

A Review Study of AI-Driven Smart Manufacturing for Quality Enhancement in Defence Production and Directions for Future Research

Gagandeep Singh^{*1}, Dr Smriti Verma², Dr Aarti Chopra³

¹Research Scholar, Faculty of Management & Commerce, Poornima University, Jaipur, Rajasthan, India.

Email ID:gagan1552@gmail.com

²Senior Assistant Professor, Symbiosis Institute of Business Management, Nagpur, Maharashtra, India.

Email ID:smritiyash@gmail.com

³Dr Aarti Chopra, Associate Professor, Poornima University, Jaipur, Rajasthan, India.

Email ID:aarti.chopra2@poornima.edu.in

***Corresponding Author**

Gagandeep Singh

Research Scholar, Faculty of Management & Commerce, Poornima University, Jaipur, Rajasthan, India.

Email ID:gagan1552@gmail.com

ABSTRACT

Defence manufacturing follows a near-zero tolerance for quality failure, however, AI applications in manufacturing quality continue to be heavily researched in the context of civilians. This literature review attempts to summarize 58 articles under four themes – intelligent quality inspection and predictive quality management, smart factories, manufacturing reliability and resilience, and human-AI collaboration along with associated security and implementation issues – in order to understand how smart manufacturing driven by AI can contribute towards quality improvement in the context of defence manufacturing. Through a thematic synthesis based on PRISMA guidelines, it has been found that although inspection, predictive maintenance and cyber-physical systems in factories have reached technological maturity in the civilian domain, the same has not been verified in the classified environment of defence manufacturing, especially in the Indian scenario of defence indigenization. Six research gaps are presented and a future research agenda is proposed, besides presenting an integrative conceptual framework which associates the four enablers in a defence manufacturing-specific context with quality improvement in defence manufacturing.

Keywords: artificial intelligence, smart manufacturing, quality management, defence production, Industry 4.0, systematic review.

1 INTRODUCTION

The production of defence products is unique in the manufacturing industry because, in contrast to civilian sectors, any failure in quality control of these products could result in loss of life, mission failure, and loss of strategic advantage. The process of quality management in this sector has been laborious and depended on manual inspection and a multi-level approval system based on military specifications. With the advent of Industry 4.0 and 5.0 in manufacturing, there has arisen a new purpose technology called artificial intelligence (AI) that is changing the face of quality inspection, prediction, and assurance.

AI-driven smart manufacturing is currently made up of computer vision based defect detection, quality prediction modeling, digital twins, and cyber-physical production systems (Hozdić, 2015; Shrouf et al., 2014), with systematic reviews showing consistent gains in accuracy and reliability in automotive, electronics, and food processing industries (Morales Matamoros et al., 2025). Defence manufacturing, on the other hand, is a different context altogether owing to classification requirements, sensitivity of data, and high standards of quality assurance which result in the defence industry being a more reserved adopter than civilian industry even while some of the technologies have high adoption potentials (Ullah et al.,

2024). This is especially true in the Indian case where there is a specific indigenisation policy in place and the DRDO is working towards AI stack sovereignty (Forbes India, 2026) and Defence AI Council has been set up to implement 70 projects related to AI across DUSPs (Press Information Bureau, 2023).

This notwithstanding, there is no dedicated academic synthesis of the topic of quality improvement through use of AI technology in defence manufacturing. This study attempts to fill the gap through systematic synthesis of literature through four thematic streams.

2. REVIEW METHODOLOGY

2.1 Review Approach

This study uses thematic synthesis informed by systematic review methodology instead of meta-analytic statistics due to the heterogeneous methodologies used in the literature. The systematic review is conducted according to the PRISMA 2021 statement (Page et al., 2021) with an additional thematic-analysis coding process—approach widely used nowadays when conducting systematic reviews within the management area (Mishra & Mishra, 2023).

2.2 Literature Search Strategy

The literature has been sourced from Scopus, Web of Science, IEEE Xplore, ScienceDirect, and SpringerLink

databases. Search strings consisted of combinations of the following three concept groups: (i) AI, machine learning, or predictive analytics; (ii) manufacturing, smart factory, or Industry 4.0/5.0; and (iii) quality, reliability, predictive maintenance, defense, or cybersecurity. The timeframe for the search was 2014–2026, focused on 2020–2026. Government and industry data sources (DRDO, Press Information Bureau) have been used to provide the Indian defence production context but are not considered as academic sources.

2.3 Inclusion and Exclusion Criteria

Studies were selected based on whether they were peer-reviewed, published between 2014 and 2026 in English, and with the full study available, and which addressed AI or machine learning usage in manufacturing quality, smart factories, predictive maintenance, or human-AI interaction and cybersecurity in a manufacturing

environment. Studies that discussed AI purely from a theoretical perspective without application in a manufacturing setting, consumer marketing studies not pertaining to manufacturing quality, duplicate datasets which had been collected earlier, or any technical content lacking, except when used in defence policy context, were not selected.

2.4 Literature Screening and Selection

Screening followed a four-stage PRISMA-style process (Figure 1). An initial pool of 612 records was identified; after removing 127 duplicates, 485 records were screened by title and abstract, excluding 275 as off-topic. The remaining 210 full-text articles were assessed for eligibility, excluding 152 that did not meet inclusion criteria. A final set of 58 studies was retained for thematic synthesis.

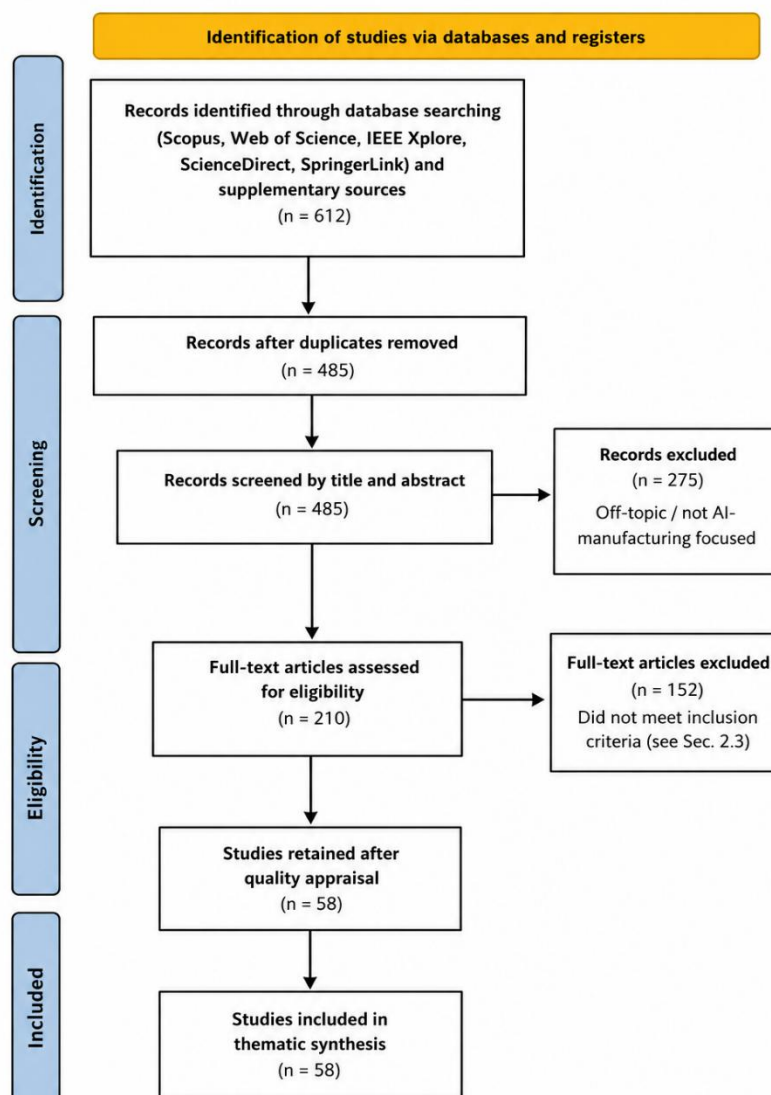


Figure 1. Literature screening and selection process

2.5 Thematic Synthesis Procedure

Open coding was done for each selected article in order to establish repeated ideas, while axial coding was utilized

in grouping these ideas into broad themes. Inductively four major themes emerged: (1) AI-enhanced intelligent quality inspection and quality management; (2) smart

factory integration and intelligent manufacturing process; (3) AI-enhanced manufacturing reliability; and (4) human-AI collaboration and security issues.

3. THEMATIC ANALYSIS

3.1 Theme 1: AI-Enabled Intelligent Quality Inspection and Predictive Quality Management

The best researched AI application in quality control in manufacturing is intelligent inspection. Manual inspections are estimated to have a maximum precision rate of 80%, while advanced deep learning techniques manage to achieve an almost perfect score of 99.86% accuracy on defect data of cast products (Sundaram & Zeid, 2023). Object detection networks further increase

the potential to apply deep learning to real-time inspection of small low-contrast surface defects, directly applicable to inspection of armour-plates in defence manufacturing (Jayawardena et al., 2026). Predictive quality management, predicting yield over the course of the whole product lifecycle, is pivotal in the concept of today's Quality 4.0, although the level of explainability in comparison to detection accuracy still lags behind (Morales Matamoros et al., 2025; Hoffmann & Reich, 2023). In case of the defence industry, human digital twins create objective and time-stamped evidence of conformity in aerospace assembly (Colaw et al., 2025), and a classified defence environment is a limiting factor in research of AI based inspection. Table 1 lists four sub-themes of this thematic area.

Table 1. Thematic Summary – Intelligent Quality Inspection and Predictive Quality Management

Core Theme	Core AI Technologies	Key Findings	Representative Studies	Relevance to Defence
Deep-Learning-Based Visual Inspection	CNN architectures, YOLO object detection	Deep-learning inspection substantially outperforms manual (~80%) and rule-based methods, reaching up to 99.86% accuracy on defect-detection tasks	Sundaram & Zeid (2023); Jayawardena et al. (2026)	Real-time, high-precision inspection of armour-plate and structural components
Explainable AI (XAI) for Quality Assurance	Explainable/interpretable AI systems	Detection accuracy is consistently prioritized over interpretability, despite explainability being essential for auditable inspection decisions	Hoffmann & Reich (2023)	Auditability is critical where inspection decisions must be defensible to quality-assurance authorities
Predictive Quality Management & Zero-Defect Manufacturing	Big-data analytics, predictive quality modelling	Forecasting product quality and yield across the production lifecycle is a central pillar of Quality 4.0, spanning quality management, zero-defect manufacturing, and perceived-quality frameworks	Morales Matamoros et al. (2025); Jagatheesaperumal et al. (2022)	Shifts quality assurance from reactive detection toward proactive, lifecycle-wide defect prevention
Defence-Specific Digital Inspection Applications	Human digital twins, cloud-based cameras, AI detection algorithms	Human digital twins generate objective, time-stamped evidence of conformity for aerospace assembly; Indian precision manufacturers are integrating AI-driven quality control into aerospace production	Colaw et al. (2025); India Strategic (2025)	Directly transferable to auditable inspection of mission-critical aerospace and armour components

Source: Author's own compilation, based on the reviewed literature.

3.2 Theme 2: Smart Factory Integration and Intelligent Production Systems

Intelligent factory integration acts as the basic framework into which AI-powered quality management tools are embedded based on cyber-physical systems, real-time data integration, and value chain connectivity (Hozdić, 2015; Shrouf et al., 2014). In the case of defence manufacturing in particular, manufacturing execution systems, big data analytics, robotics, and additive manufacturing show high maturity levels, whereas digitalization proceeds more cautiously due to intrinsic

security limitations (Ullah et al., 2024). Such selectivity can be seen even in the context of the evolution of India, which has Defence Industrial Corridors and additive manufacturing collaborations that help realize indigenous technology integration (Drishti IAS, 2025), alongside the overall smart manufacturing transformation expected to increase the manufacturing gross value significantly by 2035 (Forbes India, 2026). The use of digital twins transforms quality management into a proactive approach throughout the whole life cycle of an asset (Razorleaf, 2024), a feature that is especially important in the case of long-life defence assets. Table 2 contains the list of sub-themes of the considered thematic area.

Table 2. Thematic Summary – Smart Factory Integration and Intelligent Production Systems

Core Theme	Core AI Technologies	Key Findings	Representative Studies	Relevance to Defence
Cyber-Physical Systems & IoT Integration	Cyber-physical systems, IoT, real-time data integration	Provides the structural backbone into which AI-enabled quality tools are embedded across the value chain	Hozdić (2015); Shrouf et al. (2014)	Foundational infrastructure for indigenised, digitally integrated defence production
Industry 4.0 Technology Maturity in Defence	Manufacturing execution systems, big-data analytics, autonomous robots	MES, big data, robotics, and additive manufacturing show high defence maturity, while broader digitalisation proceeds cautiously; seven recurring concerns identified, including security and information ownership	Ullah et al. (2024)	Signals where defence manufacturers can adopt Industry 4.0 fastest, and where caution is warranted
Additive Manufacturing & Indigenisation	Additive manufacturing (3D printing)	Defence Industrial Corridors and additive-manufacturing partnerships enable rapid, low-volume, high-precision component production	Drishti IAS (2025)	Directly supports India's indigenisation agenda (Atmanirbhar Bharat) in defence manufacturing
Digital Twins for Lifecycle Quality Management	Digital twins	Shifts quality management from a reactive “controlling quality” posture to a proactive “managing quality” posture across an asset’s entire lifecycle	Razorleaf (2024)	Particularly valuable for long-lived defence platforms such as aircraft and military vehicles

Source: Author's own compilation, based on the reviewed literature

3.3 Theme 3: AI-Enabled Manufacturing Reliability and Operational Resilience

Predictive maintenance represents the most developed reliability-focused AI application in manufacturing through data analysis to predict equipment failure and intervene on time instead of waiting for its occurrence (Cheng et al., 2022). This predictive approach works best in combination with the manufacturing system’s ability to adapt and recover from disruption (Kumar & Ramakrishnan, 2024), an approach that has direct implications for the military sector, which can’t afford to have any delays in maintaining the continuity of supply of its critical platforms. One of the persisting limitations,

however, remains the data scarcity: generative AI and data–model–human approaches have been suggested to produce training data where historical failure records are not available (Ramzan & Reforgiato Recupero, 2025), a problem which is much more acute in the classified context of defence applications. Digital twins improve resiliency through the feedback of fielded asset performance data into manufacturing operations and design processes (Razorleaf, 2024), while Indian Air Force and Navy are reported to use AI-based predictive maintenance in practice (Invest India, 2025). Four sub-themes are identified in Table 3.

Table 3. Thematic Summary – Manufacturing Reliability and Operational Resilience

Core Theme	Core AI Technologies	Key Findings	Representative Studies	Relevance to Defence
AI-Driven Predictive Maintenance	Condition-based monitoring, predictive maintenance algorithms	AI-driven predictive maintenance measurably increases equipment uptime and reliability while reducing maintenance costs	Cheng et al. (2022)	Sustains continuity of supply for mission-critical defence platforms
Predictive Maintenance–Resilience Integration	Resilient-manufacturing frameworks	Predictive capability alone is insufficient unless paired with a system’s capacity to adapt to and recover from disruption	Kumar & Ramakrishnan (2024)	Directly relevant where prolonged unscheduled downtime cannot be tolerated
Data Scarcity & Generative AI Solutions	Data–model–human (DMH) framework, generative AI, large language models	Generative AI approaches can synthesize training data to support maintenance decisions where historical failure data is scarce	Ramzan & Reforgiato Recupero (2025)	Addresses defence’s structural data-scarcity challenge from classified and compartmentalized records

Core Theme	Core AI Technologies	Key Findings	Representative Studies	Relevance to Defence
Operational Resilience & Lifecycle Feedback	Digital twins, fielded-asset performance data	Digital twins close the loop between in-service reliability and manufacturing quality; AI-driven predictive maintenance is reportedly already used operationally	Razorleaf (2024); Invest India (2025)	Extends fielded-asset lifecycle and informs future design and production decisions

Source: Author's own compilation, based on the reviewed literature

3.4 Theme 4: Human–AI Collaboration, Security and Implementation Challenges

Theme 4 relates to the socio-technical and security parameters which will define the implementation process. Building trust into collaborative AI and robotic systems should begin at the very design stage as opposed to adding it as an afterthought. The factors found to play the key role in the establishment of operator trust include transparency, explainability and reliability (Elgohr et al., 2026). In the context of safety, precision and efficiency which characterize the manufacturing field, it is the symbiotic approach to human-AI collaboration that is most suitable (Fragiadakis et al., 2024), considering the

high impact that incorrectly calibrated trust has in a hierarchical culture of defence operations. Security cannot be overlooked here. Predictive AI algorithms can succumb to the risks associated with distributional drift, model inversion and data poisoning (Castillo-Villar et al., 2026; Aslam et al., 2025), which in the context of defence may lead to the clandestine undermining of the reliability of mission-critical equipment. In India, this problem is recognized, with the creation of a Defence AI Council and Defence AI Project Agency controlling 70 AI initiatives (Press Information Bureau, 2023). Table 4 shows four sub-themes of the thematic area.

Table 4. Thematic Summary – Human–AI Collaboration, Security, and Implementation Challenges

Core Theme	Core AI Technologies	Key Findings	Representative Studies	Relevance to Defence
Trust as a Design Principle	Explainable and adaptive control systems	Trust must be designed into collaborative AI systems from the outset; transparency, explainability, and reliability are critical determinants of operator trust	Elgohr et al. (2026)	Especially critical in defence's high-consequence, disciplined operational culture
Human–AI Collaboration Frameworks	Symbiotic human–AI collaboration models	A “symbiotic” mode of collaboration best fits manufacturing's emphasis on safety, accuracy, and productivity; explainability decomposes into interpretability and fidelity	Fragiadakis et al. (2024)	Miscalibrated trust—over-reliance or unwarranted rejection—is especially costly in defence settings
AI Cybersecurity Vulnerabilities	AI-ICS security, anomaly detection	Predictive AI models are susceptible to distributional drift, model inversion, and data poisoning; poisoning, evasion, and extraction attacks are active, growing concerns	Castillo-Villar et al. (2026); Aslam et al. (2025)	A compromised AI system could covertly degrade the reliability of mission-critical equipment
Institutional & Governance Challenges	AI governance frameworks	India's Defence AI Council and Defence AI Project Agency oversee 70 AI projects, signalling institutional intent but also the scale of the implementation challenge	Press Information Bureau (2023); Nelson et al. (2023)	Reflects AI's dual-use character and the governance questions this raises for defence adoption

Source: Author's Own Compilation, Based On The Reviewed Literature

4. RESEARCH GAPS AND FUTURE RESEARCH DIRECTIONS

4.1 Major Research Gaps

There arise six closely related gaps. The first one is that of sector specificity; defence sector empirical work is scarce because of data classification issues rather than lack of activities within the industry. The second one is that of data scarcity and explainability gap; predictive models

require huge amounts of data that can be provided by the defence sector while explainable-AI methods that were tested using open datasets have not been checked in the classified environment yet. The third one is a unique human-AI trust gap arising in the context of defence sector hierarchical and high-stakes environment which is unlike the civilian manufacturing plant environment. The fourth gap is that of framework integration; there is no research where all the quality inspection, smart-factory integration,

reliability and human-AI/security aspects are looked into specifically in the defence sector production. The fifth gap is the one between cybersecurity and quality, that is, there is little research that focuses explicitly on the issue of how the vulnerability of AI might translate to stealth quality failure in the defence parts production. The last gap is that of policy-practice evaluation; despite the existence of Defence AI Council and DPSU roadmaps of India.

4.2 Future Research Agenda

Six areas deserve focus. Empirical studies conducted in defense-representative settings—Defence Industrial Corridors or iDEX testbeds, for instance—could help confirm the performance of AI models under realistic data-scarce conditions. Privacy- and federated learning-based architectures suitable for compartmentalized defense data could help fill the data-scarcity void. Studies on trust calibration among defense production workers, not just civilian workers, would help determine if existing collaboration frameworks need to be adapted. Cyber-physical resilience frameworks integrating Quality 4.0/5.0

concepts and defense cybersecurity would fill the cybersecurity-quality nexus void. Cross-country studies that explore AI adoption maturity across defense industrial bases would contribute to institutional insights. Longitudinal studies of DPSU AI roadmap projects in terms of quality and reliability metrics would help fill the policy-practice evaluation void.

4.3 Proposed Conceptual Framework

The relationship between the aforementioned thematic enablers and defence contextual moderators is illustrated in Figure 2, in which the four moderators are regulation and security, military specification, skill, and indigenisation such as the ‘Atmanirbhar Bharat’ policy. These moderators will influence the relationship between the enablers and the primary outcome of the proposed theoretical framework: quality improvement in defence manufacturing, which will lead to mission-critical reliability, lower lifecycle cost, and increased self-reliance. This framework is only a beginning for the research agenda above mentioned.

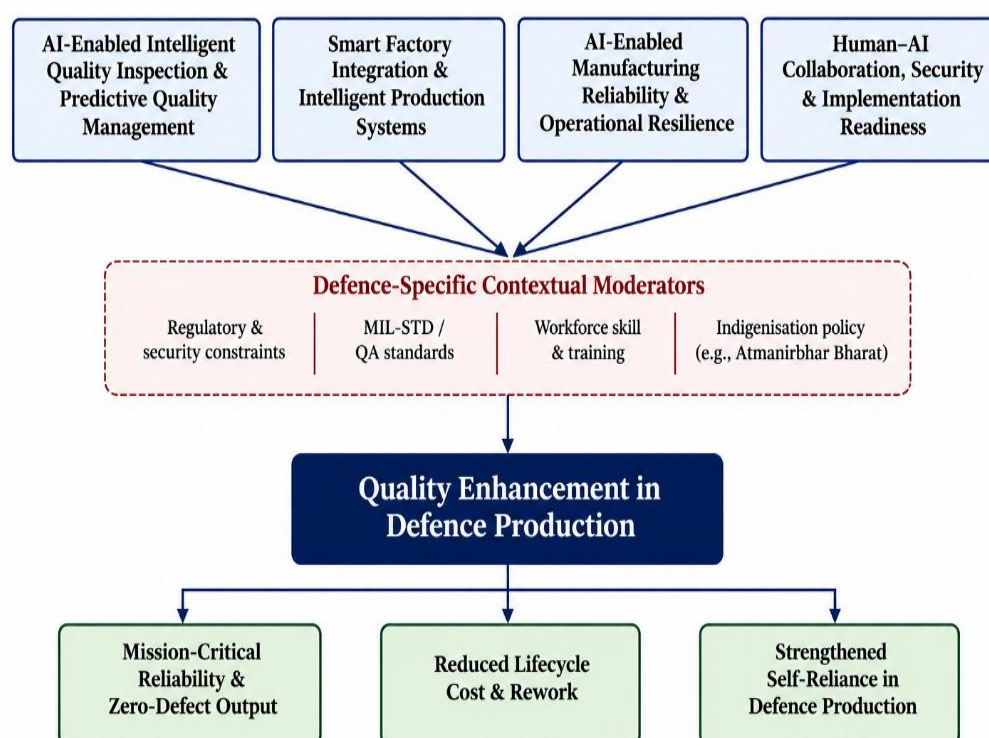


Figure 2. Proposed conceptual framework for AI-driven quality enhancement in defence production.

5. CONCLUSION AND IMPLICATIONS

5.1 Conclusion

The use of artificial intelligence technology has been quantitatively changing the quality of manufacturing in the civilian industrial sector, and in the domain of defence manufacturing, where there is an emphasis on indigenisation policy in India, this is now also happening, although not with the same level of comfort as in civilian industries. While the thematic synthesis reveals that the technical maturity is high for the industrial sector as a whole, there are few validations in the defence manufacturing sector due to security issues.

5.2 Theoretical Implications

In that regard, this review adds an integrative theoretical conceptual framework that connects the broader literature on Quality 4.0 and AI in manufacturing with contextual moderators specific to the defense industry, drawing from similar conceptualizations found elsewhere. This paper also adds to the body of knowledge on dual-use AI (Nelson et al., 2023) by applying it to the quality management literature.

5.3 Practical Implications

AI-based inspection and predictive maintenance capabilities that have been proven within civilian applications of high-end manufacturing can serve as the most promising starting point for manufacturers of defence equipment. For quality managers, explainability and auditability must be considered as primary

requirements owing to standards of accountability in the defence industry. For technology managers, security of AI, especially its robustness against data poisoning and model inversion, should be assessed as an integral part of implementation of the quality system. For policy makers, the institutional framework of India (Defence AI Council, Defence AI Project Agency, DPSU Roadmaps) could use some investment in evaluation research.

5.4 Limitations and Future Scope

This research, however, is a literature-based thematic review and is limited by the breadth of studies being synthesized. As dedicated research on AI manufacturing quality in the defence sector is sparse in the literature, several points made about the defence sector had to be based on literature from the civilian sector and India-related policy and industry reports, not on defence sector literature itself—an aspect that is reflective of, and explains, the research gap addressed in this paper. The review is also limited to English literature, as well as to databases used in the search process. Further research should aim at validating the propositions suggested in this research review.

REFERENCES

1. Aslam, M. M., Tufail, A., Gul, H., et al. (2025). Artificial intelligence for secure and sustainable industrial control systems: A survey of challenges and solutions. *Artificial Intelligence Review*. Advance online publication. <https://doi.org/10.1007/s10462-025-11320-9>
2. Castillo-Villar, K. K., Dai, H., Martinez Medina, G., & Mehrzadi, H. (2026). Cybersecurity for smart and resilient manufacturing and supply chains: A systematic review of the evolving knowledge base. *Computers & Industrial Engineering*. Advance online publication. <https://www.sciencedirect.com/science/article/pii/S0360835226004456>
3. Cheng, X., Chaw, J. K., Goh, K. M., Ting, T. T., Sahrani, S., Ahmad, M. N., Kadir, R. A., & Ang, M. C. (2022). Systematic literature review on visual analytics of predictive maintenance in the manufacturing industry. *Sensors*, 22(17), 6321. <https://doi.org/10.3390/s22176321>
4. Colaw, C. L., Madison, G., Tseng, B., Griser, G. M., Truelson, G., Gallo, A., & Hurmuzlu, Y. (2025). Methodology for enablement of human digital twins for quality assurance in the aerospace manufacturing domain. *Sensors*, 25(11), 3362. <https://doi.org/10.3390/s25113362>
5. Drishti IAS. (2025). Empowering India's defence sector. <https://www.drishtias.com/daily-updates/daily-news-editorials/empowering-indias-defence-sector>
6. Elgohr, A. T., Rashad, M., El-Gendy, E. M., Shaaban, W., & Saafan, M. M. (2026). Trust as a design principle in human–robot collaboration: A review of explainable and adaptive control. *Artificial Intelligence Review*, 59(5), Article 134. <https://doi.org/10.1007/s10462-026-11554-1>
7. Forbes India. (2026). Reimagining manufacturing: How India is building its next industrial advantage. <https://www.forbesindia.com/article/upfront/brand-connect/reimagining-manufacturing-how-india-is-building-its-next-industrial-advantage/2997617/1>
8. Fragiadakis, G., Diou, C., Kousiouris, G., & Nikolaidou, M. (2024). Evaluating human-AI collaboration: A review and methodological framework. *arXiv*. <https://arxiv.org/abs/2407.19098>
9. Hoffmann, R., & Reich, C. (2023). A systematic literature review on artificial intelligence and explainable artificial intelligence for visual quality assurance in manufacturing. *Electronics*, 12(22), 4572. <https://doi.org/10.3390/electronics12224572>
10. Hozdić, E. (2015). Smart factory for Industry 4.0: A review. *International Journal of Modern Manufacturing Technologies*, 7(1), 28–35.
11. India Strategic. (2025). Artificial Intelligence (AI) in Indian defence. <https://www.indiastrategic.in/artificial-intelligence-ai-in-indian-defence/>
12. Invest India. (2025). India's defence tech boom: Six opportunities in an expanding strategic sector. <https://www.investindia.gov.in/team-india-blogs/indias-defense-tech-boom-six-opportunities-expanding-strategic-sector>
13. Jagatheesaperumal, S. K., Rahouti, M., Ahmad, K., Al-Fuqaha, A., & Guizani, M. (2022). The duo of artificial intelligence and big data for Industry 4.0: Applications, techniques, challenges, and future research directions. *IEEE Internet of Things Journal*, 9(15), 12861–12885. <https://doi.org/10.1109/JIOT.2021.3139827>
14. Jayawardena, A., Sul, J.-H., Moratuwage, D., Wijayaraja, J. L., & Piyathilaka, L. (2026). State of the art in AI-based visual inspection for industrial quality control: Methods, benchmarks, challenges, and autonomous systems. *Electronics*, 15(12), 2727. <https://doi.org/10.3390/electronics15122727>
15. Kumar, J. H., & Ramakrishnan, R. (2024). Artificial intelligence-enabled predictive maintenance for the resilient manufacturing: Current applications and challenges. In *Predictive maintenance and resilient manufacturing systems*. Springer. https://doi.org/10.1007/978-981-97-4700-9_27
16. Mishra, V., & Mishra, M. P. (2023). PRISMA for review of management literature – Method, merits, and limitations – An academic review. In S. Rana, J. Singh, & S. Kathuria (Eds.), *Advancing methodologies of conducting literature review in management domain*. Emerald Publishing.
17. Morales Matamoros, O., Takeo Nava, J. G., Moreno Escobar, J. J., & Ceballos Chávez, B. A. (2025). Artificial intelligence for quality defects in the automotive industry: A systemic review. *Sensors*, 25(5), 1288. <https://doi.org/10.3390/s25051288>
18. Nelson, J. P., Biddle, J. B., & Shapira, P. (2023). Applications and societal implications of artificial intelligence in manufacturing: A systematic review (arXiv:2308.02025). *arXiv*. <https://arxiv.org/abs/2308.02025>
19. Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2021 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71. <https://doi.org/10.1136/bmj.n71>
20. Press Information Bureau, Government of India. (2023). Self-reliance in production of defence products.

<https://www.globalsecurity.org/wmd/library/news/india/2023/india-230210-india-pib03.htm>

21. Ramzan, F., & Reforgiato Recupero, D. (2025). A literature review on enhancing predictive maintenance in smart manufacturing industries: Fostering human-technology collaboration and overcoming data scarcity limitations with advanced AI models. *SN Operations Research Forum*, 6(4), 1–30. <https://doi.org/10.1007/s43069-025-00584-0>
22. Razorleaf. (2024). Why digital twin is mission critical for aerospace & defense manufacturing companies. <https://www.razorleaf.com/blog/why-digital-twin-is-mission-critical-for-aerospace-defense-manufacturing-companies/>
23. Shrouf, F., Ordieres, J., & Miragliotta, G. (2014). Smart factories in Industry 4.0: A review of the concept and of energy management approached in production based on the Internet of Things paradigm. In *Proceedings of the 2014 IEEE International Conference on Industrial Engineering and Engineering Management* (pp. 697–701). IEEE.
24. Sundaram, S., & Zeid, A. (2023). Artificial intelligence-based smart quality inspection for manufacturing. *Micromachines*, 14(3), 570. <https://doi.org/10.3390/mi14030570>
25. Ullah, H., Uzair, M., Jan, Z., & Ullah, M. (2024). Integrating industry 4.0 technologies in defense manufacturing: Challenges, solutions, and potential opportunities. *Array*, 23, Article 100358. <https://www.sciencedirect.com/science/article/pii/S2590005624000249>