is based on an Isolation Forest algorithm, selected for its robustness in unsupervised detection of rare events in multidimensional datasets, while a logistic regression classifier estimates failure probability based on engineered operational features. This hybrid approach aligns with established predictive-maintenance architectures combining anomaly scoring and probabilistic risk estimation [16],[18].

The feature set used for anomaly detection and failure-risk estimation included: vibration RMS, vibration trend slope (24h window), mean temperature, temperature gradient, electrical current deviation, operating hours since last maintenance, cumulative load cycles, and recent alert frequency. All features were aggregated over rolling 24-hour windows. Continuous variables were standardized using z-score normalization. Outliers beyond three standard deviations were capped to reduce extreme-value distortion. Missing values were handled through forward filling within operational intervals. The Isolation Forest model was implemented with 100 estimators, contamination rate set to 0.05, and default subsampling size. Logistic regression used L2 regularization with regularization parameter C = 1.0. Anomaly alerts were triggered when the Isolation Forest score exceeded the 95th percentile of baseline anomaly distribution. Failure-risk alerts were generated when predicted probability exceeded 0.7, selected based on ROC curve analysis to balance recall and false positive rate. Model performance was evaluated using area under the ROC curve (AUC), precision, recall, and false positive rate. Evaluation was conducted on the simulated dataset using 5-fold cross-validation.

6. CASE STUDIES: VEHICLE FLEET AND CNC WORKSHOP

6.1. Maintenance of a ground-vehicle fleet

The fleet consists of 180 ground vehicles: 60 tracked armored vehicles, 80 8×8 logistics trucks, and 40 special-purpose vehicles (mobile workshop, tanker, recovery/evacuation). The fleet is used for national training and for preparing participation in multinational exercises. The unit leadership reported below-target technical availability, delays in deployment, and a high volume of unplanned corrective maintenance.

The initial approach relied on fixed periodic inspections, reactive corrective maintenance, and paper-based failure recording later consolidated in spreadsheets.

Key indicators:

- 432 recorded failure events (279 unplanned);
- average technical availability: 87%;
- mean time to repair: 4.8 days;
- 23 logistics missions were postponed or reconfigured due to insufficient availability.

Event analysis showed precursor signals for many unplanned failures, like rising engine temperatures before cracks in the cooling system, increasing drivetrain vibrations before differential failures and gradual pressure losses in pneumatic systems, not detected in time.

After 18 months, for 120 vehicles (all armored vehicles and 50% of the 8×8 trucks), the brigade implemented:

- telemetry modules collecting mileage, fuel consumption, engine and oil temperatures, pressures in main systems and onboard alarm;
- data transmission every 15 minutes during operation to the brigade's central server via the existing communications network;
- integration into a technical management application linked to maintenance records;
- algorithms for anomaly detection and failure-risk estimation.

Figure 1 presents the KPI-based monitoring structure of the system, showing how telemetry data and CMMS records are integrated and evaluated against predefined performance thresholds, where a "warning" indicates an early deviation from normal parameters and a "recommended intervention" denotes a threshold level requiring corrective maintenance action.

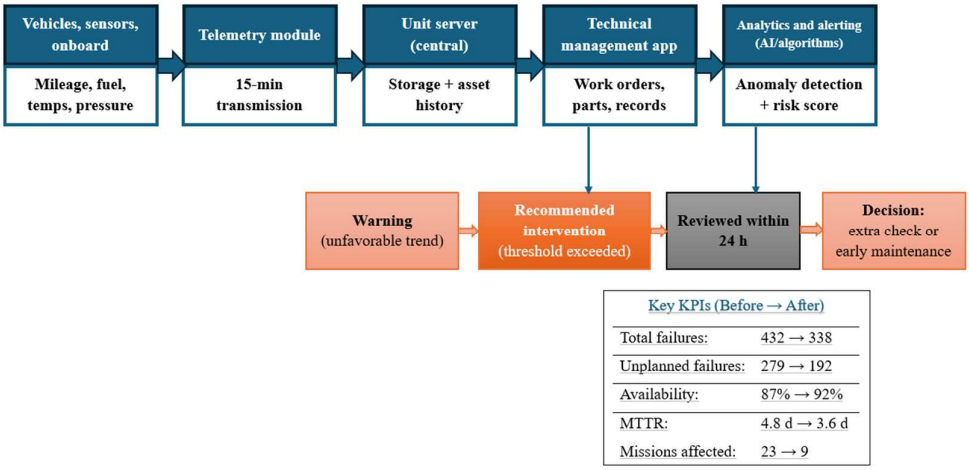


Fig. 1. Data-driven fleet maintenance workflow and KPI impact

Alerts:

- "warning" (unfavorable parameter trend);
- "recommended intervention" (parameters above defined thresholds).

Procedural rules:

- every "recommended intervention" alert is reviewed by the vehicle workshop chief within 24 hours;
- based on that review, the unit schedules an additional check or performs maintenance before the standard interval.

In the first full year, total failures dropped from 432 to 338(−22%), unplanned failures from 279 to 192(−31%), MTTR from 4.8 to 3.6 days, availability increased from 87% to 92%, and postponed missions fell from 23 to 9.

The evaluation report indicates that cooling-system failures on armored vehicles dropped by ~40%, and in 21 cases alerts led to preventive checks and planned replacement of components (hoses, gaskets, pumps) before a major crack occurred.

In parallel, supply actions and team allocation were initiated earlier, weekly plans became more stable, and field emergencies decreased.

This study uses a synthetic case dataset designed to reflect plausible maintenance and logistics dynamics. The purpose is to demonstrate the proposed data-to-decision workflow and to test KPI behavior under controlled assumptions; therefore, numerical results should be interpreted as illustrative rather than empirical evidence.

6.2. CNC workshop

The workshop produces and refurbishes spare parts for vehicles, generator sets, and various equipment. The workshop operates five computer numerical control (CNC) machines (three machining centers, two lathes), four conventional machines, and 14 personnel working two shifts per day.

Maintenance was periodic and reactive, with downtime recorded in logbooks. Each CNC averaged four unplanned stoppages per year, lasting three days, totaling approximately 60 downtime days and a 7% reject rate. *In a year, about 2 cases the workshop failed to meet delivery deadlines for part batches, forcing downstream replanning.*

Most common causes:

- unexpected wear of main-spindle bearings;
- lubrication system issues;
- jams caused by chip and debris accumulation;
- positioning drift due to mechanical shocks or overloads.

In the simulated post-implementation scenario, sensor-based monitoring (vibration, temperature, electrical current) was integrated into a local server and linked to maintenance records for anomaly-based alerting.

The adaptive learning engine processes structured learner inputs, including response accuracy, decision time, error type, and scenario difficulty. A supervised classification model identifies recurring error patterns and knowledge gaps, while performance metrics are updated dynamically. Based on this analysis, the system generates targeted feedback, recommends additional modules, and adjusts scenario complexity. Learner progression is evaluated through periodic performance scoring and scenario-based reassessment to ensure measurable skill improvement.

Anomaly-detection model (after the first 3 months):

- "normal" vibration and temperature zones defined for each machine and operating regime;
- alerts:
  - level 1: moderate deviation, suggesting a check at the next scheduled inspection;
  - level 2: significant deviation, recommending machine stoppage and detailed diagnostics.

Weekly routine:

- the workshop chief reviews automatically generated reports (vibration trends, temperatures, number of alerts);
- based on reports, decides early checks, machining-parameter adjustments, or increased cleaning frequency.

In the simulated post-implementation scenario, modeled stoppages decreased, stoppages decreased to two per machine per year, unplanned stoppage to 1.5 days, downtime to approximately 30 days, and reject rate to 3.5%, eliminating delivery delays.

Table 1 presents the comparative "before/after" KPI results for the CNC workshop case, including total downtime (days/year), unplanned stoppages (events/machine/year) and reject rate (%). The quantitative values presented in Table 1 are derived from the structured illustrative dataset described in Section 4 and reflect simulated performance scenarios rather than empirical measurements from a specific operational workshop. The before-and-after comparison represents modeled performance variation under defined parameter adjustments and should be interpreted as methodological demonstration rather than field-validated outcomes.

Table 1

CNC workshop KPIs: before-and-after performance

Indicator	Unit	Before	After	Relative change (%)
Late deliveries	cases/year	2	0	100

Reject rate	%	7	3.5	50
Total downtime	days/year	60	30	50
Average stoppage duration	hours	3	1.5	50
Unplanned stoppages	events/ machine/ year	4	2	50

For one machine, an upward vibration trend triggered three level-2 alerts in four days. Inspection found advanced bearing wear, and bearings were replaced in a planned manner, avoiding spindle seizure and scrapped batches. Using the data, the workshop differentiated preventive-maintenance frequency, stricter for two machine, and less frequent for other two. Like this, it was justified investment requests to replace two older machines, supported by quantified downtime, associated costs, and delivery impact. Table 1 consolidates the impact of the approach by expressing the main performance gains as percentage improvements.

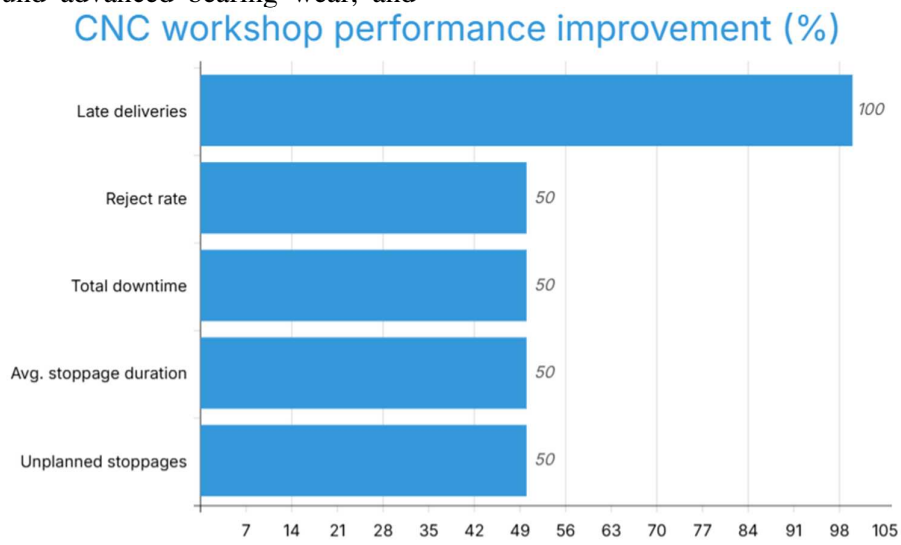


Fig. 2. CNC workshop performance: percentage improvements in key KPIs

Recent publicly available NATO documentation indicates that agencies such as the NATO Support and Procurement Agency (NSPA) coordinate large-scale sustainment and maintenance support activities for complex defense systems, with a documented focus on availability, lifecycle support, and performance optimization [13]. In parallel, studies published under the NATO Science and Technology Organization (STO) framework address predictive maintenance methodologies aimed at reducing unscheduled downtime and improving operational readiness through data-driven approaches [14]. Although detailed operational datasets are not publicly accessible due to security constraints, these documented initiatives confirm the practical relevance of predictive analytics and structured maintenance optimization within NATO contexts. The illustrative case studies presented in this article were therefore designed in alignment with publicly reported operational objectives and documented performance directions observed in allied maintenance modernization efforts.

The datasets used in the case studies are illustrative rather than empirical, as access to real operational maintenance records is limited by security constraints. The reported values were generated using a structured statistical simulation approach based on Poisson-modeled failure frequencies, calibrated repair-time distributions, and defined performance-adjustment factors to ensure coherent and reproducible KPI outcomes.

The proposed technical stack is structured in four layers:

(1) data acquisition layer, including sensors and digital log entries;

(2) data processing and storage layer, integrating secure data pipelines and standardized formats;

(3) analytics layer, where anomaly detection and fault-risk models operate;

(4) decision-support interface layer, providing dashboards, alerts, and traceable outputs for human validation.

Cybersecurity and access-control mechanisms should operate across all layers.

7. WORKFORCE COMPETENCIES AND REFERENCE ARCHITECTURE

Digital transformation and the introduction of AI in logistics and maintenance are reshaping not only equipment and IT systems, but also the professional profile of military personnel. Technicians, warrant officers, and officers are no longer just procedure users. They are becoming advanced users of data and digital tools.

In a modern logistics system, military technicians work not only with wrenches and classic measuring tools, but also with electronic diagnostic interfaces, maintenance management applications and automatically generated reports based on sensor data.

Digital transformation requires technicians to develop digital literacy, interpret sensor-based indicators, work within integrated systems, collaborate across specialties, and critically evaluate AI-generated recommendations rather than accept them unconditionally. They should neither trust the system blindly nor ignore it. A new skill is needed: critical evaluation of algorithm outputs.

AI tools support not only equipment operation, but also training. AI-assisted training platforms adapt content based on performance patterns, provide clarification through virtual assistants, and generate scenario-based exercises that simulate operational pressure.

These tools should be used in balance. They should not replace hands-on training on real equipment, but complement it. In career courses, the focus should be on teaching trainees how to use AI as a learning aid. While AI-assisted training improves theoretical understanding and scenario exposure, operational competence must be validated through hands-on interaction with real equipment. Practical training therefore remains essential to ensure reliable performance under real-world conditions.

Beyond technical upskilling, digital transformation requires careful change management. Resistance may arise from limited digital literacy, concerns about increased monitoring, or distrust in algorithmic recommendations. A gradual implementation strategy, pilot projects, leadership engagement, and clear preservation of human decision authority are essential to ensure acceptance and sustainable adoption.

A balanced training roadmap should integrate AI-assisted digital learning with structured scenario-based exercises and supervised hands-on validation. Digital modules can develop data interpretation and decision-support skills, while scenario exercises simulate operational pressure, and real-equipment practice confirms technical proficiency.

8. RECOMMENDATIONS FOR DIGITAL MILITARY LOGISTICS

Achieving full interoperability across heterogeneous national systems and legacy equipment requires a phased approach. First, a data-normalization layer can map local maintenance records and codification schemes to NATO standardized formats. Second, semantic harmonization ensures that key indicators such as availability, downtime, and failure categories are defined consistently across systems. Third, selective digital retrofitting of mission-critical platforms enables sensor integration without requiring full fleet replacement. Finally, federated interoperability can be achieved through secure APIs and standardized data-exchange protocols, allowing

coexistence of legacy and modern systems during transition.

Full implementation requires financial, logistical, and time investment, which may vary significantly across NATO members depending on existing infrastructure and digital maturity. For less technologically advanced organizations, immediate large-scale deployment may not be feasible, making phased migration aligned with available budget cycles and resource constraints essential. The proposed tiered architecture supports gradual adoption without imposing disproportionate initial costs. A scalable implementation pathway differentiating core functions for smaller units and full-suite deployment for large bases is summarized in Table 2.

Table 2

Scalable Resource Allocation for Modular Digital Logistics Implementation

Component / Cost Driver	Small Units – Core Functions	Large Bases – Full Suite Implementation
Data governance, codification	Standardized digital records; basic data harmonization	Enterprise-level data governance; integrated multi-domain data
Sensing and asset monitoring	Limited sensors on mission-critical assets; local gateways	Fleet-wide sensing; advanced telemetry and predictive modules
Data platform and integration	Lightweight, interoperable cloud	Centralized data platform with integrated supply
Cybersecurity and training	Baseline access control and monitoring; technical training	Zero-trust architecture, continuous monitoring, dedicated IT/SOC

The model organizes digital transformation in layered steps, from equipment and sensors to local collection, a central data and application platform, and a decision layer. It reflects existing military command structures and allows modular, gradual implementation instead of a single large deployment. Industry 4.0 principles are linked to concrete logistics functions, connecting real-time visibility, analytics, controlled local autonomy, and modularity with asset tracking, maintenance planning, inventory control, and transport optimization.

Main limits concern data quality and integration into current force structures. The model requires consistent records for equipment, maintenance, consumption, and stocks, yet many organizations rely on mixed paper, spreadsheet, and legacy systems with uneven codification, which reduces AI effectiveness without prior standardization. Equipment diversity adds difficulty: newer assets can transmit data, older or partially upgraded ones cannot, so connectivity priorities and methods to combine digital inputs with field observations are necessary.

Progress should start with stronger data governance: standardized identifiers, clear entry and validation procedures, measurable data-quality indicators, and defined responsibilities across all levels. The long-term objective is a secure, fully digital logistics ecosystem where technical, logistics, and operational data circulate under controlled governance, analytics and AI support decisions, and interoperability with allied standards is maintained.

9. CONCLUSION

The paper shows a clear shift in how a NATO member state should organize logistics and maintenance: from a system that mainly reacts to shortages and failures to one that anticipates them using data, continuous monitoring, and models. Industry 4.0 is useful here because it frames logistics as an integrated cyber-physical ecosystem, not a set of disconnected registries and reports. A practical outcome is a layered architecture, from equipment and sensors, to local collection and filtering, to a central data and analytics platform, and finally to the decision level where dashboards and planning tools translate data into operational choices. This modular approach supports phased adoption without disrupting existing command-and-support structures and helps maintain interoperability from the start.

Across the logistics functions, AI has a defined role as decision support, not decision

replacement. Predictive analytics improves demand estimation and stock sizing, while anomaly detection and reliability models enable condition-based and risk-based maintenance instead of purely calendar-driven servicing. Pattern discovery links failures and consumption to real operating contexts, and optimization models can support stock positioning, transport planning, and prioritization under constraints and risk. The same logic reshapes maintenance into a readiness lever: fewer unplanned stoppages, better timing of interventions, stronger justification for spares and investment decisions, and more stable support during deployments and exercises. None of this works without people: technicians and logistics leaders need digital literacy, the ability to interpret trends and alerts, disciplined data entry in integrated systems, and critical judgment when validating model outputs. AI-enabled training tools can accelerate learning through adaptive modules and scenario practice, but they must complement hands-on work on real equipment.

The model also makes cybersecurity and resilience non-negotiable. A digital logistics system can become a target, so segmentation, access control, encryption, monitoring, auditing, and clear degraded-mode procedures are required, along with redundancy in infrastructure and in trained personnel. The critical risks are familiar and solvable: inconsistent data and codification, mixed fleets where not all platforms can be connected, organizational resistance, and the temptation to treat AI as a product rather than a continuously validated process. A realistic path is incremental, built on data governance first, followed by well-scoped pilots, gradual onboarding of prioritized equipment classes, and expansion from maintenance into movement and transport analytics, while mapping interfaces to NATO standards and tools to avoid national dead ends. Done this way, digital transformation becomes a credible modernization route with measurable readiness gains, rather than a fragile IT project.

Future research should extend the proposed framework toward an Industry 5.0 perspective, emphasizing human–AI collaboration, resilience in contested environments, interoperability validation, and empirical testing based on real operational data.

10. REFERENCES

[1] NATO Standardization Office, *Allied Joint Doctrine for the Reception, Staging and Onward Movement of Forces (AJP-4.6)*, Edition C, NATO Standardization Office, Brussels, 2018.

[2] Paksoy T., Kochan Ç. G., Ali S. S., Logistics 4.0: Digital Transformation of Supply Chain Management, CRC Press, ISBN 978-0-429-32763-6 (eBook), Boca Raton, 2020.

[3] Toth Z., Goga A.-S., Boscoianu M., AI *Integration in Fundamental Logistics Components: Advanced Theoretical Framework for Knowledge Process Capabilities and Dynamic Capabilities Hybridization*, Logistics, MDPI, eISSN 2305-6290, Basel, 2025.

[4] NATO, *NATO Logistics Handbook*, NATO Logistics Committee, ISBN 978-92-845-0190-8, Brussels, 2012.

[5] Boscoianu M., Toth Z., Goga A.-S., *Sustainable Strategies to Reduce Logistics Costs Based on Cross-Docking—The Case of Emerging European Markets*, Sustainability, MDPI, eISSN 2071-1050, Basel, 2025.

[6] Lasi H., Fettke P., Hoffmann M., *Industry 4.0.*, Business & Information Systems Engineering, eISSN 1867-0202, Berlin, 2014.

[7] Lee J., Bagheri B., Kao H. A., *A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems*, Manufacturing Letters, ISSN 2213-8463, Vol. 3, Elsevier, Amsterdam, 2015.

[8] Achouch M., Dimitrova M., et al., *On Predictive Maintenance in Industry 4.0: Overview, Models, and Challenges*, Applied Sciences, ISSN 2076-3417, Basel, 2022.

[9] Minculete G., *Relational Approaches to Modernizing Operational Logistics Related to Industry 4.0 and Supply Chain Management 4.0*, Journal of Defense Resources Management, eISSN 2247-6466, Brașov, 2021.
[10] NATO Standardization Office, *Allied Joint Doctrine for the Conduct of Operations (AJP-3)*, Edition D, Version 1, NATO Standardization Office, Brussels, 2025.
[11] NATO Standardization Office, *Allied Joint Doctrine for Logistics (AJP-4)*, Edition C, Version 1, NATO Standardization Office, Brussels, 2025.
[12] NATO Standardization Office, *Allied Joint Doctrine for Movement (AJP-4.4)*, Edition C, NATO Standardization Office, Brussels, 2022.
[13] NATO Support and Procurement Agency, *Annual Report,* 2024
[14] NATO Science and Technology Organization, *Advanced Analytics and Artificial Intelligence for Defence Enterprise Resource Planning,* ISBN 978-92-837-2378-3, 2022
[15] Milošević D. A., Ilić D., Vulić M., *Machine Learning for Predictive Maintenance in Industry 4.0: Current Trends and Challenges*, Acta Technica Corviniensis – Bulletin of Engineering, eISSN 2067-3809, Hunedoara, 2024.
[16] Zonta T., da Costa C. A., Righi R. R., de Lima M. J., da Trindade E. S., Li G. P., *Predictive maintenance in the Industry 4.0: A systematic literature review*, Computers & Industrial Engineering, ISSN 0360-8352, Vol. 150, 106889, Elsevier, Amsterdam, 2020.
[17] Chandola, V., Banerjee, A., Kumar, V., *Anomaly Detection: A Survey*, ACM Computing Surveys, ISSN 0360-0300, Vol. 41, No. 3, Article 15, ACM, New York, 2009.
[18] Susto, G. A., Schirru, A., Pampuri, S., McLoone, S., Beghi, A., *Machine learning for predictive maintenance: A multiple classifier approach*, IEEE Transactions on Industrial Informatics, ISSN 1551-3203, New York, 2015.

Transformarea digitală a logisticii militare în era Industriei 4.0: AI pentru dezvoltarea competențelor tehnice și optimizarea mentenanței

Rezumat. Lucrarea analizează modul în care un stat membru NATO poate moderniza logistica și mentenanța militară prin principiile Industriei 4.0 și prin AI ca suport decizional. Logistica este tratată ca funcție operațională, influențată de interoperabilitatea multinațională, dislocarea rapidă și mediile contestate. Este propusă o arhitectură de referință pe niveluri, care conectează senzorii și nodurile locale la o platformă centrală de date, module analitice și tablouri de bord, cu securitate cibernetică și reziliență integrate. Sunt discutate analiza predictivă, detectarea anomaliilor, estimarea fiabilității și optimizarea stocurilor și transporturilor, precum și dezvoltarea competențelor și instruirea asistată de AI. Recomandările vizează guvernanța datelor, proiecte pilot etapizate și alinierea la standardele aliate.

Ciprian CUSUTURĂ, Engineer, "Nicolae Bălcescu" Land Forces Academy of Sibiu, Romania, cusutura.ciprian@armyacademy.ro, +40 269 432 990, 3-5 Revolutiei Street, Sibiu, Romania.
Toma PLEȘANU, Professor, Engineer, PhD, "Nicolae Bălcescu" Land Forces Academy of Sibiu, Romania, plesanu.toma@armyacademy.ro, +40 269 432 990, 3-5 Revolutiei Street, Sibiu, Romania.
Tiberiu GIURGIU, Associate Professor, Engineer, PhD, "Nicolae Bălcescu" Land Forces Academy of Sibiu, Romania, giurgiu.tiberiu@armyacademy.ro, +40 269 432 990, 3-5 Revolutiei Street, Sibiu, Romania.